كلية الحقوق و العلوم السياسية

قسم: الحقوق

الحماية الجنائية للاسرار المعلوماتية

مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر أكاديمي حقوق

تخصص قانون جنائي

إعداد الطالبتين:

- معطالله عبد الحميد
- بن كريد جيلالي

اشراف الأستاذ

د. بن بادة عبد الحليم

لجنة المناقشة

إسم ولقب الأستاذ	الرتبة	الجامعة	الصفة
د.فروحات سعيد	أستاذ محاضر أ	جامعة غرداية	رئيسا
د.بن بادة عبد الحليم	أستاذ محاضر ب	جامعة غرداية	مشرفا ومقررا
د بن رمضان عبد الكريم	أستاذ محاضر ب	جامعة غرداية	ممتحنا

السنة الجامعية:

2019م / 2020م – 1440هـ / 1441هـ


بسم الله الرحمن الرحيم

الإهداء

الحمد لله المتصرف في الملك والملكوت، الباقي الذي لا يفنى ولا يموت القائل في محكم كتابه: {إنا نَحْنُ نَرِثُ الْأَرْضَ وَمَنْ عَلَيهَا والينا يرْجَعُونَ {40} سورة مريم، والصلاة والسلام على السراج المنير معلم الإنسانية والبشرية، وأخرج به الناس من الظلمات إلى النور، سيدنا محمد عليه أفضل الصلاة وأزكى التسليم، وعلى آله وأصحابه والتابعين لهم بإحسان إلى يوم الذين.

هكذا بمشيئة الله جل جلاله وبتظافر جهود الكثير من الأوفياء والأصدقاء، الدين لم يبخلوا علينا ولو بكلمة تدخل البهجة وسر القلب في سبيل إنجاز هذه المذكرة أتقدم بجزيل الشكر إلى الوالدين الكريمين وكل العائلة الكريمة، جميع أفراد الأسرة، كما أهدي هذا العمل إلى جميع الأصدقاء والزملاء، سواء في العمل أو الحي أو الدارسة في الجامعة، كما أهذي هذا العمل إلى كل الأساتذة الكرام، سائلا المولى عز وجل أن يجازيهم عنا خير الجزاء.

إهداء

شكر وعرفان

الحمد لله الذي أنار لنا درب العلم والمعرفة
وأعاننا على أداء هذا الواجب ووفقنا إلى
انجاز هذا العمل العلمي الأكاديمي
أولا وكما يقول عليه الصلاة والسلام "من لا
يشكر الناس لا يشكر الله" (رواه الترمذي في كتاب
البر والصلة وقال الترمذي حديث حسن(495).
نتوجه بجزيل الشكر والامتنان
إلى كل من ساعدنا من قريب أو من بعيد
على انجاز هذا العمل
وفي تذليل ما واجهناه من صعوبات
ونخص بالذكر الأستاذ المشرف الدكتور بن
بادة عبد الحليم
الذي لم يبخل علينا بتوجيهاته ونصائحه
القيمة
التي كانت عونا لنا في إتمام هذا البحث.
ولا يفوتنا أن نشكر كل طاقم قسم الحقوق من
الرئيس إلى الأمانة وكل أساتذة القسم
وبالخصوص اساتذة قسم الثانية ماستر قانون
جنائي.
كما نتقدم بالشكر إلى جميع موظفي جامعة
غرداية
وبالأخص موظفي طاقم مكتبة قسم الحقوق
والمكتبة المركزية.
كل الأصدقاء والزملاء في الجامعة وكل من ساهم
في دعم ومساعدة الطالب الجامعي

قائمة المتخصرات

1. ج.ر.ج.ج.د.ش: الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية
2. ق.ع.ف.: قانون العقوبات الفرنسي
3. ق.ع.ج.: قانون العقوبات الجزائري
4. ق.ع.م.: قانون العقوبات المصري
5. ق.م.ج.: قانون المدني الجزائري
6. ق.م.ف.: قانون المدني الفرنسي
7. م.ق.ج.: المجلة القضائية الجزائرية
8. ج.م.: الجريمة المعلوماتية
9. م.م.: المجرم المعلوماتي

بالغة الأجنبية

1- O.C.D.E : L'Organisation de Coopération et de Développement écnomique

2- O.E.C.D : Organisation for Economic Co-operation and Development

3- D.A.R.P.A : Defense Advanced Research Project Agenecy

4- W.W.W. : World wide wele « le réseau d'information internationales »

5- C.C : Computer Crime : le crime par l'ordinateur la criminalité

6- T.C.P/I.P : Protocole de Transmission et de Contrôle.

7- F.T.P : File Transfer Protocol

8 -I.C.3: Internet Crime complaint Center

9-I.F.C.C: National White coller center

10-C.T.C: Computer and Télecommunication coordinattor

الملخص:

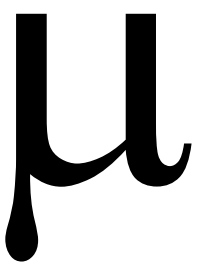
في هذه الدراسة ندرس الجريمة المعلوماتية دراسة تحليلية لكل ما يشملها وخصائصها وكذا تعامل المجتمع الدولي معها كونها حديثة الظهور وحاولنا معرفة ما مدى قدرة النصوص القانونية الجزائرية على كبح جماح منفذيها فقمنا في بداية بحثنا بشرح بعض المفاهيم للجرائم الماسة بأسرار المعلوماتية بداية بمفهوم الجريمة المعلوماتية بتعريفها والكشف عن بعض خصائصها وما يحيط بها من مصطلحات متعلقة بها من اجل ازالة الغموض الذي يواجه من يريد دراسة هذه الجريمة ثم تطرقنا الى بعض الاصناف من الجرائم التي تقع على اسرار المعلومات من جرائم الدخول او البقاء غير لمصرح بهما وجرائم سرقة المعلومات وكذا افشاء الاسرار كما تطرقنا الى بعض اساليب القيام بهده الجرائم من اختراق واستعمال مختلف الفيروسات وقد تعددت هذه الاساليب وتنوعت ومع تطور تكنولوجيا الاتصالات لا شك اننا سنشهد اساليب وتقنيات جديدة يعتمدها الذين احترفوا هذا النوع من الاجرام وبعدها كان لابد لنا من التحدث عن الحماية الجنائية لأسرار المعلوماتية من الناحية الاجرائية حيث تناولنا بداية اليات التحقيق والتحري عن المجرمين في هذه الجرائم ودلك باعتراض المراسلات وتسجيل الاصوات والتقاط الصور وغيرها وكذا الجهود الدولية والوطنية للحد من هده الجريمة الخطيرة ثم قمنا بسرد بعض العقوبات التي قررها المشرع الجزائري لبعض الجرائم فقد كشفنا عن بعض العقوبات المقررة على مرتكبي هده الجرائم سواء كان مرتكبها شخص طبيعيا او معنوي واشتملت هده الاخيرة على عقوبات اصلية واخرى.

الكلمات المفتاحية: لحماية. القانون. الاسرار. المعلومات.

Abstract

This research is about electronic crime or better to say cybercrime. Cybercrime is newly appearing crime that causes many damages to individuals, organisation, and even government. In this conducted research, we began with giving an explanation of some concepts related to cybercrime, as well as giving a definition of its terminology and characteristics to learn more about this type of crimes. Then we dealt with categories of electronic crime, so that includes illegal entry into accounts, breeches of privacy, stealing and divulging secrets. After that, we tried to find out the methods or ways that used to do this kind of crimes. For instance, hacking personal accounts, creating malfunctions and viruses. However, cybercrime's methods are still varied and numerous, especially with the development of technology, there are criminals working on developing new strategies in this field. Furthermore, we moved to highlight legal solutions to curb criminals and limit or reduce by giving the most effective solutions to protect the privacy of the information network. Besides that, we talked about the role of criminal law protection to preserve user's information and secret. In the end of this study, we touched upon the most important legal procedures and penalties stipulated in the Algerian Criminal Code to face or better say confront all types of cybercrime.

Key words: protection, Law, secret, the information.



مقدمة:

سمي القرن العشرين، بقرن الثورة المعلوماتية، وهذا بفضل الدور الذي تلعبه المعلومات في الوقت الحالي.

إذ تحتاج لها الدولة وأصحاب الاعمال وعموم الناس، فالمحور الرئيسي الذي قامت عليه هذه الثورة هو دون شك هي الانترنت، إي الشبكة المعلوماتية الدولية؛ وما انتجته من تطور مذهل في قطاعي تكنولوجيا المعلومات والاتصال والتداخل الحاصل بينهما.

ولان عصرنا الحالي أصبحت احدى مميزاته؛ بل من ابجدياته وضرورياته هي تكنولوجيا المعلومات، فقد اتاحت هذه الاخيرة وسهلت الاتصال والتواصل وحققت الانفتاح والتعايش، مع مختلف الاقطار والمجتمعات ولذلك سمي عصرنا هذا، بعصر المعلومات؛ لان حاجتنا للمعلومات أصبحت لا تخفى ولا ينكرها أحد فالحاجة لها؛ متعلقة بشتى جوانب الحياة وجميع الانشطة والتعاملات، لذا توجب على كل مجتمع يسعى الى تحقيق نموه وتقدمه، ان يتمكن من التحكم في الوسائط وأوعية المعلومات وتقنيات تخزينها واستعمالها عند الحاجة اليها.

اذن فالتحكم في التواصل الامثل وتخزين المعلومات وحمايتها، كونها في كثير من الاحيان تعتبر اسرار شخصية أو مهنية، ما يجعل من التفريط أو الرعونة والتساهل أو التهاون في تحقيق الحماية السديدة والمثلى لهذه المعلومات، يشكل تهديد محدقا بمصلحة الفرد أو صاحب هذه المعلومات مهما كانت صفته أو مركزه، ومن الواضح ان هذا الخطر وهذا التهديد؛ الذي يمس بسرية المعلومات اشد خطورة، مما كان عليه في السابق مع الوسائل التي كانت تستخدم وقتها.

اذن ففي مقابل، هذه الميزات والتسهيلات، نجد بعض الاخطار، التي تحملها في طياتها والتي قد نكون عرضة لها نتيجة لبعض الاستعمالات غير المشروعة، فيما تعارف على تسميتها بالجريمة المعلوماتية، وسميت

كذلك لكونها ارتبطت بالمعلومات، بما جاءت بها من تطور في وسائلها وكذا محل الجريمة لذلك اختلفت عن غيرها من الجرائم بخصائص وتقنيات عديدة.

لذلك تعتبر سرية المعلومات، أبرز الامور التي يسعى مستعملي برامج الحاسب وانظمة المعالجة الخاصة بشبكات المعلومات، باعتباره أحد الاهداف المعرضة للاعتداء.

من هنا تتضح أهمية موضوعنا هذا؛ الحماية الجنائية للأسرار المعلوماتية، كونه من الموضوعات الحديثة التي فرضت نفسها على المستوى المحلي والوطني والاقليمي وحتى الدولي، وهذا لان هذا الموضوع مرتبط بالشغل الشاغل لجميع مستخدمي تكنولوجيا المعلومات افرادا ومؤسسات، الا وهو ضمان سرية معلوماتهم، فضلا عما لهذا الموضوع من انعكاسات هامة؛ من الناحية العملية نظرا لاجتياح المعلوماتية لأغلب التعاملات والمجالات خاصة منها الفني والتقني.

ولذلك كان من الواجب؛ حماية الوسائط والاجهزة؛ التي تعالج أو تخزن فيها هذه المعلومات، من مختلف الاعتداءات والاختراقات، التي ستكون ضحية لها، وهذا بالنظر الى المؤهلات الفنية التي أصبح يتمتع بها، ما يطلق عليه المجرم المعلوماتي، ما يمكنه من نشر المعلومات، من مكانه الذي يتواجد فيه إلى اقصى اصقاع الدنيا وبالتالي يمكنه إلحاق اضرار بليغة جدا بضحيته وتهديده بنشر هذا، اذ لم يمتثل لطلباته اي ابتزازه بخطر كشف خصوصياته أو فقدانه لبعض ممتلكاته الفكرية أو المعنوية.

لذلك فان من أهم الاسباب، التي دفعت لاختيار هذا الموضوع، هي الوقوف على هذا النوع الجديد من الجرائم، الذي استفحل في كل العالم ومجتمعنا طبعا، مع الانتشار الواسع لاستخدام الانترنت وتسليط الضوء على عدم مشروعية انتهاك أسرار المعلوماتية ومحاولة التصدي لها والحد منها عن طريق ما نص عليه المشرع

الجزائري في القانون 04/15 المؤرخ في 10 نوفمبر 2004 في القسم السابع تحت عنوان المساس بأنظمة المعالجة الالية للمعطيات ذلك في المادة 394 مكرر[1]

كما ان النظام المعلوماتي، وما يتمتع به من قدرة على التخزين المعلوماتي ،ومن امكانيات تكنولوجيا تكاد لا تقف عند حدود، فهي في تطور مستمر وتجدد لا يكاد يتوقف وبفضل هذا التطور المطرد اصبح من الممكن جدا اقتحام حرمة الفردية وحتى الجماعية، وهتك سرية المعلومات بجميع انواعها وتعدد الاشكال الاعتداء خاصة مع توسع رقعة مستعملي الانترنت وتحسن تدفقها، اصبحت ميدانا خصبا للتخطيط والقيام بعدد لا حصر له من الجرائم، مع سهولة الافلات من الرقابة واعين الجهات الامنية ،فكلما سمعنا كلمة امن المعلومات فان أول ما يدور في خاطرنا أو مخيلتنا هو كشف معلومات ،كان الاجدر بها ان تبقى سراً أو الحقيقة، ان الحقيقة ان الحفاظ على سرية المعلومات وهو احد اشكال الامن المتعددة .

الهدف من دراستنا؛ لموضوعنا الموصوف بجريمة العصر؛ هو تحديد المقصود بالجريمة المعلوماتية والمجرم المعلوماتي والتعرف على كيفية اصباغ الحماية الجنائية على الجرائم الماسة بسرية المعلومات والإطار القانوني لهذه الجرائم وكذا الاليات والجهود المحلية والدولية المبذولة من اجل مكافحتها والاطلاع على مدى مسايرة المشرع الجزائري، من خلال قانون العقوبات للتطورات التكنولوجيا وما انتجته من مشاكل قانونية.

مع أول ظهور لشبكة الانترنت، لم يكن يساورنا؛ اي شك حيال ما قد تنتجه لنا من مشاكل أو سلوكيات مجرمة وهذا بسبب اقتصار استخدامها على اغراض البحث العلمي وبالتالي كانت منحصرة على فئة معينة توسع استخدامها وتغلغلها في حياة المجتمعات في شتى المعاملات وتضاعف اعداد مستخدميها، ظهرت لنا عدة اشكال من الجرائم، ازدادت وتنوعت مع اكتساب الافراد مهارات الاختراق والتعديل والنشر.

[1] القانون رقم 04-15 المؤرخ في 2004/11/04 المتضمن قانون العقوبات الجزائري المعدل والمتمم لأمر 156/66 الصادر في الجريدة الرسمية للجمهورية الجزائرية العدد 71 ا لمؤرخ في 8 جوان1966.

كما ان الجريمة المعلوماتية تختلف عن نظيرتها التقليدية، من الناحية العملية نظرا لان الأولى تكتسي طابعا معنويا في اغلب اثارها في حين يغلب على الثانية الاثر المادي الناتج عنها وهذا ما نجم عنه اشكالا في تفسير النصوص القانونية ومنع استعمال القياس في المواد الجنائية ومبدأ الشرعية الجنائية، الكثير من المجرمين يفلتون من العقاب.

ان الحماية لأسرار المعلوماتية، هي المطلب التي يرجو جميع اصناف مستخدمي تكنولوجيا المعلومات تحقيقه، ومن هذا المنطلق فيبرز لانا التساؤل العلمي، بشأن قدرة النظام القانوني الجزائري على مواجهة هذه الجرائم عند وقوعها؛ اي ما مدى قدرة النصوص العقابية التقليدية في الجزائر على الحد من الجرائم الماسة بسرية المعلومات الالكترونية؟ ام يتوجب عليها تطوير وتعديل وادراج تشريع جديد خاص بالجرائم الماسة بأسرار المعلوماتية؟ ولهذا المنهج الوصفي المقترن بالمنهج التحليلي في هذا البحث والذي اعتمدناه من اجل تحديد وتحليل الجرائم الماسة بأسرار المعلوماتية وفي سبيل اعداد بحثنا ارتأينا تقسيم هذه الدراسة الى فصلين:

الفصل الأول: تطرقنا فيه لمفاهيمي الحماية الجنائية الموضوعية؛ للجرائم الماسة للأسرية المعلوماتية من خلال مفهوم السرية، وتمييز السرية عن الخصوصية، تم الخصوصية المعلوماتية وهدا في المبحث الأول اما في المبحث الثاني تطرقنا الى تصنيف الجرائم الواقعة على اسرار المعلوماتية، من جريمة الدخول والبقاء غير الصرح بيهما، وجريمة الاعتراض غير القانوني، وجريمة سرقه الاسرار معلوماتية.

الفصل الثاني: تناولنا فيه الحماية الجنائية الاجرائية، ودلك بالتطرق الى المتابعة والتحقيق في الجرائم الماسة بإسرار المعلوماتية، بدايتنا بإجراءات التحري وجمع الأدلة، تم المكافحة الاجرائية في القانون الجزائري، والتحقيق في الجرائم وهدا في المبحث الاول، اما في المبحث الثاني آليات البحث والتحري، وتسجيل الاصوات واعتراض المراسلات والتقاط الصور، واجراءات المترتبة على المساس بإسرار المعلوماتية.

الفصل الأول

حماية الجنائيـة الموضوعيـة

تمهيد:

مما لا شك فيه انا كل شخص ،مهما كانت ديانته او مستواه التعليمي او الثقافي ،فان له جانب من الخصوصية في حياته لا يريد ان يطلع عليه احد وقد يؤدي اكتشافه من طرف غيره الى فضحه او تضرره مادي ومعنويا، لذلك فنجد أي شخص يسعى لحماية اسراره بكل ما يتأتى له من وسائل لمواجهة كل اشكال الاعتداء واقتحام لسريته ، الا اننا نجد بعض اللبس يقع بين الخصوصية والسرية، فنجد هنالك من يرى انهما لفظين يراد منهما معنى واحد ، في حين نجد من يرى ان كل منهما يدل على شيء مختلف عن الاخر في حين هناك من يرى انهما متدخلتان والاكيد في الامر انه سواء كانت الخصوصية والسرية بنفس المعنى او منفصلتين عن بعضهما البعض الا انهما يتفقان في كونهما شيء شخصي ،ينبغي الا يتعدى الغير والسبب في هذا التخوف هو اتقان بعض الاشخاص لتقنيات التحكم في تكنولوجيا المعلومات وتسخير هذه التقنيات واستعمال وسائط تساعدهم على تنفيذ عملهم الاجرامي، لأنه اصبح من السهل عليهم اقتحام الحياة الشخصية للأفراد وتنفيد ما تسول لهم انفسهم فيه بطرق و ادوات متطورة جدا وتقدم نتائج فورية وبدون ترك للأثار.

المبحث الاول: ماهية السرية في المجال المعلومات

توصف السرية في المجال المعلوماتي بالسرية المعلوماتية، والتي أصبحت ضرورية مع انتشار تقنية المعلومات وزيادة الاعتماد عليها من جهة، وانخفاض تكلفة معالجة تلك البيانات والمعلومات من جهة أخرى.

فالحاجة اليوم إلى حماية السرية المعلوماتية أصبحت ملحة وضرورية وتزداد باستمرار، خاصة بعدما أصبح الحاسب وسيلة جديدة للحفظ والتخزين وهي مميزات عالية جلبت معها مخاطر كبيرة وأصبحت فرصة الاطلاع على لأسرار المعالجة آليا أكثر سهولة، فضلا على إمكانية نسخها في وقت لا يكاد يلحظ، ناهيك عن إمكانية

اختراقها الاطلاع عليها من مسافات شاسعة، ولتحديد المقصود بالسرية المعلوماتية سيتم التفصيل في تعريف كل من السرية[1].

المطلب الأول: مفهوم السرية المعلوماتية

تعتبر السرية مفهوم قديم مرافق للإنسان بشكل مرافق لمصالحه الاجتماعية والاقتصادية والسياسية والعسكرية وغيرها، إلا أن هذا المفهوم قد طرأ عليه تغيير كان سببه الثورة الحالية في مجال الكمبيوتر وظهور الانترنت[2]. فأصبح لدينا ما يعرف بالسرية المعلوماتية، فما المقصود بالسرية المعلوماتية؟

الأمر يتطلب التطرق لمفهوم: الأحكام العامة للأسرار المعلوماتية السرية بشكل عام بطبيعة الحال في المجال القانوني، ثم التعرف على المقصود بالسرية المعلوماتية.

الفرع الأول: تعريف السرية وشروطها

سرية المعلومات انشغال لطالما كان من اهتمامات الإنسان مند القدم لارتباطه بجل مصالحة وعلى جميع الأصعدة، إلا أن هدا الانشغال طرأ عليه تغيير نتيجة التطور الحاصل بالتكنولوجيا الحديثة وظهور الثورة الحالية في مجال تقنية الحاسوب والاتصالات فبرز لدينا ما يسمى بالسرية المعلوماتية.

أولا: تعريف السرية

تباينت تعاريف السرية بين اللغوية والاصطلاحية، قد تختلف في صياغتها ولكن دوما تبقى تصب في نفس المضمون، وهي كالتالي:

[1] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، مصر، 2006 ص 56.

[2] رابحي عزيزة. الأسرار المعلوماتية وحمايتها الجزائية. أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد – تلمسان352ص.2018.

1-تعريف السرية لغة:

السرية مؤنث السري، والسري المنسوب إلى السر، السري الذي يصنع سرا، والسر ما يكتم ويخفى، والسر من كل شيء: أكرمه وخالصه[1]. والسر ما يسره المرء في نفسه من الأمور التي عزم عليها، قال تعالى:﴿ **وإن تجهر بالقول، فإنه يعلم السر وأخفى** ﴾[2].

والسر أيضا من الأسرار التي تكتم والسر ما أخفيت والجمع أسرار، ورجل سري: يصنع الأشياء. سرا من قوم سريين[3].

والسر هو ما أخفيه وأكتمه وهو خلاف الإعلان ويستعمل في المعاني والأعيان. والجمع أسرار قولك: أسررت الحديث أي أخفيت[4].

وأسره كتمه، وأسر إليه حديثا: أفضى، كقوله تعالى:﴿ وإذ **أسرّ ال نّبي إلى بعض أزواجه حديثا.** ﴾ [5]، ويرى البعض أن السر هو كل ما يضر إفشاؤه بالسمعة أو بالكرامة[6]، ويرى البعض الآخر أن الواقعة تعتبر سرا إذا كانت هناك مصلحة يعترف بها القانون في حصر . العلم بها في شخص أو أشخاص محددين[7].

---

[1] محمد مصطفى الشقيري، السرية المعلوماتية، ضوابطها وأحكامها الشرعية، الطبعة الأولى، دار البشائر الإسلامية، للطباعة والنشر بيروت لبنان، 2008، ص 266.

[2] سورة طه، الآية رقم 6.

[3] جمال الدين أبي الفضل محمد بن مكرم ابن منظور الأنصاري الإفريقي المصري، راجعه عبد المنعم خليل إبراهيم، المجلد الثالث، الطبعة الأولى دار الكتب العلمية بيروت لبنان، 2005، ص 333.

[4] الرازي محمد بن أبي بكر، مختار الصحاح، دار الكتب العلمية، بيروت، لبنان، 1983، ص 146.

[5] سورة التحريم، الآية رقم 3.

[6] عصام أحمد البهجي، حماية الحق في الحياة الخاصة، في ضوء حقوق الإنسان والمسؤولية المدنية، دار الجامعة الجديدة، للنشر الإسكندرية، مصر ،2005، ص 90.

[7] علي أحمد عبد الزغبي، حق الخصوصية في القانون الجنائي، دراسة مقارنة، الطبعة الأولى، المؤسسة الحديثة للكتاب، طرابلس، لبنان، 2006، ص 185.

2تعريف السرية اصطلاحا :

السر هو ما يفضي به الإنسان إلى آخر متكتما إياه من قبل أومن بعد، ويشمل ما حفت به قرائن دالة على طلب الكتمان إذا كان العرف يقضي بكتمانه، كما يشمل خصوصيات الإنسان وعيوبه التي يكره أن يطلع عليها الناس، وهو أمانة لدى من استودع حفظه، التزاما بما جاءت به الشريعة الإسلامية وهوما تقتضي به المودة وآداب التعامل[1].

ويعرف أيضا أنه واقعة أو صفة ينحصر نطاق العلم بها في عدد محدود من الناس، إذا كانت ثمة مصلحة يعترف بها القانون لشخص أو أكثر في أن يظل العلم بها محصورا في ذلك النطاق[2].

والملاحظ أن السرية وكما يشير المعنى اللغوي هو صناعة تعتمد على إرادة الشخص نفسه في تحديد مكامن مصالحه، فهل الكتمان وإخفاء السر عن الغير هو الأفضل، لقوله صلى الله عليه وسلم: "استعينوا على قضاء حوائجكم بالكتمان فإن كل ذي نعمة محسود "، أم في الإفشاء وعندها، فعليه تحمل علم الغير بما لم يجب علمهم به.

تم تعريف السرية أيضا بواسطة المنظمة الدولية للتوحيد القياسي (ايزو) على أنها "ضمان أن تكون المعلومات متاحة فقط لأولئك الذين يؤذن لهم بالاطلاع"، وهي أحد الأركان الأساسية لأمن المعلومات، فالسرية هي واحدة من أهداف التصميم لنظم ترميز كثيرة، مما جعلها ممكنة من الناحية العملية عن طريق تقنيات التشفير الحديثة [3] وحيث أصبحت الأسرار مخزنة في ذاكرة الحاسب الآلي بعدما كانت توضع في خزانة مقفلة، تولد لدينا الأسرار المعلوماتية والتي نقصد بها الأسرار المعالجة آليا، أي تتناول المعالجة الآلية للمعلومات السرية بشكل منظم وفعال

[1] محمد مصطفى الشقيري، المرجع نفسه، ص 267.

[2] عصام احمد البهجي، حماية الحق في الحياة الخاصة، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2005، ص، 90-91.

[3] أنظر الموقع الالكتروني http://ar.wikipedia.org/wiki، يوم الاطلاع 2020/05/17، الساعة (12:20).

بحيث لا تكون هذه المعلومات في مجموعها أوفي الشكل والتجميع الدقيقين لمكوناتها معروفة عادة أو سهلة الحصول عليها من قبل الأشخاص خاصة الذين يتعاملون في نوع تلك المعلومات.

ثانيا: شروط اتصاف الواقعة بالسرية

ان التطرق لتعريف السرية قد يصعب علينا أحيانا تحديد وصف الواقعة بالسرية من عدمها، وسواء كان السر بمفهومه الحديث أو التقليدي يشترط لتحديد طبيعته مجموعة من الشروط، يمكن أن تتلخص في الآتي:

1 -أن يكون السر بطبيعته أو بسب الظروف المحيطة به : لقد انقسم الفقه بشأن تحديد طبيعة السر إلى اتجاهين اتجاه أخذ بالمعيار الشخصي، حيث يتم تحديد وصف السرية عن طريق صاحب السر طواعية، أما الاتجاه الآخر فيأخذ بالمعيار الموضوعي الذي يعتمد في تحديد وصف السرية بالنظر إلى الظروف والأحوال الموضوعية التي أحاطت بالواقعة، كالمعلومات التي تتصل بالحياة الخاصة للأفراد، وبأسرارهم المالية والتجارية والشخصية.[1]

2 –أن لا يكون معلوما للكافة: يفقد الأمر صفة السرية إذا كانت الواقعة التي تتعلق بها معلومة للكافة، على أنه ينبغي أن يلاحظ هنا بأن الطابع السري للواقعة أو المعلومة لا ينتقي حتى لو كانت معروفة بهذا الشكل أي للكافة، ما دامت غير مؤكدة.

فالسر يمكن أن يكون معلوماً من قبل عدد محدود من الناس حتى لو كان كبيراً ما داموا من محيط عائلي، أو من محيط عمل واحد، وبرغم ذلك يبقى طابع السرية ملازماً له. بينما تنتفي صفة السرية عن الواقعة، حتى لو لم يعلم بها كثير من الناس، إذا علم بها من لا تربطهم بصاحب السر علاقة خاصة، كالعلم بالوقائع عن طريق جلسة محاكمة علنية.[2]

[1] أنظر الموقع الالكتروني، http://www.mohamah.net/law الموقع نفسه.

[2] أنظر الموقع الالكتروني، http://www.mohamah.net/law، الموقع نفسه.

الفرع الثاني: أنواع الأسرار المعلوماتية

تتنوع الأسرار وتختلف باختلاف الأشخاص والظروف فما يعتبر سرا بالنسبة لشخص قد لا يعتبر سرا بالنسبة لآخر وما يعتبر سرا في ظروف معينة قد لا يعتبر كذلك في ظروف أخرى.

فمثلا هناك الأسرار الاقتصادية، والتي تتعاظم أهميتها في الوقت الراهن والمستقبل بالنسبة للدول والمشروعات الخاصة. حيث أصبحت الأسرار الاقتصادية هي أساس المنافسة الاقتصادية بين الدول والكيانات الاقتصادية. كما توجد الأسرار الدبلوماسية ويقصد بها، الحقائق بعلاقات الدولة الدبلوماسية بأشخاص القانون الدولي العام، مثل اعتراف الدولة بقطع علاقاتها السياسية بدولة معينة أو الاعتراف بهيئة ثورية معينة وكذلك المعلومات المتعلقة بسير المفاوضات السياسية .

كما توجد الأسرار العسكرية وتشمل كل ما يتعلق بالشؤون العسكرية والاستراتيجية. هذا بالإضافة إلى وجود ما يسمى بالأسرار الإدارية، وأيضا الأسرار الخاصة بالأفراد، أسرار التقاضي، الأسرار المهنية وغيرها وهكذا يمكن أن نتصور أن السرية بصفة عامة تشبه دائرة كبيرة يتم تقسيمها إلى أجزاء غير متساوية وغير محددة ومن هذه. الأجزاء ما يكون متعلقا بسرية المراسلات، وما يكون متعلقا بسرية لتحقيقات، وغيرها[1] وحيث أنه للتوضيح أكثر بشأن أنواع الأسرار المعلوماتية، كان لابد من التطرق لأنواع المعلومات الالكترونية بصفة عامة، والتي تعتبر المعلومات الالكترونية السرية جزء منها وتفاديا للتكرار فالمعلومات التي تتصف بالسرية هي المعنية بالدراسة، والتي هي خلاف ذلك فليست هي المقصودة بهذه الدراسة مثل المعلومات المتاحة .

أولا: المعلومات الإسمية

وتنقسم بدورها إلى مجموعتين وهما المعلومات الشخصية والمعلومات الموضوعية كالتالي:

[1] عصام أحمد البهجي، مرجع سابق، ص 98 وما بعدها.

أ – المعلومات الشخصية:

هي المعطيات المعلوماتية الاسمية أو الشخصية وهي المعلومات المرتبطة بالشخص كالحالة الاجتماعية أو المدنية كالاسم واللقب والجنسية والسوابق العدلية وغيرها. ووفقا أغلبية القوانين انعدام حق الغير في الاطلاع على هذه المعلومات مراعاة للخصوصية إلا في حالة وجود موافقة شخصية من صاحبها أو بأمر من السلطة المختصة.[1]

والجدير بالذكر أن المشرع الفرنسي، حاول إدراج تعريف صريح للمعطيات ذات الصيغة الشخصية وأنشأ لذلك هيئة مكلفة بحماية مصالح الأفراد الطبيعيين والذين تم جمع أو معالجة أو حفظ معلوماتهم.

ب – المعلومات الموضوعية:

هي بخلاف الشخصية موجهة إلى الغير وليست لصيقة بشخصية صاحبها، ومن أمثلتها المقالات الصحفية والملفات الإدارية للموظفين، وهناك من يرى أنه يمكن الفصل بين مالك المعلومة والشخصية المتصلة بها، فالصحفي الذي يكتب مقالا عن شخص معين له حق على المقال، ولكن لا يجب أن يتعدى على حق الشخص محل المقال نفسه. [2]

ثانيا: المعلومات الخاصة بالمصنفات الفكرية

هي معلومات متمثلة في مصنفات فكرية وهذه المصنفات محمية بقوانين الملكية الفكرية ويستوي في ذلك أن تكون تلك القوانين متعلقة بالملكية الأدبية والفنية أو متعلقة بالملكية الصناعية والعلامات التجارية[3]، كالمؤلفات والأغاني أو الأفلام أو البرامج المعلوماتية وغيرها.

[1] محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، 2004، ص 44.

[2] محمد أمين الرومي، مرجع سابق، ص 44.

[3] خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2009، ص 55.

ثالثا: المعلومات المباحة

هي تلك المعلومات التي يتاح للجميع الحصول عليها لأنها بدون مالك، مثال ذلك تقارير البورصة اليومية النشرات الجوية، وتنعقد ملكية هذه المعلومات للأسبق إلى جمعها وصياغتها. فإذا تم تجميعها وتخزينها واسترجاعها، أو بقصد تخليق معلومات جديدة فإنها لا تصبح متاحة بل ستتصف بالسرية وتنقسم إلى التالي:

أ – المعلومات المعالجة: ويقصد بها المعلومات التي تعالج للتشغيل على جهاز الكمبيوتر بقصد تخزينها وحفظها فيه واسترجاعها وقت الحاجة.

ب – المعلومات المتحصلة: ويقصد بها تلك المعلومات التي تنتج عن معالجة مجموعة من. المعلومات وتقرر حق ملكيتها هنا طبقا لقاعدة حيازة المال المنقول.[1]

الفرع الثالث: أسس السرية

ان موضوع حماية السرية المعلوماتية جزائيا هو من الموضوعات ذات الأبعاد المختلفة، فهو يمس الشخص من جميع الجوانب الاقتصادية والنفسية والنظامية وغيرها، ذلك أنه متعلق بضروريات تسعى الإرادة التشريعية للحفاظ عليها. لاسيما وأن كفالة حماية المعلومات السرية تحقق مبدأ عظيم من المبادئ القانونية وهي حفظ المصالح، بينما التعرض للمعلومات السرية بالإفشاء أو الاطلاع أو غير ذلك ينتج عنه أضرار جسيمة تؤثر في كيان الشخص وحتى الدولة.

لذلك كان لابد من التعرض لأسس السرية أو أسبابها، فمنها ما هو نفسي، اجتماعي، اقتصادي، وهناك ما هو قانوني وسيتم التفصيل فيها على النحو التالي:

[1] خالد ممدوح إبراهيم، المرجع نفسه، ص 55.

أولا: الأساس النفسي والاجتماعي

يعتبر السبب النفسي في كتمان السر الأساس الأول الذي يدعو إلى السرية، حيث أن أي شخص ترفض نفسه أن يعلم سره أي شخص غير مخول له بذلك، فيذهب جانب من الفقه إلى أن السرية يمكن تحليلها بأنها انعكاس للحذر الذي ينحو صوب الماضي، ويرفض الصراع في مواجهة المجهول[1] ويبقى الشخص دوما حريص على سرية معلوماته، بينما قد تتعرض هذه المعلومات لخطر الانتهاك بالوسائل الفنية حيث ترك الأفراد الوسائل التقليدية خلفهم في الوصول إلى المعلومات وأصبح اعتمادهم أكثر فأكثر على الانترنت والحاسب الآلي، وهو ما يسبب الأذى النفسي والمعنوي ربما الأكثر إضرارا منه عن المادي.

وعن الأساس الاجتماعي للسرية فهو يرتبط ارتباطا مباشرا بالأساس النفسي، ويمكن وصف السرية بصفة عامة أنها حدث اجتماعي يصف العلاقة بين مجموعة واحدة[2]، هذه العلاقة تحمل بين طياتها وظيفتين، الأولى تتعلق بالسلطة حيث يمنح السر لصاحبه قوة تميزه عن سواه، والثانية تتعلق بالفصل استنادا إلى أن بعض المعلومات يجب ألا تكون مباحة للجميع[3] فإذا كانت المعلومة هي القوة فإن الحفاظ عليها يعني استمرار القوة، وبالتالي فإن المصلحة تقتضي عدم العلم بها ممن لا يجوز لهم ذلك، وبالتالي فللسرية مدلول خارجي يحدد العلاقة بين من يملك السر و من لا يملكه [4] .

[1] نادية محمد معوض، أثر المعلومات على الحق في سرية الاعمال، كلية الحقوق، جامعة حلوان، الشارقة، بدون سنة، ص 33.

[2] SIMMEL (G.), La Sociéte Seréte, Novelle revue Psychanalyse, 1976, n° 14, P.281 .

[3] SIMMEL (G.), La Sociéte Seréte, Novelle revue Psychanalyse, 1976, n° 14, P.224 مرجع سابق، ص

[4] ZEMPLENI (A.), La Chàine du secret, Novelle revue Psychanalyse, 1976, N° 14, P .316

ثانيا: الأساس الاقتصادي والقانوني

للتحكم في المعلومات في المجتمعات المعاصرة دور متنامي وعامل أساسي في النجاح الاقتصادي، فلا شك أن المفاجأة بالنسبة للمنافسين والتشويق بالنسبة للعملاء والمضاربة في السوق أكيد أنها تتم من خلال السرية ولابد من إحاطة النظام المعلوماتي للمؤسسات الاقتصادية بالأمان لتحقيق النجاح.

والجدير بالذكر أنه بدون سرية المعلومات من المستحيل خلق مجتمع متماسك على جميع الأصعدة بما فيها الاقتصادية.

وفي نفس السياق يطرح السؤال عمن أين تستمد السرية مشروعيتها القانونية، والإجابة هي ما يعبر عنه بالأساس القانوني. وفي هذا المجال فإن القانون يحمي السرية من جميع الأصعدة المدنية من خلال القانون المدني والجزائية من خلال قانون العقوبات والقوانين المكملة له.

وما زاد من التخوف على السرية من الانتهاك، طبعا التقدم الهائل في المجال المعلوماتي حيث أنه يعتبر سبب أساسي في العصر المعلوماتي. فالثورة المعلوماتية التي ألقت بظلالها على جميع الأصعدة وباتت المعلومات السرية فيها أكثر تعرضا لخطر الانتهاك، والذي سيتم بكل سرعة وسهولة وألقت بظلالها أيضا على المعلومات الخاصة بالأفراد سواء كانت سرية أو لا، وهو الأمر الذي يتطلب البعض من التفصيل حول الفرق بين المعلومات السرية والخاصة بالأفراد.[1]

[1] SIMMEL (G.), OP.Cit, P.281. 24 المرجع نفسه، ص

المطلب الثاني: تمييز السرية عن الخصوصية

عند المرر بمصطلح السرية إلا وصادفنا مصطلح الخصوصية، ودراستنا هاته تتعلق أساسا بكل جوانب السرية المعلوماتية، ورأينا أنه من الواجب التطرق للخصوصية أو «السرية الشخصية كما يسميها البعض"[1]، ومعرفة العلاقة الموجودة بينها وبين السرية طالما أنه تم التعثر بها في أكثر من محطة ونحن بصدد هاته الدراسة.

"الخصوصية كحق عام يمتد لحماية الشخص من كافة أوجه الاعتداءات والتدخل في حياته، ويمكن القول أن كافة دول العالم على وجه التقريب أقرت بشكل أو بآخر الحق في الخصوصية في واحد أو أكثر من مظاهره. فالخصوصية مفهوم يتعلق بالعزلة والسرية، والاستقلال الذاتي ولكنها ليست مرادفة لهذه المصطلحات"[2]

فالخصوصية من الناحية اللغوية تقترب من مفهوم السرية لكنها ليست مرادفة له، وذلك لأن السرية تفترض الكتمان والتخفي في حين أن الخصوصية وإن كانت تفرض قدرا من الكتمان والتخفي لكنها قد تتوفر رغم انعدام السرية[3]. كما أن الخصوصية لا تقتصر على عدم الكشف عن الأسرار بل تعني كذلك الامتناع عن الاعتداء على هدوء الآخرين وسكينتهم[4]. ومنه فإن الحق في السرية يعد جوهر الحق في الخصوصية إن لم يكن وجها. لازما لهذا الأخير[5] ولكن رغم كل هذا، فإن هناك من يرى بأن السرية والخصوصية شيء واحد لهذا كان لابد من التعرض للعلاقة بين الخصوصية والسرية، فهناك اتجاهين تعرضا لهاته المسألة بين اتجاه قضى بضرورة الفصل بين الخصوصية والسرية ولم يعتبرهما شيء واحد واتجاه آخر يرى العكس وسنعرض الاتجاهين كالتالي:

---

[1] ماجد أحمد عبد الرحيم الحيارى، مسؤولية الصحفي المدنية، دراسة مقارنة بين القانونين الأردني والمصري، الطبعة، الأولى، دار يافا العلمية للنشر والتوزيع، عمان، الاردن ،2008، ص 30.

[2] فريد هكيت، الخصوصية في عصر المعلومات، ترجمة محمد محمود شهاب، الطبعة الأولى، مركز الأهرام للترجمة، والنشر، القاهرة، مصر، 1999، ص 34.

[3] ماجد أحمد عبد الرحيم الحيارى، مرجع سابق، ص 29.

[4] علي أحمد عبد الزغبي، حق الخصوصية في القانون الجنائي، دراسة مقارنة، الطبعة الأولى، المؤسسة الحديثة للكتاب، طرابلس لبنان، 2006، ص 125.

[5] علي أحمد عبد الزغبي، المرجع نفسه، ص 180.

الفرع الأول: الاتجاه الأول القائل بالفصل بين الخصوصية والسرية

يرى جانب من الفقه إلى أنه لا يجوز الخلط بين الحق في السرية والحق في الخصوصية، فالخصوصية مرحلة وسط بين السرية والعلنية فإذا كان المشرع يحمي الحق في الخصوصية فهو يحمي الحق في السرية من باب أولى ولكن يمكن أن يكون ما هو خصوصي ولكن لا يكون سريا في نفس الوقت. فالسر هو ما يعرفه صاحبه أو أمنية أما الخصوصي فهو ما لا ينشر أي ما لا يعتبر علنا مكشوفا للكافة حتى ولو لم يكن كتمانه قد وصل إلى حد السر.

ويؤسس وجهة نظره على الأسانيد الآتية:[1]

1-من الخطأ الكبير الخلط بين السرية والخصوصية فدقائق العلاقة بين الأزواج لا تتصف بالسرية لمعرفة الكثيرين بها من الأقارب والأصدقاء ولكنها مع ذلك تحتفظ بخصوصيتها ويحرص الشخص إلى عدم النشر خارج هذه الدائرة.

2-ويستشهد بما قضى به القضاء من إدخال وقائع تعتبر بعيدة كل البعد عن نطاق الحياة الخاصة وبعيدة عن السرية مثل الاسم فالاسم لا يعتبر سرا ومع هذا يدخلها القضاء في نطاق الحياة الخاصة.

3-ويضيف بأن مجرد النشر لبعض مظاهر الحياة الخاصة وكشف أسرار الحياة الخاصة إلى العلن وكشف النقاب عن السر يستحيل معه القول بأنه مازال هناك سرا فالكشف عن السر يحوله إلى العلن ويظل علنا دائما وأبدا ولا يتصور أن يعود العلن إلى حظيرة السرية وبالتالي يجوز إعادة النشر لهذه الأسرار دون الحصول على إذن أو رضاء من صاحب السر ولا يتصور وجود ضرر في إعادة النشر.

فلا يعقل أن يوصف بالسرية والخصوصية ما هو معلن على الملأ ومعروف للكافة فالكشف عن السر ولو مرة واحدة ينفي عنه إلى الأبد صفة السر ويدخله في نطاق العلنية ومن يقبل الكشف عن خصوصيات حياته فهو لم

[1] عصام أحمد البهجي، المرجع نفسه، ص، 103-104.

يقبل إلا الكشف عن السر أي نفي هذه الصفة عنه فإذا تم النشر فعلا في حدود ما سمح به الشخص فلا يقبل ولا يعقل بأن يعود مرة أخرى ويدعى أنه هناك مساسا بخصوصيات حياته قد وقع.

4-ويضيف أصحاب هذا الاتجاه بأنه لا يمكن فهم المسألة إلا إذا فرقنا بين السرية والخصوصية وفهمنا الأخيرة على أنها أكثر اتساعا من الأولى ويذهب البعض من أنصار هذا الاتجاه إلى أن الحياة الخاصة هي التي تدخل في نطاق السرية التي تكون للشخص على بعض أنشطته.

5-كما يضيف هؤلاء بأن الخصوصية لا تكون مرادفة للسرية حيث أن الخصوصية قد تتوافر على الرغم من عدم وجود السرية.

وينتهي هؤلاء إلى القول بأن السرية تفترض إذن الكتمان والخفاء التام أما الخصوصية فلا يلزم لتوافرها هذا القدر من عدم العلانية على الأقل في بعض جوانبها.

وينتصرون بما ذهب إليه إدوارد شليز أن الفارق بين السرية والخصوصية يكمن في أن السرية يحظر القانون الإعلان عنها بأي معلومات أو الكشف عنها أما في الخصوصية. فالكشف عن المعلومات أو الإعلان عنها مسألة ترجع إلى تصرف من يملك المعلومات[1]

الفرع الثاني: الاتجاه الثاني القائل بالربط بين السرية والخصوصية

ويرى أنصار هذا الاتجاه إلى الربط الوثيق بين الحق في السرية والحق في الخصوصية ولكنهم اختلفوا في وصف هذا الربط وطبيعة العلاقة، فنجد جانب منهم يذهب إلى إحلال الحق في السرية محل الحق في الخصوصية إذ أنهم يعتبرون أن الحق في الخصوصية أو الحق في احترام الحياة الخاصة هو ما يطلق عليه الحق في السرية، ولكل شخص الحق في المحافظة على سرية خصوصيات حياته وعدم جعلها عرضة لأن تلكوها. ألسنة الناس أو أن تكون موضوعا لصفحات الجرائد[2] ورغم تعرض الآراء الفقهية فيما يتعلق بتمييز السرية عن الخصوصية، إلا أن الرأي

[1] عصام أحمد البهجي، مرجع سابق، ص 105.

[2] عصام أحمد البهجي، المرجع نفسه، ص 105.

الغالب هو الثاني حيث أن السرية والخصوصية هما ليسا شيء واحد، وعلى هذا الأساس كانت هذه الدراسة شاملة لحماية المعلومات الالكترونية السرية، وقد يكون منها ما هو يتعلق بالحياة الخاصة للأفراد ومنها ما هو ليس كذلك.

فكل معلومة تمت معالجتها الكترونيا تتصف بالسرية سنعالج النصوص التجريمية التي جرمت سلوكيات انتهاكها كالدخول غير المشروع للنظام المعلوماتي ومشاركة صاحب المعلومة الاطلاع عليها من دون رضاه مثلا، أو الحصول على هذه المعلومة السرية بطريقة غير مشروعة والتعامل فيها بطريقة غير مشروعة أيضا، أو اعتراض رسالة

الكترونية بعث بها صاحبها إلى المرسل إليه وأعترض طرقها وأطلع عليها مع ما يمكن أن تحمله هذه الرسالة من أسرار خاصة، وغيرها من صور الاعتداءات التي تتعرض لها المعلومة السرية، وهو ما سيتم التفصيل فيها أدناه مع العلم أنه تم اعتبار مصطلح المعلومات السرية كمرادفة للبيانات التي تمت معالجتها الكترونيا.

إذن كل ما ورد أعلاه كان للتفرقة بين السرية والخصوصية بوجه عام، ولا ننسى أنه ظهر لنا ما يعرف بالخصوصية المعلوماتية وهي أحد الحقوق التي قد تنتهك سريتها بأحد الصور التي سيرد التفصيل فيها ولهذا رأينا أن نفصل فيها بعض الشيء مع ما يخدم الدراسة، باعتبار أن المعلومات فيها هي جزء من الكل من موضوع الدراسة.

المطلب الثالث: ماهية الخصوصية المعلوماتية

إنا خلو الإنسان إلى نفسه فكرة بأن يشعر بالهدوء والسكينة البعيدة عن أعين الناس أو مراقبة الفضوليين أو الاحتفاظ بأفكاره أو علاقاته الحميمة أو ارتباطاته وأفراد أسرته وراء ستار السرية، حاجة قديمة قدم وجود الإنسان نفسه.

لذا تحرص المجتمعات خاصة الديمقراطية منها على كفالة الخصوصية، وتعتبره حقا مستقلا قائما بذاته، ولا تكتفي بسن القوانين لحمايته بل تسعي إلى ترسيخه في الأذهان، وذلك بغرس القيم النبيلة التي تلعب دوراً كبيراً وفعالا في منع المتطفلين من التدخل في خصوصيات الآخرين وكشف أسرارهم.

ولقد حظي هذا الحق باهتمام كبير سواء من جانب الهيئات والمنظمات الدولية أومن جانب الدساتير والنظم القانونية.

فعلى الصعيد الدولي، نجد أن هذا الاهتمام يبرز في صورة اتفاقيات دولية كالإعلان العالمي لحقوق الإنسان الصادر من الجمعية العامة للأمم المتحدة[1] في المادة رقم 12 التي تنص على أنه " لا يتعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات."

ولقد تضاعف الاهتمام بهذا الحق نظرا لما يتعرض له من مخاطر تحيط به وتهدده أبرزها التقدم التكنولوجي والإعلامي والذي كان له دور كبير في اقتحام حصون هذا الحق واختراق حواجزه وتسلق أسواره، الأمر الذي يقتضي تدخل المشرع لحمايته بالأسلوب الذي يتفق وطبيعة هذه الأخطار.

أما على الصعيد المحلي أو الداخلي فإن الاهتمام بهذا الحق يبرز من خلال ما نصت، عليه في الدساتير والنظم السياسية للدول[2] كالدستور الجزائري[3] من خلال المواد[4] 46 و41 بالإضافة إلى ذلك نجد أن غالبية الدول ومن خلال تشريعاتها الوطنية قد أصبغت حمايتها الجزائية لهذا الحق، كالقانون الفرنسي في قانون العقوبات بموجب المواد

[1] ذلك بموجب قرارها رقم 217 المؤرخ في: 1948/12/10.

[2] كالنظام الأساسي لسلطنة عمان الصادر بالمرسوم السلطاني رقم 96/101 في المواد ،30،27،18 منه والمواد 57 ،45، من الدستور المصري، والمواد 7، 10، 15 من الدستور الأردني 1952 م، والمواد ،11، 29، 30، 31، 39 من الدستور الكويتي وغيرها.

[3] الدستور الجزائري لسنة 2016 بموجب القانون رقم 01/16 المؤرخ في 6 مارس 2016، جريدة رسمية رقم 14 مؤرخة في 7 مارس 2016.

[4] نصت المادة 40 على أن الدولة ضمن عدم انتهاك حرمة الإنسان كما يعاقب القانون بموجب المادة 41 من الدستور على المخالفات المرتكبة ضد الحقوق والحريات وعلى كل ما يمس بسلامة الإنسان البدنية أو المعنوية. مرجع سابق

226 -1، -226 2، 226-8 والمواد 309 مكرر[1] و309 مكرر(أ) من قانون العقوبات المصري[2]، والمادة 303 مكرر قانون العقوبات الجزائري[3] .كما أنه يمكن إقرار الحق في حرمة الحياة الخاصة من

خلال نص المادة 47 من القانون المدني الجزائري [4]

ولهذا الحق العديد من المفاهيم المنفصلة لكنها ترتبط معا في ذات الوقت وهي[5]:

1-خصوصية المعلومات والتي تتضمن القواعد التي تحكم جمع وإدارة البيانات الخاصة كمعلومات بطاقات الهوية والمعلومات المالية والسجلات الطبية والسجلات الحكومية وهي المحل الذي يتصل عادة بمفهوم حماية البيانات.

2-الخصوصية الجسدية أو المادية، والتي تتعلق بالحماية الجسدية للأفراد ضد أية إجراءات ماسة بالنواحي المادية لأجسادهم كفحوص الجينات، فحص المخدرات، الخصوصية الصحية.[6]

3- خصوصية الاتصالات والتي تغطي سرية وخصوصية المراسلات الهاتفية والبريد الالكتروني وغيرها من وسائل الاتصال والتحادث في البيئة الرقمية.

4-الخصوصية الإقليمية نسبة إلى الإقليم المكاني والتي تتعلق بالقواعد المنظمة للدخول إلى المنازل وبيئة العمل أو الأماكن العامة والتي تتضمن التفتيش والرقابة الالكترونية والتوثق من بطاقات الهوية.

---

[1] المادة 309مكرر و309 مكرر (ا)من قانون العقوبات المصري رقم (58) لسنة 1937.

[2] نفس مرجع سابق ق.ع. م.

[3] بالنسبة لقانون العقوبات الجزائري صدر تعديل بشأنه بموجب القانون 06/ 23 المؤرخ في 20 ديسمبر 2006 جريدة عدد 84 صادر بتاريخ 24 ديسمبر 2006 الذي عدل وتمم الأمر 156/66 المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات الجزائري.

[4] نصت المادة 47 من ق.م.ج.: " لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته، أن يطلب وقف هذا الاعتداء والتعويض عما يكون قد لحقه من ضرر".

[5] صليحة على صداقة، مرجع سابق، ص 175، يونس عرب، الخصوصية وحماية البيانات، بحث منشور على شبكة الإنترنت من خلال موقع www.arablaw.net، ص 12. ساعة 30-13، يوم 2020/07/08، مكتبة القانونية الشاملة.

[6] أدى التطور التكنولوجي إلى ظهور علم جديد هو علم إدارة وتقنية المعلومات الصحية أو نظام المعلوماتية الصحية حيث أنه علم يجمع بين علوم الحاسب الآلي من جهة وعلوم الطب والرعاية الصحية من جهة أخرى، أنظر صليحة على صداقة، مرجع سابق، ص 35.

فالخصوصية المعلوماتية مفهوم تولد من خلال المعالجة الآلية والتحليل للبيانات المتعلقة بالحياة الخاصة للأفراد ويدخل في نطاق هذه الدراسة كل أوجه التجريم المتعلقة بالجانب السري للخصوصية المعلوماتية باعتبار أن المعلومات الخاصة هي في الأصل من المعلومات الجديرة بالحماية الجزائية، وكان لزوما ادراج بعض التفصيل في مفهوم الخصوصية المعلوماتية، من خلال التطرق إلى تعريفها (فرع أول) ثم بعض صور الاعتداء عليها (فرع ثان) وسيتم التطرق للبعض منها في حدود ما يتعلق بالاعتداء على السرية فقط.

الفرع الأول: تعريف الخصوصية المعلوماتية

الخصوصية من الناحية اللغوية تعني حالة الخصوص، والخصوص نقيض العموم، يقال: اختص فلان بالأمر وتخصص له إذا انفرد به واختصه، والخصوص إذا الانفراد. ويقابله العموم، كما يفيد الحصر وضده لإطلاق[1]ويعبر عن الخصوصية في النظام القانوني اللاتيني بمصطلح الحياة الخاصة، ورغم كثرة تعريفات الخصوصية إلا أنها تعتبر في غالبيتها صدى لبعضها البعض[2]، فقد جاء في تعريف بأنها:" حق من طبيعة مادية يرتبط بالشخصية الإنسانية التي لها عليه سلطة تقديرية كاملة."

فهناك نوع من المعلومات يطلق عليها خاصة كونها تتعلق بالشخص ذاته وتنتمي إلى كيانه كإنسان مثل الاسم والعنوان ورقم الهاتف وغيرها من المعلومات، فهي معلومات تأخذ شكل بيانات تلزم الالتصاق بكل شخص طبيعي معرف أو قابل للتعريف[3] .

وهذه النوعية من المعلومات أصبحت في وقتنا الحاضر على درجة كبيرة من الأهمية في ظل فلسفة المعلوماتية المعاصرة، لاسيما وأن فكرة العالم الرقمي، لا يمكن لها السير في التطور ومواكبة اهتمامات الإنسان سوى باستخدام المعلومات، من هنا ظهر ما يعرف بالخصوصية المعلوماتية.

[1] أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دار النهضة العربية، الطبعة الأولى، القاهرة، مصر، 2010، ص 49، عن ابن منظور، لسان العرب، مطبعة بولاق، الجزء الثامن، الطبعة الأولى، القاهرة، مصر، ص 390. كتاب متوفر وموجود في لأنترنت

[2] أحمد محمود مصطفى، المرجع نفسه، ص 50.

[3] عمر أبوبكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة، مصر ،2004، ص 614.

ويعتبر مبدأ الخصوصية المعلوماتية الذي يقصد به حق الشخص في أن يتحكم بالمعلومات التي تخصه[1]. ويعود الفضل في توجيه الانتباه لمفهوم خصوصية المعلومات في هذه الفترة إلى مؤلفين أمريكيين هامين في هذا الحقل الأول كتاب الخصوصية والحرية لمؤلفه ويستن[2]، والثاني كتاب الاعتداء على الخصوصية لمؤلفه ميلر،[3] وكلاهما قدم مفهوما وتعريفا لخصوصية المعلومات.

فويستن ذهب في تعريفه للخصوصية المعلوماتية إلى أنها " حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للآخرين، في حين عرَف ميلر الحق في خصوصية المعلومات على أنها قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم[4].

وعرف البعض الخصوصية أيضا أنها:" حق احترام سرية وخصوصية الأشخاص من أي تدخل مادي أو معنوي، وهو حق عميق الجذور من الوجهة التاريخية"[5]. وعرفه البعض الآخر أنه " حق الإنسان في أن تحترم الحياة الخاصة به وأن تحفظ أسراره التي يجب ألا يطلع عليها الآخرون بغير إذنه، يتمثل في حماية حرمة المسكن وحرمة الاتصالات والمراسلات الخاصة بالإنسان[6] .

[1] محمد عبد المحسن المقاطع، نحو صياغة جديدة لمفهوم الحياة الخاصة للأفراد وضماناتها في مواجهة تهديدات الكمبيوتر، بحث مقدم لمؤتمر الكويت الأول للقانون والحاسب الآلي، كلية الحقوق، جامعة الكويت، الطبعة الأولى 1994، ص 174.

[2] يونس عرب دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي، ورقة عمل مقدمة إلى ندوة أخلاق المعلومات 17 أكتوبر 2002، عمان، الأردن، نادي المعلومات العربي 16.

[3] المرجع نفسه.

[4] طارق عفيفي صادق أحمد، الجرائم الالكترونية جرائم الهاتف المحمول، الطبعة الأولى، المركز القومي للإصدارات. القانونية، القاهرة، مصر، 2015، ص 149.

[5] طارق عفيفي صادق احمد، المرجع نفسه، ص 150.

[6] طارق عفيفي صادق احمد، مرجع سابق، ص 150.

الفرع الثاني: صور سلوكيات الاعتداء على الخصوصية المعلوماتية

صور واشكال الاعتداء على الأسرار المعلوماتية تكون بصفة عامة، وفيما يتعلق بتجريم تلك السلوكيات سيرد التفصيل فيها في الباب الثاني من هذه الدراسة وذلك لتفادي التكرار، لأن هذه الدراسة لا تعني الأسرار الخاصة بالإنسان فقط وإنما تعني الخصوصية الفردية والجماعية. وبالتالي فهي تخص كل المعلومات السرية الالكترونية أيا كانت الجهة التي تخصها هذه المعلومات، فالخصوصية المعلوماتية هي جزء من هذه الدراسة حيث أنها لا تعتبر هي السرية المعلوماتية، ذلك لأن هذه الدراسة موضوعها كل معلومة معالجة آليا قد تكون خاصة بالأفراد أو تكون خلاف ذلك، ولكنها لابد أن تتصف بالسرية. وتتمثل سلوكيات الاعتداء على الخصوصية الفردية في الآتي:

أولا: الاطلاع المجرد

في هذه الحالة الاطلاع يكون هو معلومات شخصية وخاصة يريد صاحبها إبقاءها سرية، وأما صورة هذا السلوك هو الاطلاع الكلي أو الجزئي على تلك الأسرار الخاصة بحيث يقوم اليقين بالعلم بها وفهمها، فإذا كانت الأسرار بلغة لا يفهمها الفاعل أولا يحسن تحليلها، لم يتحقق الاطلاع إلا بتكامل الصورة وترابط أجزائها. فإذا لم يكن ما أطلع عليه الفاعل سوى جزيئات غير مترابطة، غير ذات معنى مفيد لم يتحقق الاطلاع أيضا، وهذا الاطلاع يجب أن يكون في ذاته غير مشروع وأن يتم من شخص لا يملك قانونا ترخيصا بالولوج إلى تلك المعلومات، كما يشترط لتحقق هذه الصورة أن يكون الاطلاع مجردا أي أن. يكون قصد الفاعل هو الاطلاع فقط على تلك المعلومات السرية ومجرد العلم الشخصي بها[1] .

– ذلك كأن يقوم الشخص العالم بأوجه الدخول إلى أنظمة الغير بالتسلل إلى أنظمة الحاسب الآلي لشخص آخر وإعطائه الأوامر اللازمة بفتح ملفات الشخص المعتدى عليه والاطلاع عليها عن طريق المشاهدة على شاشة

[1] سهيل محمد العزام، الوجيز في جرائم الإنترنت، الطبعة الأولى، دائرة مكتبة الجامعة، الأردنية، 2009، ص 101، 102.

عرض جهازه هو، إن هذا الفعل يشكل خرق للسرية والخصوصية وذلك أن السر إنما جعل سرا لكونه يخفي ما لا يرغب الإنسان في إظهاره لعلة شخصية قد تتعلق بسلوك أو مصلحة إذا أفشت عادت بالضرر على صاحبها[1] .

ثانيا: الاطلاع بقصد الافشاء

الاطلاع في هذه الحالة على الأسرار الخاصة المخزنة في الحاسب مجردا وإنما لتحقيق غرض أو هدف معين وهو إفشاء تلك الأسرار.

يقوم بهذا السلوك إما الشخص المتاح له بحكم عمله الاطلاع على المعلومات والبيانات الخاصة السرية كموظف في مستشفى أو دائرة الأحوال المدنية أو محكمة، وهذا ما يسمى بإفشاء الأسرار المهنية هذا إذا كانت أسرارا خاصة في حين إذا كانت بيانات اسمية عموما لا تتصف بالسرية هنا نفرق بين سلوكي الاعتداء عليها أدناه فيما يتعلق بإفشاء الأسرار. ولا يفوتنا هنا أن نشير أن نصوص التجريم الحديثة لا تنطبق على هذه الحالة لأن جل القوانين تصدت لهته الجريمة بنصوص عقابية كافية وحددت من خلالها أركان الجريمة والتي لابد أن يكون الإفشاء من طرف موظف أو مستخدم بينما ما نقصده الآن وهو من يتوصل إلى تلك المعلومات السرية الالكترونية بخبرته ودرايته بأنظمة المعلومات لتحقيق اختراقات أو اتصالات بعدية أو مباشرة مع الحاسوب الموجودة به تلك الأسرار بحيث يتمكن من الاطلاع عليها وإفشائها.

ويمكن أن يشكل الحاسب الآلي وسيلة أكثر فعالية في نشر الأسرار بشمولية وتوسع كبيرين وبسرعة وكفاءة عاليتين، وذلك باستخدام قنوات الاتصال المتعددة التي تتيحها أنظمة الاتصالات المعلوماتية الحديثة، مع ظهور الانترنت بشكل خاص[2].

[1] محمد مصطفى الشقيري، مرجع سابق، ص 286.

[2] محمد مصطفى الشقيري المرجع نفسه، ص288

ثالثا: الابتزاز

يصبح التهديد بالاستغلال غير المشروع للأسرار الشخصية، حيث يستغل الفاعل ما يتحصل عليه من معلومات الكترونية سرية وذات علاقة بالحياة الشخصية للأفراد في تحقيق منافع مادية أو معنوية، وذلك بتهديد صاحب الأسرار بإفشائها أو فضح أمرها في حال عدم. تحقيق مطالبه، ولابد أن يكون لهذا الشخص القدرة على تنفيذ تهديداته[1].

رابعا: الاحتفاظ بنسخة

عند التوصل إلى المعلومات السرية الالكترونية بكل سهولة ونسخها بسرعة فائقة، والخطورة تكمن هنا في إمكانية استخدام تلك المعلومات السرية الخاصة في المستقبل لتحقيق أغراض غير مشروعة.

فكل أشكال الاعتداء الواقعة على سرية الخصوصية المعلوماتية ترتكب بطبيعة الحال بوسائل تقنية معلوماتية سهلت وبشكل كبير في ذلك الأمر الذي يتطلب دراسة مختصرة عن هاته الوسائل، والمتمثلة في عناصر النظم المعلوماتية.

المطلب الثاني: خصائص الجرائم المعلوماتية

إن ما نقصد به من ذاتية الجرائم المعلوماتية هو استقلاليتها وتميزها عن غيرها من الجرائم سيما التقليدية منها، وذلك بمجموعة من الخصائص أثرت بشكل مباشر على التشريعات العقابية والإجرائية التقليدية القائمة، وسوف نحاول أن نبرز أهم هذه الخصائص فيما يلي:

أولا: الجريمة المعلوماتية متعدية للحدود (عابرة للوطنية): إنه وبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال أسفر هذا الأمر إلى نتيجة مؤداها

[1] سهيل محمد العزام، مرجع سابق، ص 10.

أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد، حيث يمكن أن ترتكب الجريمة من مجرم في دولة على مجني عليه في دولة أخرى في وقت يسير جدا.

فالجريمة المعلوماتية بهذا الشكل لا تعترف بالحدود بين الدول وهي بذلك شكل جديد من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة،[1] ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمال الإجرامية التي يعمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، وهو ما يعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا، إذ أن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء، فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الحاسب الآلي الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصا آخر موجود في بلد ثالث،[2] أو القيام بإعداد أحد البرامج الخبيثة (Vérus) في بلد ما ثم يتم نسخ هذا .

البرنامج ويرسل إلى دول مختلفة من العالم.[3] وتظهر هذه المشكلة بصفة خاصة في التعاملات البنكية عبر شبكات المعلومات الدولية، حيث أدى التوسع الكبير لإجراء التعاملات البنكية عبر شبكات المعلومات الدولية

---

[1] خالد ممدوح ابراهيم. الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الأولى 2009، ص 88.

[2] نائلة محمد فريد قورة، جرائم ابغاسب الاقتصادية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 2003، ص 52.

[3] ومن الأمثلة عن القضايا التي لفتت النظر إلى البعد الدولي للجرائم المعلوماتية قضية عرفت باسم مرض نقص المناعة المكتسبة (الايدز). وتتلخص وقائعها أنه في عام 1989 قام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي يهدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة. إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (Vérus) يترتب على مجرد تشغيله تعطيل جهاز الحاسب الآلي عن العمل ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان إلكتروني ليتمكن المجني عليه من الحصول على مضاد للفيروس (Antivirus) وقد تم التمكن في 03 /02/ 1990 من إلقاء القبض على جوزيف بوب في الولايات المتحدة الأمريكية بولاية أوهايو وتقدمت المملكة المتحدة البريطانية بطلب تسليمه للمحاكمة أمام القضاء الانجليزي ذلك ان إرسال هذا البرنامج تم من داخل المملكة المتحدة وبالفعل وافق القضاء الامريكي على تسليم المتهم ووجهت له احدى عشر تهمة وقعت معظمها في دول مختلفة. وكانت لهذه القضية أهميتها من حيث أنه لأول مرة يتم فيها تسليم متهم في جريمة معلوماتية وأنها المرة الأولى أيضا التي يقدم فيها شخص للمحاكمة بتهمة إعداد برامج خبيثة (Vérus)، مشار إلى هذه القضية لدى نهلا عبد القادر المومني مرجع سابق، ص 51.

إلى إعطاء بعد دولي لهذه الجرائم ذلك أن ربط وسائل الاتصالات بالحاسبات الآلية ضاعف من المعاملات المالية الدولية والتي أصبحت تتم بواسطة وسائل إلكترونية، وبصفة خاصة من خلال التحويل الإلكتروني للأموال والتبادل الإلكتروني للمعلومات.

ومفاد ما سبق ذكره أن الجرائم المعلوماتية تتميز بالتباعد الجغرافي بين الفاعل والمجني عليه ومن الوجهة التقنية التباعد بين أداة الجريمة ومحلها، وهذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة أو خارجها ليطال دولة أخرى يتواجد فيها نظام الحاسوب المخزنة فيه المعلومات محل الاعتداء.

ولقد أثارت هذه الخاصية الدولية للجريمة المعلوماتية عدة إشكالات قانونية تتعلق أساسا بتحديد الدولة صاحبة الاختصاص القضائي[1] في محاكمة مرتكب هذه الجريمة، فهل هي الدولة التي وقع فيها النشاط الإجرامي أم التي أضيرت مصالحها نتيجة هذا التلاعب، بالإضافة إلى إشكالية مدى فعالية القوانين القائمة في التعامل مع الجريمة المعلوماتية، وبصفة خاصة مسألة جمع الأدلة وقبولها، إذ تتباين مواقف الدول فيما يتعلق بقبول الأدلة المستخلصة من أنظمة الحاسبات الآلية، وغيرها من المشاكل التي يمكن أن تثيرها الجرائم العابرة للوطنية بشكل عام.

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

ومن أجل ذلك فقد تعالت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لها بحزم،[2] وأن يشمل هذا التعاون تبادل المعلومات وتسليم المجرمين وضمان أن الأدلة التي يتم جمعها في دولة تقبل بمحاكم دولة

[1] تجدر الإشارة في هذا المجال إلى قضية (R.V Thompso) والتي تتلخص وقائعها في قيام مبرمج إنجليزي يعمل بأحد البنوك في دولة الكويت بالتلاعب بنظام الحاسب الآلي الخاص بالبنك ليقوم بإجراء خصومات من أرصدة العملاء ثم يقوم بإيداعها في الحساب الخاص به وبعد أن رجع المتهم إلى انجلترا قام بالكتابة إلى البنك طالبا منه أن يقوم بتحويل الحساب الخاص به إلى عدة حسابات بنكية في إنجلترا وهو ما قام به البنك فعلا، وقدم للمحاكمة أمام القضاء الانجليزي إلا أنه طعن في الحكم استنادا إلى عدم اختصاص القضاء الانجليزي بما أن فعلي السحب والايداع كانا في الكويت وليس بانجلترا.مشار إلى هذه القضية لدى نائلة عادل محمد فريد قورة، مرجع سابق، ص 54.

[2] نظر في هذا المثال مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاقبة المجرمين المنعقد في هافانا عام 1990.قرار بشأن الجرائم ذات صلة بالكمبيوتر والتوصيات لجنة الوزراء الأوربي في إطار معالجة المشكلات الخاصة بالجرائم المعلوماتية، لتفاصيل أكثر انظر رامي المتولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات مقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، القاهرة، الطبعة الأولى ,2011، ص64 وما بعدها.

أخرى. ولكن ومع ضرورة هذا التعاون والمناداة به إلا أنه تقف أمام هذا المبدأ عقبات ومعوقات تحول دون تحققه وتجعله صعب المنال، من أهمها انعدام نموذج موحد للنشاط الإجرامي المكون للجريمة المعلوماتية، وأن كثيرا من القوانين لم يتم تعديلها بحيث تتلاءم مع هذه الجرائم حتى يتسنى إدراجها ضمن الاتفاقيات الدولية الخاصة بتبادل المساعدة الجنائية في مجال الجرائم المعلوماتية، بالإضافة إلى تنوع واختلاف النظم القانونية والإجرائية[1].

ثانيا: صعوبة اكتشاف الجريمة المعلوماتية وإثباتها: تقع الجريمة المعلوماتية في بيئة افتراضية تقنية لا تترك أية آثار محسوسة، إذ يغلب عليها أنها تتم في الخفاء لأن الجناة يعمدون في كثير من الأحيان إلى إخفاء نشاطهم الجرمي عن طريق تلاعبهم بالبيانات، والذي يتحقق أحيانا إن لم نقل في الغالب في غفلة من المجني عليهم.

كما أنه من السهل عليهم تدمير الأدلة ومحوها مما يعقد أمر كشف الجريمة وإثباتها، وإذا ما قورنت حالات اكتشاف الجريمة المعلوماتية على ضوء ما يتم اكتشافه من الجرائم التقليدية فإن عددها قليل، فمعظم الجرائم المعلوماتية تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابه، ذلك أن هذا النمط الإجرامي لا يحتاج إلى عنف أو جثث أو اقتحام إنما هي معلومات وبيانات تغير أو تعدل أو تمحى كليا أو جزئيا من السجلات المخزونة في ذاكرة الحاسب الآلي [2]فلا تترك أثرا خارجيا مرئيا أو ملموسا فهي كما وصفها بعض الفقهاء بأنها جريمة هادئة بطبيعتها لا تتطلب سوى عدد من اللمسات الخاطفة على لوحة المفاتيح حتى تؤدي إلى اختراق المعلومات المخزنة في الحاسب الآلي وهتك سريتها ومحوها أو تشويهها أو تعطيل الأنظمة التي تحتويها.

استدلال بأقوالهم ولا أدلة مادية يمكن فحصها وإنما تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بواسطة نبضات إلكترونية غير مرئية.

فالجريمة المعلوماتية من الجرائم المستحدثة التي لا تترك شهودا يمكن كما ذهب البعض للقول بأن صعوبة اكتشاف الجريمة المعلوماتية وكذا صعوبة إثباتها راجع أيضا إلى عدة أسباب، من بينها وسيلة تنفيذها والتي تتسم

[1] د. نهلا عبد القادر المومنى – مرجع سابق –50 , 51 ,53
[2] خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، دار الفكر الجامعي، الطبعة الأولي، الإسكندرية، مصر، 2008، ص 45-46

في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، إذ أنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات وذلك سواء لارتكابها أو التحقيق فيها أو لملاحقة مرتكبيها. فأحيانا نجد رجال الضبطية القضائية غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذا النوع من الجرائم. بالإضافة إلى صعوبة الاحتفاظ الفني بدليل الجريمة المعلوماتية، إذ للمجرم المعلوماتي القدرة على تدمير الدليل في أقل من ثانية[1].

ويمكن اعتبار أنه من بين الأسباب أيضا التي تقف وراء صعوبة اكتشاف الجريمة المعلوماتية وإثباتها المجني عليهم أنفسهم، ذلك أن هؤلاء قد يلعبون دورا رئيسيا في ذلك من خلال الإحجام عن الإبلاغ عنها في حالة اكتشافها، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو تمنى بخسائر فادحة من جراء ذلك عن عدم الكشف حتى بين موظفيها عما تعرضت له وتكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهزا للثقة في كفاءتها.[2] ويبدو ذلك أكثر وضوحا في المؤسسات المالية مثل البنوك والمؤسسات الادخارية ومؤسسات الإقراض. حيث تخشى مجالس إدارتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها، حيث أن الجانب الأكبر من الجرائم المعلوماتية لا يتم الكشف أو التبليغ عنه، وهو ما يؤثر سلبا على السياسة التي يمكن أن توضع لمكافحتها.[3]

وقد تم طرح عدة اقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم وبالتالي إنقاص حجم الإجرام المعلوماتي الخفي، ومن هذه الاقتراحات التي طرحت لحمل المجني عليه على التعاون مع السلطات في الولايات

[1] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة الطبعة الأولى، 1994، ص 16.

[2] أشارت بعض التقديرات في الولايات المتحدة الأمريكية، أن ما يتراوح بين 20 و25 % من جرائم الحاسبات لا يتم الإبلاغ عنها خشية الإساءة إلى السمعة وفي دراسة أجريت على ألف شركة من الشركات المنتجة لجهاز(Fortune) أظهرت نتائجها أن 2% فقط من كل جرائم المعلوماتية التي يتم التبليغ عنها للشرطة أو لمكتب التحقيقات الفدرالي، مشار إليه لدى رشيدة بوكر، مرجع سابق، ص 472.

[3] نهلا عبد القادر المومني، مرجع السابق، ص 55.

المتحدة الأمريكية مطالبة البعض بأن تفرض النصوص المتعلقة بجرائم المعلوماتية على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يصل علمهم به من جرائم في هذا المجال مع تقرير جزاء على الإخلال بهذا الالتزام. وعرض ذات الاقتراح على لجنة خبراء مجلس أوروبا ولاقت الفكرة رفضا باعتبار أنه ليس مقبولا تحويل المجني عليه إلى مرتكب الجريمة[1] .

المطلب الثالث: أساليب الجريمة المعلوماتية

إنه وعلى خلاف الجرائم التقليدية التي تتطلب بطبيعتها نوعا من المجهود العضلي الذي قد يتخذ شكل العنف والإيذاء كما هو الحال في جريمة القتل مثلا، فان الجرائم المعلوماتية تعد بطبيعتها جرائم هادئة لا تتطلب سوى عدد من اللمسات الخاطفة على أجهزة الحاسوب حتى تؤدي إلى اختراق أكبر نظم المعالجة الآلية وهتك سريتها أو محو ما تحتويه من معلومات أو تعطيل برامجها، على اعتبار أن الجريمة المعلوماتية إنما تتم في صورة أوامر تصدر إلى جهاز الحاسوب ولا يحتاج مرتكبوها إلى القدرة والدراية في التعامل مع نظم المعالجة الآلية والإلمام بالمهارات والمعارف التقنية. فالمجرم المعلوماتي يستهدف محلا ذا طبيعة متميزة ونعني بذلك المعلومات التي تحتويها هذه النظم المعلوماتية، أي تلك الإشارات أو النبضات الإلكترونية غير المرئية التي تنساب عبر أجزاء نظم المعالجة الآلية وشبكات الاتصال العالمية[2] .

وتبعا لذلك فإنه كلما كان للمجرم المعلوماتي خبرة ومهارة عالية في مجال المعلوماتية واستخدام شبكات الحاسب الآلي كلما زادت خطورته الإجرامية وتعاظمت لديه الدوافع والأهداف في ارتكاب الجريمة المعلوماتية.[3]

أولا: أساليب وتقنيات ارتكاب الجريمة المعلوماتية

تتشابه جرائم المعلوماتية مع الجرائم التقليدية من حيث استخدام المجرم لوسائل وأساليب غير مشروعة في سبيل ارتكابه لجريمته، ومع ذلك فإن جرائم المعلوماتية تتميز بارتكابها من طرف مجرمين يستعملون كل ما من شأنه

[1] د. نائلة عادل محمد فريد – مرجع سابق – ص 58
[2] د. نائلة عادل محمد فريد – مرجع سابق – ص 63
[3] نهلا عبد القادر المومني، مرجع سابق، ص 125.

خداع الحاسب الآلي والتحايل على أنظمته المعلوماتية، وتتنوع أساليب ارتكاب الجريمة المعلوماتية التي يستعمل من خلالها المجرمون تقنيات مختلفة لتنفيذ جرائمهم وحتى وإن أمكن حصرها في الوضع الراهن إلا انه لا يمكن التنبؤ بالوسائل الفنية والتقنية التي قد تستحدث في مجال تكنولوجيا المعلومات، [1]ولعل من أهم هذه التقنيات هي الاختراق واستعمال البرامج الخبيثة[2] (Vérus) وسوف نحاول شرح ذلك فيما يلي:

ثانيا: الاختراق :«**Haking**» :تقوم معظم جرائم المعلوماتية على تقنية الاختراق وذلك بغرض الدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات، والاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف أو الوصول إلى البيانات الموجودة على الأجهزة الشخصية بوسائل غير مشروع [3].

ويحتاج التسلل إلى جهاز الضحية دون علمه إلى مجموعة من الأدوات والوسائل، فقد يتم الاختراق عن طريق استعمال نظم التشغيل لكونها مليئة بالثغرات من خلال البروتوكولات التي يستخدمها نظام التعامل مع شبكة الإنترانت، فيقوم المخترق بالبحث عن ضحية من خلال معرفة رقم(IP) الخاص به. ويتم البحث عن هذا الرقم بمجموعة من الخطوات يقوم بها المخترق على جهازه الذي يشترط أن يكون متصلا بجهاز الضحية عبر شبكة الأنترنت وفي نفس اللحظة، لأن هذا الرقم يتغير مع كل اتصال جديد.

---

[1] محمد خليفة، مرجع سابق، ص 40.

[2] طبقا لمؤتمر سام للاختراق فإن للاختراق 06 مستويات بحسب درجة الخطورة:

– المستوى الأول : يعرف بهجوم قنبلة صندوق البريد ويؤدي إلى إعاقة النظام عن تقديم الخدمة.

– المستوى الثاني : الدخول غير مرخص به لنظام المعلومات والحسابات بما يتيح قراءة الملفات أو نسخها للمخترق غير مرخص له.

– المستوى الثالث : يتمكن المخترق فيه من الدخول إلى مواقع غير مرخص له بالدخول إليها.

– المستوى الرابع : يتمكن المخترق فيه من قراءة ملفات سرية.

– المستوى الخامس : يتمكن المخترق من نقل ونسخ الملفات السرية

– المستوى السادس : يتمكن المخترق من إيجاد قناة مفتوحة للدخول إلى سائر أرجاء النظام والعبث بمحتويات، نقلا عن سعيداني نعيم .مذكرة ماستر اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري جامعة باتنة،ص56.

[3] يتطلب تشغيل نظم الاتصالات الكمبيوترية أن تكون هناك آلية من أجل عنونة الأجهزة سواء المرسلة أو المستقبلة، كما (Address IP تتطلب أيضا أن تكون هناك آلية لضمان وصول أو التحقق من وصول الاتصال أو الرسالة للجهة المقصودة والتحقق من جهة الإرسال (IP Internet protocol) ويستخدم في تحقيق هذه الغاية بروتوكول الأنترنات.

وقد يتم الاختراق باستخدام البرامج،[1] ويشترط في هذه الطريقة وجود برنامجين أحدهما بجهاز الضحية ويسمى بالبرنامج الخادم لأنه يأتمر بأوامر المخترق وينفذ المهام الموكلة إليه داخل جهاز الضحية وبرنامج آخر يوجد بجهاز المخترق ويسمى بالبرنامج المستفيد، وأخطر هذه البرامج برنامج "حصان طروادة"،[2] وتتجلى خطورته لتميزه بالقدرة على الاختراق دون إمكانية كشفه وتتبعه والقضاء عليه واحتلال هذا البرنامج مكانا داخل النظام المخترق حتى ولو قام الضحية بحذفه فلا فائدة من ذلك، كما أنه يكفي أن يعمل البرنامج هذا لمرة واحدة فقط حتى يقوم بمهامه، ويمكن إرساله للضحية عن طريق رسائل إلكترونية أو عن طريق استخدام برامج الدردشة.

كما قد يتم اللجوء في عملية الاختراق إلى أسلوب التفتيش في مخلفات التقنية وذلك بالبحث في مخلفات الحواسيب من القمامات والمواد المتروكة على مستوى الجهاز عن أي شيء يساعد على اختراق النظام، كالبرامج المدون عليها كلمة السر أو مخرجات الكمبيوتر التي قد تتضمن معلومات مفيدة،[3] ومن خلال الأساليب أيضا في عملية الاختراق أسلوب المحاكات وذلك عن طريق التخفي بانتحال شخصية وصلاحيات شخص مفوض ومسموح له بالدخول إلى نظم المعلوماتية عن طريق استخدام وسائل التعريف الخاصة به، وفيها يتم إعطاء حزم عناوين (IP) شكلا معينا لتبدو وأنها صادرة من جهاز حاسوب مسموح له بالدخول إلى تلك الأجهزة.

كما يوجد أسلوب آخر للاختراق وهو انتحال شخصية الموقع، ويعتبر هذا الأسلوب حديثا نسبيا في مجال الجرائم المعلوماتية، ويقوم هذا الأسلوب على قيام المخترق بوضع نفسه في موقع بيني بين البرنامج المستعرض

---

[1] وكلاهما يندرجان تحت اسم SERVER.EXE والثاني (Client.exe معظم برامج الاختراق تستخدم نوعين من الملفات الأول يسمى من الدخول إلى الحاسب من خلال Client على فتح ثغرة في الحاسب المستهدف ليمكن ملف SERVER حيث يعمل ملفTROJAN كل برنامج اختراق يعتمد على رقم منفذ خاص به يمكن المخترق من إدخال عنوان الحاسب المستهدف PORT هذه الثغرة. والمقصود بالثغرة ويرسل ملف الاختراق إلى الحاسب المستهدف بواسطة الطرق التالية"L'addressr IP" :

إنزال البرامج من الموقع غير الموثوق به. – (ICQ) برامج الدردشة –MAIL–E –رسائل البريد الالكتروني

[2] صمم برنامج حصان طروادة في البداية لغرض حسن ومفيد وهو معرفة ما يقوم به الأبناء على جهاز الكمبيوتر في غياب الوالدين أو معرفة ما يقوم به الموظفون على جهاز الكمبيوتر في غياب المدراء إلا أنه تطور هذا البرنامج بحيث أصبح يمكن المخترق من الحصول على كلمة السر الخاصة بالدخول إلى الجهاز والتي يستخدمها صاحب الجهاز نفسه فلا يمكن لصاحب الجهاز ملاحظة وجود دخيل.

[3] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، مرجع سابق، ص 21.

للحاسب الخاص بأحد مستخدمي الأنترانت وبين الموقع (WEB) ومن هذا الموقع البيني يستطيع المجرم المعلوماتي من خلال جهاز حاسوبه مراقبة أي معلومة متبادلة بين الضحية الذي يزور الموقع وبين الموقع نفسه، كما له أن يقوم بسرقة هذه المعلومات أو تغييرها.

وكل ما يحتاجه من يقوم بهذه العملية هو السيطرة على أحد المواقع التي تتم زيارتها بكثرة وتحويله ليعمل كموقع بيني ثم يقوم المخترق بتركيب البرنامج الخاص به هناك، وبمجرد أن يكتب مستخدم الإنترانت اسم هذا الموقع فإنه يدخل في الموقع المشبوه الذي أعده المخترق.

ثالثا: البرامج الخبيثة« Les Vérus » : تعد الفيروسات بمثابة المرض المعدي الذي يصيب المعطيات فيقضي عليها أو يشوهها فتذهب في كلتا الحالتين بفائدتها، وفيروس الحاسب الآلي يشبه إلى حد كبير الفيروس الذي يصيب الإنسان لقدرته على الانتقال من حاسب إلى آخر[1].والفيروس في مجال المعلوماتية هو برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي يصمم بشكل يجعل منه قادرا على التكاثر ونسخ نفسه إلى نسخ كثيرة والانتشار من نظام لآخر عبر شبكات الاتصال والقدرة على الاختفاء داخل برنامج سليم بحيث يصعب اكتشافه، كما أنه قد يكون مصمما لتدمير برامج أخرى أو تغيير معلومات ثم يقوم بتدمير نفسه ذاتيا دون أن يترك أي أثر يدل عليه.

ويمكن أن يصاب الحاسب الآلي بالفيروس عند تشغيل الجهاز بواسطة أسطوانة مرنة مصابة وكذا عند نسخ برنامج أو تحميل ملفات أو برامج من الإنترانت، وكذلك عند تبادل البريد الإلكتروني المحتوي على الفيروسات.

وتتمتع الفيروسات بقدرة فائقة على مهاجمة أجهزة الحاسوب والشبكات المعلوماتية وتعطيل الاتصالات وتشويه البيانات وأحيانا تضلل المستخدم ببيانات خاطئة. ويستخدم الفيروس بشكل عام لتحقيق أحد الغرضين:

[1] محمد خليفة، مرجع السابق، ص50.

–الغرض الحمائي : ويكون ذلك لحماية النسخة الأصلية من خطر النسخ غير المرخص به فينشط الفيروس بمجرد النسخ ويدمر نظام الحاسوب الذي يعمل عليه ويعد ذلك بمثابة عقوبة تلحق بالناسخ.

–الغرض التخريبي : ويتم إعداد هذه الفيروسات من طرف خبراء البرامج يهدف التخريب بحد ذاته أو إلى التخريب يهدف الحصول على منافع شخصي.[1]

ومن الآثار التي يخلفها الفيروس والتي تختلف بحسب نوعه:

- البطء الشديد في الحاسب بما يجعل التعامل معه مستحيلا.
- عدم القدرة على تشغيل معظم التطبيقات وظهور رسالة خطأ كلما تمت محاولة تشغيلها.
- مسح الملفات التنفيذية وكذا حذف جميع المعطيات الموجودة داخل القرص الصلب.

أما عن أنواع الفيروسات فهي كثيرة جدا ولا يمكن حصرها، إذ أنها آخذة في التزايد بشكل متسارع وأهمها: الفيروسات المقيمة، الفيروسات النائمة، الفيروسات الاستعراضية، فيروسات الثغرات...

المبحث الثاني: تصنيف الجرائم الواقعة على اسرار المعلوماتية.

إن الانتشار الواسع و المتزايد لتطبيقات نظم المعالجة الآلية واعتمادها على التعاملات بشتى أنواعها بالإضافة إلى ازدياد عدد زبائن ومستخدمي التطبيقات الإلكترونية المعتمدة على نظم المعالجة الآلية، أدى إلى تضخم المصالح المرتبطة بها وبالمعلومات التي تقوم بتخزينها، إلا أن هذا الدور تم استغلاله في أغراض غير مشروعة، فأصبح هذا النظام ومعلوماته محلا للعديد من الاعتداءات التي تمس بسرية وسلامة المعلومات الإلكترونية، و التي ترتكب من قبل أشخاص لديهم من المهارات والمعرفة والقدرة ما يجعلهم يمثلون تهديدا حقيقيا على المجتمع [2]، ومن بين هذه الاعتداءات التي أعطيت وصفا جرميا: الدخول أو البقاء غير مصرح بهما الذي سنعرضه في المطلب

[1] سامي الشوا، مرجع سابق، ص 190.

[2] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات حلبي، الحقوقية: لبنان، 2012، ص 151.

الأول، والاعتراض غير القانوني في المطلب الثاني.

المطلب الاول: جريمة الدخول أو البقاء غير المصرح بهما على نظام معالجة آلي يتضمن أسرار معلوماتية.

ان ظاهرة انتشار وتطور لاتصالات وتنامي الشبكات المعلوماتية ادى إلى اختراق النظام المعلوماتي من قبل أفراد غير مصرح لهم بالدخول إليه والبقاء فيه، حيث ان البعض يصنف هذه الجريمة من باب الجرائم المعلوماتية المرتكبة بواسطة النظام المعلوماتي[1]، أما البعض الآخر يطلق عليها جرائم الاعتداء على نظم المعالجة الآلية للبيانات أو جرائم السلوك المجرد المتصلة بنظام المعالجة الآلية للمعلومات.[2]

وعلى رغم من أن الدخول أو البقاء غير المصرح بهما إلى النظام المعلوماتي يعد مرحلة سابقة وضرورية لارتكاب الجرائم المعلوماتية الأخرى مثل سرقة المعلومات وتزويرها أو التجسس المعلوماتي أو جريمة الاحتيال المعلوماتي إلى غير ذلك من الجرائم، إلا أن مرتكب هذا السلوك قد يقصده بحد ذاته دون أن يهدف إلى ارتكاب جريمة أخرى من ورائه، وهذه الحالة أثارت جدلا فقهيا حول مدى انطباق وصف الجريمة المعلوماتية عليها وبالتالي إذا كانت تستوجب الحماية أم لا؟

الاتجاه الأول: هذا الاتجاه يعارض او بأحرى ينفي تجريم الدخول أو البقاء غير المصرح بهما إلى النظام المعلوماتي، خاصة إذا لم تكن لدى الفاعل نية لارتكاب جريمة لاحقة لهذا الدخول أو البقاء، ويبرر هذا الاتجاه رأيه أن هذا السلوك لا يخرج عن كونه طريقة لعرض القدرات التقنية والذهنية التي يتمتع بها الشخص الذي قام بهذا الفعل، وهذا الفعل لا يشكل جريمة تستدعي العقاب.[3]

[1] رشيدة بوكر، مرجع سابق، ص151.

[2] نهلا عبد القادر المومني، مرجع سابق، ص 156.

[3] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الكتب القانونية، القاهرة، مصر، 2002، ص 235.

الاتجاه الثاني: يذهب هذا الاتجاه إلى تجريم الدخول أو البقاء غير المصرح بهما إلى النظام المعلوماتي حتى لو لم يكن يقصد ارتكاب جريمة لاحقة فيما بعد، كما يبرر الاتجاه رأيه بالإشارة إلى أن هناك خسائر مادية تترتب على حالات الدخول غير المصرح به للنظام المعلوماتي قد تكون هذه الخسائر نتيجة محاولة وقف هذا الدخول، وبهذا الصدد يمكن الإشارة إلى الخسائر التي تحملها إحدى المعامل الخاصة بتصنيع الأسلحة النووية في كاليفورنيا في الولايات المتحدة الأمريكية التي قدرت حوالي مائة ألف دولار أمريكي، وهي تكلفة الأبحاث التي أجريت لمحاولة وقف الدخول غير المصرح به الذي قام به أحد الأشخاص إلى نظام الحاسوب الخاص بهذا المعمل .[1]

والأجدر هو الأخذ بما جاء به الاتجاه الثاني الداعي إلى تجريم هذا السلوك بحد ذاته، كونه يعد مرحلة أساسية لارتكاب بقية الجرائم المعلوماتية الأخرى.[2]

هذه الجريمة تفترض وجود عنصر نظام المعالجة الآلية للمعطيات، بحيث إذا لم يتوافر هذا العنصر فلا يمكن البحث في مدى توافر الأركان الأخرى للجريمة، وهل يشترط لتحقق جرائم الاعتداء على نظام المعالجة الآلية أن يكون مزودا بوسائل للحماية.

الفرع الأول: الركن المفترض.

جرم المشرع الجزائري بعد صدور القانون رقم 15/04[3] بعض الاعتداءات التي يكون محلها نظام المعالجة الآلية للمعطيات أو ما يسمى بالنظام المعلوماتي وهي التي نخصها بالدراسة، وكل هذه الجرائم و إن اختلفت في أركانها وعقوبتها إلا أن ما يجمعها هو أنها تحقق حماية جنائية لنظم المعالجة الآلية للمعطيات، أي أن القاسم المشترك بينها هو" النظام المعلوماتي"[4] ويعتبر هذا النظام شرط أولي أو لازم، بحيث يلزم تحققه حتى يمكن توافر الأركان

[1] نائلة عادل محمد فريد قورة، مرجع سابق، ص 323.

[2] نهلا عبد القادر المومني، مرجع سابق، ص 157.

[3] القانون رقم 15/04 المؤرخ في: 10 /11/ 2004 المتضمن ق. ع. ج. م. م.للأمر 66 /156 الصادر في الجريدة الرسمية للجمهورية الجزائرية، المؤرخ في 8 جوان 1966.

[4] نهلا عبد القادر القهوجي، مرجع سابق، ص 25.

الأخرى للجريمة، وعليه قبل دراسة هذه الجرائم يجب أولا توضيح المقصود بهذا النظام، ثم البحث فيما إذا كان يشترط في هذا النظام أن يتمتع بالحماية الفنية حتى يحظى بحماية قانون العقوبات أم لا ؟

أولا: نظام المعالجة الآلية للمعطيات.

تبنى المشرع الجزائري للدلالة على الجريمة المعلوماتية مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة المعلوماتية، وهذه المكونات لا تظهر في حالة واحدة إذ قد تكون مخزنة به أو منقولة منه أو عليه وهو ما يتوجب علينا التطرق لدراسة المقصود بنظام المعالجة الآلية للمعطيات.

– المقصود بنظام المعالجة الآلية للمعطيات: عند تعديل المشرع الجزائري لقانون العقوبات و إضافته للقسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات عارضا من خلاله صور هذه المعطيات لم يعرف نظام المعالجة الآلية للمعطيات بل ترك مهمة تعريفه للفقه فعرفه مجلس الشيوخ الفرنسي بأنه: " كل مجموعة مركبة من وحدة أو عدة وحدات للمعالجة وسواء كانت متمثلة في ذاكرات الحاسب وبرامجه ووحدات الإدخال والإخراج التي تساهم في نتيجة معينة[1] .

هذا التعريف يتضمن نظام المعالجة الآلية بمكوناته المادية كالمعدات والأجهزة، والمعنوية كالمعلومات والبرامج، وأن توجد بين هذه العناصر علاقة تربط بينهما لتحقق هدف معين وهو المعالجة الآلية للبيانات.

ويعرف أيضا على أنه: " مجموعة الوحدات المترابطة التي تألفت معا لتشكل كلا لا يتجزأ وليعمل معا كوحدة واحدة ". فهو نظام وظائف الإدخال والمعالجة والإخراج والتخزين والرقابة التي تحول البيانات إلى معلومات مفيدة باستخدام الأجهزة و البرامج الجاهزة [2].

[1] سامي منصور، الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية، دون طبعة، المنشورات الحقوقية صادر، لبنان، 2006. ص 32.

[2] سامي منصور، مرجع سابق، ص 33.

و يشير مجلس الشيوخ الفرنسي إلى أن النظام لا بد أن يكون محميا بجهاز للأمان وأن الأنظمة المحمية هي فقط التي تخصها الحماية الجنائية[1]، إلا أن هذا التعريف حذف من النص النهائي ومع ذلك يمكن للقضاء أن يعتمد عليه فيما يعرض أمامه من منازعات في هذا الخصوص حيث يعتبر هذا للقضاء التعريف من الأعمال التحضيرية التي يمكن الاستعانة به .[2]

ومن خلال هذه التعاريف التي تم ذكرها نستنتج أن مصطلح نظام المعالجة الآلية يستخدم في الحقل القانوني للدلالة على المعنى المقصود نفسه وفقا لمفهومه العلمي.

ثانيا: مدى اشتراط الحماية الفنية لنظام المعالجة الآلية.

احتدم الجدال في الفقه الفرنسي حول وجوب توافر هذا الشرط أو عدمه و سبب إثارة هذا الخلاف أن الأعمال التحضيرية للقانون أكدت على وجوب أن يكون النظام محميا ضد الاعتداءات عليه بأجهزة أو وسائل أمنية، وهذا ما تمسك به مجلس الشيوخ الفرنسي وحجته في ذلك جذب انتباه أصحاب الأنظمة إلى هذه النقطة الأساسية كي يدعموا أنظمتهم بأجهزة الأمن، في حين جاءت النصوص القانونية خالية من تطلب هذا الشرط فكان الرأي الراجح في الفقه الفرنسي انسجاما مع النص عدم اشتراط وجود نظام حماية لنظم المعالجة الآلية، وقد قضي تطبيقا لذلك أنه لا يشترط لتحقيق الجريمة أن يكون الدخول إلى النظام مقيد بوجود حماية فنية، ولكن إذا نظرنا إلى الواقع نلاحظ أن غالبية أنظمة المعالجة تتمتع بنظام الحماية الفنية فضلا عن أن وجود مثل تلك الحماية تساعد على اثبات أركان الجريمة ولاسيما الركن المعنوي.[3]

[1] محمد خليفة، مرجع سابق، ص 27 ،28.

[2] عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، الإسكندرية، مصر، 1999، ص 26.

[3] الامانة العلمية مذكرة ماستر الحماية الجنائية لسرية المعلومات الالكترونية جامعة ام البواقي ص من 49 الى 52

الفرع الثاني: صورتي جريمة الدخول أو البقاء غير المصرح بهما.

نصت المادة 394 مكرر من القانون رقم 15/04 السابق الذكر على أنه: " يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 10.0000 دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة "(6) أشهر إلى سنتين (2) و الغرامة من 50.000 دج إلى 150.000 دج .[1]

وتقابله المادة 1/323من قانون العقوبات الفرنسي والتي تنص على: " عقوبة فعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات هي الحبس لمدة سنتين وبغرامة 30.000 أورو.

أما إذا نتج عن فعل الدخول أو البقاء محو أو تغيير في المعطيات الموجودة داخل النظام أو تعييب تشغيل النظام فالعقوبة تشدد و تصبح الحبس لمدة ثلاثة سنوات و الغرامة 45.000 أورو[2] .

و قد حثت اتفاقية بودابست على ضرورة تبني القوانين الداخلية لهذا النوع الإجرامي من خلال المادة الثانية منها تحت عنوان " الدخول غير القانوني " التي نصت على أنه: " يجب على كل طرف أن يتبنى الإجراءات التشريعية و أي إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية وفقا لقانونه الداخلي، الولوج العمدي لكل أو لجزء من جهاز الحاسب دون حق كما يمكن له أن يشترط أن ترتكب الجريمة من خلال انتهاك

[1] انظر المادة 394 مكرر من القانون رقم 15/04 المؤرخ في 10 /11/ 2004 المتضمن قانون العقوبات الجزائري المعدل والمتمم للأمر 156/66 المؤرخ في: 8 جوان 1966.

[2] 2Art 323-1 le fait d'accéder ou de maintenir، frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni «deux ans [ancienne rédaction ;d'un an]» d'emprisonnement et de «30.000 € [ancienne rédaction; 15.000 euros]» d'amende.

إجراءات الأمن، بنية الحصول على بيانات الحاسب أو بنية " إجرامية أخرى، أو أن ترتكب الجريمة في حاسب آلي يكون متصلا عن بعد بحاسب آخر .[1]

يستخلص من خلال المادة 394 مكرر من القانون 04/ 15 والمادة 323 /1 من قانون العقوبات الفرنسي أن لهذه الجريمة صورتين سنعرضهما كالآتي:

أولا: جريمة الدخول والبقاء غير المصرح بهما في صورتها البسيطة.

من خلال الفقرة الأولى من المادة 394 مكرر من قانون 15/04 نستخلص أن جريمة الدخول أو البقاء غير المصرح بهما لا تقوم إلا بسلوكي الدخول أو البقاء سواء في صورتها البسيطة أو المشددة، وهذا هو الركن المادي.

1/ الركن المادي: الركن المادي لهذه الجريمة نوعان قد يكون إيجابيا أو سلبيا، فالأول يتمثل في فعل الدخول والثاني في الامتناع عن الخروج من نظام المعالجة الآلية للمعطيات أو البقاء فيه في الوقت الذي كان من المفروض عليه المغادرة،[2] وعليه ما المقصود بكل من فعل الدخول والبقاء؟

أ–فعل الدخول: نعني به الولوج غير المصرح به إلى النظام المعلوماتي باستخدام الحاسوب بحيث يتحقق الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات بمجرد الوصول إلى المعلومات المخزنة داخل النظام المعلوماتي ودون رضا صاحب هذا النظام.[3]

فالركن المادي لهذه الجريمة يتحقق بفعل الدخول الكلي أو الجزئي بإحدى الوسائل الفنية أو التقنية في إحدى أنظمة المعالجة الآلية إلا أن المشرع لم يحدد الوسائل التي يتم عن طريقها الدخول إلى النظام، ويكون الدخول غير المصرح به متى كان الجاني لا يحق له هذا الدخول لسبب من الأسباب، وعلى ذلك فإن مفهوم عدم مشروعية الدخول يرتبط أساسا بمعرفة من له الحق أو السلطة في الدخول إلى نظام المعالجة أو في التصريح بالدخول إليه،

[1] هلالي عبد الله أحمد، اتفاقية بودابست لمكافحة الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر،2007، ص 48.

[2] محمد خليفة، مرجع سابق، ص 138.

[3] محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية، الطبعة الأولى، دار الفكر والقانون للنشر والتوزيع، المنصورة، مصر، 2017، ص 59.

فمناط عدم المشروعية هنا هو انعدام سلطة الفاعل في الدخول إلى هذا النظام مع عمله بذلك[1]. وتتعدد صور الدخول غير المصرح به على النحو التالي:

قد يتم الدخول غير المصرح به عن طريق استعمال الجاني طريقة التخفي، أي انتحال صفة من له صفة الدخول إلى نظام معلوماتي معين بهدف الحصول على الحقوق والامتيازات العائدة لهذا الأخير، ويتحقق الركن المادي كذلك إذا قام الجاني بالتسلل وراء مستعمل مرخص له بالدخول إلى النظام المعلوماتي، وقد يلجأ الجاني مثلا إلى جهاز تنصت يستطيع من خلاله اختراق النظام أو عن طريق تجاوز نظم الحماية إذا كان ضعيفا، أو الاستيلاء على كلمات السر العائدة للمستخدمين الشرعيين، و مثال ذلك قيام موظف سابق بإحدى البنوك الفدرالية الأمريكية باختراق النظام المعلوماتي الخاص بهذا البنك باستخدام كلمة السر التي تحصل عليها من زميل سابق له، و يمكن الوصول إلى الرقم السري عن طريق الاكتساح أي إرسال مجموعة أو حزمة أو دفعة كبيرة من المعلومات إلى النظام المعلوماتي بغية التوصل إلى أي من هذه المعلومات يلقي أجوبة إيجابية، ويتحقق الدخول

أيضا في الفرض الذي يسمح به للشخص الدخول بناء على موافقة صاحب النظام أو بموجب اتفاق ما إلى جزء من النظام فيدخل إلى كامل النظام أو إلى جزء آخر منه محظورا عليه دخوله أصلا .[2]

إن جريمة الدخول غير المصرح به تقع من أي إنسان أي كانت صفته، شرط أن يكون ليس له الحق في الدخول إلى النظام، فتقوم الجريمة في كل حال يكون فيها الدخول مخالفا للشروط التي نص عليها القانون أو يكون مخالفا لإرادة من له الحق في السيطرة على النظام، كما أن هذه الجريمة تتحقق بمجرد الدخول المجرد بصرف النظر عن أي نتيجة، تبعا لذلك فإنها تعتبر جريمة سلوكية أو شكلية فالمشرع يعاقب على مجرد السلوك في حد ذاته حتى لو لم تكن للجاني النية في تحقيق ضرر أو نتيجة ما.[3]

[1] سامي منصور، مرجع سابق، ص 48.
[2] سامي منصور، المرجع نفسه، ص 49.
[3] سامي منصور، المرجع نفسه، ص 51.

ولذلك فبمجرد الدخول البسيط إلى النظام يمكن أن يقع تحت طائلة القانون الجنائي لأن الدخول غير المصرح به تم وفقا لتعليمات القائم على النظام والذي يتم باستعمال كلمة مرور مسروقة، تقنيا يعتبر الدخول مشروعا أما قانونيا فالدخول غير مشروع لأنه يشكل انتحال للشخصي. [1]

ب–فعل البقاء غير لمصرح به: وهي الصورة الثانية للسلوك، ونقصد به: " التواجد داخل نظام المعالجة الآلية ضد إرادة من له الحق في السيطرة على هذا النظام " [2]. تتحقق هذه الجريمة متى دخل الجاني عن طريق الخطأ أو الصدفة إلا أنه يقرر البقاء و عدم قطع الاتصال به، و لذلك فإن الركن المادي لهذه الجريمة لا يتمثل في السعي إلى إقامة اتصال للدخول إلى النظام إنما يتمثل في ضرورة قيام الجاني بقطع الاتصال الذي قام عن طريق الخطأ وامتناعه عن القيام بهذا الواجب يحقق صورة السلوك المجرم، وتعتبر هذه الجريمة من الجرائم التي يصعب إثباتها حيث يزعم المتهم في حالة القبض عليه أنه على وشك الانفصال المتعدي عليه هذا من جهة ومن جهة أخرى فإن تحقق الاتصال و من ثم السعي إلى قطعه يثير مشكلة عملية تتمثل في أن الجاني قد يجد نفسه في هذا الموقف ويحاول أن يقطع الاتصال لكنه يفشل إما لسبب أن النظام مزود بنظام أمني الغرض منه تحديد مصدر هذا الاتصال ومن ثم محاولة ضبطه، لذلك لا يمكن قطع الاتصال إلا بعد التعرف على مصدر الاتصال وتحديد موقعه، أو لسبب فني قد يجهله الجاني لا سيما إذا كان مستخدم النظام ممن لا يمتلكون الخبرة الكافية لذلك[3] .

وتتحقق الجريمة أيضا في الحالة التي يستمر فيها الجاني باقيا داخل النظام بعد المدة المحددة له للبقاء داخله أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها بالرؤية و الاطلاع فقط، وقد يجتمع فعل الدخول والبقاء غير المصرح بهما و ذلك في الحالة التي لا يكون فيها للجاني الحق في الدخول إلى النظام ويدخل إليه فعلا ضد إرادة من له الحق في السيطرة عليه ثم يبقى داخل النظام بعد ذلك، وهنا يتحقق

[1] عبد الفتاح بيومي حجازي، الحكومة الإلكترونية، دون طبعة، دار الفكر الجامعي، الإسكندرية، مصر، 2004، ص 361.
[2] شيماء عبد المغني عطاءالله، الحماية الجنائية للتعاملات الإلكترونية، دون طبعة، دار الجامعة الجديدة، الأزرايطية، مصر،2007، ص 121.
[3] رشيدة بوكر، مرجع سابق، ص، 215-216.

الاجتماع المادي بين الجريمتين، لذلك فإن جريمة البقاء غير المصرح بها تبدأ منذ اللحظة التي يبدأ فيها الجاني بالتجول داخل النظام بعد دخوله إليه بطريقة غير مشروعة، وإذا قام الجاني مثلا بالدخول إلى النظام عن طريق استعمال كلمة السر فإنه بمجرد كتابتها وقيامه بإجراء معين داخل النظام فعندها تكون جريمة البقاء غير المصرح به قد بدأت، أما إذا اقتصر فعله على كتابة هذه الكلمة فإن الجرم يعد دخول غير مشروع، ويتوافر الركن المادي بمجرد البقاء داخل النظام سواء كله أو جزء منه دون أن يضاف إليه ضرورة التقاط المعلومات .[1]

ج –تمييز البقاء غير المصرح به عن الدخول غير المصرح به:

الواضح من نص المادة 394 مكرر من القانون 15/04 الذي سبق وأن أشرنا إليها تضمنت جريمة الدخول أو البقاء غير المصرح بهما معا على خلاف التشريعات المقارنة التي ضمنت البقاء في نصوص مستقلة ومنها القانون الفدرالي الأمريكي لذا يثار تساؤل فقهي حول إمكانية اجتماع الدخول والبقاء غير المصرح بهما معا، وبمعنى آخر هل يمكن أم يحصل بقاء دون دخول غير مصرح به؟ لذلك نجد أن الفقه تنازع بين اتجاهين، الأول يري إمكانية الجمع بين كل من الدخول والبقاء، أما الثاني فيرى عكس ذلك، وهذا ما سنعرضه فيما يلي:

الاتجاه الأول: يرى أصحاب هذا الاتجاه أن يمكن الجمع بين الدخول والبقاء كون هذا الأخير لا يكون فقط عندما يكون الدخول مشروعا وذلك لأنه كل دخول غير مصرح به يقابله بقاء غير مصرح به أي أن هناك جمع بينهما، ويعاب هذا الاتجاه لأنه ليس من العدل أن يتساوى من دخل إلى النظام ثم خرج منه مع من دخله ثم بقي فيه، أي بين من ارتكب جريمة واحدة ومن ارتكب جريمتين، والأخذ بذا الرأي يشجع العدول عن جريمة البقاء لمن ارتكب جريمة الدخول.

الاتجاه الثاني: يذهب أنصار هذا الاتجاه إلى القول بأن كل جريمة تقع مستقلة عن الجريمة الأخرى ويعتمد هذا الرأي على حجتين:

[1] سامي منصور، مرجع سابق، ص 54.

الأولى تقتضي على المشرع في حالة استعمال كلمتين أو مصطلحين مختلفين فلا بد أن يكون لكل مصطلح معناه المختلف عن المصطلح الآخر، **أما الحجة الثانية** هي أن صفة الغش لا تنطبق على الدخول فقط انما تنطبق على البقاء أيضا وهو الرأي المؤيد.[1]

وتعتبر جريمة الدخول جريمة وقتية لأن هذا السلوك يبدأ وينتهي في وقت واحد كما أن هذا الأخير قابل بطبيعته للاستمرار، أما بالنسبة لجريمة البقاء غير المصرح به فهي من الجرائم المستمرة.[2]

2/ الركن المعنوي:

يعتبر الفقهاء جريمة الدخول أو البقاء غير المصرح بهما من الجرائم العمدية حيث يتخذ فيها الركن المعنوي صورة القصد الجنائي، أي يجب توافر القصد الجنائي العام دون القصد الجنائي الخاص،[3] حيث لا تتطلب المادة 394 مكرر من القانون 04/ 15 وكذا المادة 323 /1 من قانون العقوبات الفرنسي نية خاصة لدى الجاني حتى تقوم هذه الجريمة، ولا بد من توافر عنصري العلم والإرادة.

أ– العلم: يقدم الجاني على القيام بعمل أو الامتناع عن القيام به و هو يعلم بعدم مشروعيته، والمنطق القانوني يحتم في هذه الجرائم أن تكون عمدية لأن عمليات الدخول إلى أنظمة الحاسبات الآلية والبقاء فيها هي عملية تكرر بشكل مذهل في اليوم الواحد خاصة مع تزايد مستخدمي الإنترنت، إذ أنه ليس من المستبعد أن تكون هناك عمليات دخول أو بقاء غير مصرح بهما لكنها غير عمدية، لكن إذا كانت مثل هذه الجرائم كلها غير عمدية لوقع كل مستخدمي هذه الشبكة تحت طائلة قانون العقوبات، لذلك من الواجب أن تكون هذه الجرائم عمدية من أجل الموازنة بين حماية المعلوماتية من جهة وحرية الأفراد في استخدام الإنترنت من جهة أخرى .[4]

[1] رشيدة بوكر، مرجع سابق، ص 219.
[2] سامي منصور، مرجع سابق، ص 55.
[3] شيماء عبد الغني عطا الله، مرجع سابق، ص 126.
[4] نائلة عادل محمد فريد قورة، مرجع سابق، ص 365.

ب–الإرادة: بالإضافة للعلم طبعا يجب أن تتوافر الإرادة والتي تبين الموقف النفسي للفاعل من سلوكه ومن النتيجة المترتبة عليه لأن هذه الجريمة لا يتطلب قيامها تحقق نتيجة معينة فإن الإرادة تقتصر على السلوك الإجرامي، ويكفي أن يعلم الجاني أن دخوله أو ولوجه أو تواجده داخل نظام المعالجة الآلية للمعطيات دون رغبة ممن لهم السلطة أو السيطرة عليه مهما كان الدافع، ولا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاؤه داخل النظام مسموح به.[1]

ثانيا: جريمة الدخول أو البقاء في صورتها المشددة.

تنص المادة 394 مكرر في فقرتها الثانية من القانون 15/04 السالف الذكر بقولها: " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة ". وتشير الفقرة الثالثة على أنه: " وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج."

نستنتج من هذه الفقرات أن هناك ظرف مشدد في حالة الدخول أو البقاء غير المصرح بهما على أساسه تضاعف العقوبة ولتحقق هذا الظرف عندما ينتج عن فعل الدخول أو البقاء غير المصرح بهما:

-إما حذف أو تغيير معطيات النظام،

-أو عدم صلاحية النظام لأداء وظائفه.

إن وجود هذا الظرف المشدد يستوجب وجود علاقة سببيه بين فعل الدخول أو البقاء غير المصرح بهما وتلك النتيجة الضارة سواء محو أو تعديل المعطيات التي يحتويها النظام، ونلاحظ أن المشرع إما يحمي النظام من خلال حمايته للمعطيات التي يحتويها وإما عدم صلاحية النظام للقيام بوظائفه فإنه يعني عدم قدرته على تنفيذ المعالجة الآلية للمعطيات.[2]

[1] نائلة عادل محمد فريد قورة، مرجع سابق، ص 366.

[2] عبد القادر القهوجي، مرجع سابق، ص 137.

أ–طبيعية الجريمة: تعتبر جريمة الدخول أو البقاء غير المصرح بهما في صورتها البسيطة لا تتطلب حدوث أية نتيجة معينة، بينما تشدد عقوبة الجريمة إذا ترتب عنها ثلاث نتائج عددها المشرع وهي الحذف أو تغيير معطيات المعالجة الآلية أو تخريب هذا النظام، ولا يشترط المشرع أن تكون هذه النتيجة قصدية لأن هذا قد يقودنا إلى جريمة أخرى وهي الاعتداء العمدي على النظام.[1]

والظرف المشدد هنا ظرف مادي يكفي لتحققه وجود علاقة سببية بينه وبين جريمة الدخول أو البقاء غير المصرح بهما، ولذلك إذا حدثت النتيجة من فعل آخر فلا وجود للظرف المشدد، وإذا أثبت الجاني انتفاء تلك العلاقة كأن يثبت أن التعديل أو المحو أو تخريب النظام كان سببه القوة القاهرة أو الحادث المفاجئ[2]، وخارج هذه النتائج الثلاث يمكن للمتضرر أم يطالب بالتعويض وفقا للقواعد العامة للمسؤولية المدنية.[3]

ب–الركن المعنوي: يعتبر الأثر المترتب على جريمة الدخول أو البقاء غير المصرح بهما والذي يعتبر ظرف مشدد هو نتيجة غير عمدية، أي غير إرادية حيث لم تتجه نية الفاعل إلى الإضرار بالمعطيات أو النظام، فإن نظرنا إلى العبارة التالية: " فإذا ترتب على ذلك حذف أو تخريب ..." نجد أن نتيجة جريمة الدخول أو البقاء غير المصرح بهما غير مقصودة وعليه هذه النتيجة تدخل في الركن المادية للجريمة وليس الركن المعنوي أي أن المسؤولية عن ظرف مشدد هي مسؤولية مادية أو موضوعية.[4]

المطلب الثاني: جريمة الاعتراض غير القانوني لأسرار معلوماتية.

ذكرت المادة الثالثة من اتفاقية بودابست المبرمة في 23 نوفمبر 2001 على أنه: " يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية وفقا لقانونه

[1] مرجع نفسه، ص 138.
[2] عبد القادر القهوجي، مرجع سابق، ص 138.
[3] محمد خليفة، مرجع سابق، ص 162.
[4] محمد خليفة، مرجع نفسه، ص 164.

الداخلي واقعة القانون العمدي وبدون حق من خلال وسائل فنية للإرسال غير العلني لبيانات الحاسب بما في ذلك الانبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات، كما يمكن لأي طرف أن يستوجب أن ترتكب الجريمة بنية إجرامية أو ترتكب الجريمة في حاسب يكون متصلا عن بعد بحاسب آخر "[1] .

والغرض من النص على هذه الجريمة هو حماية الحق في حرية الاتصالات واحترام نقل البيانات دون التدخل من أطراف أخرى في الحديث أو المكالمات التليفونية التقليدية أو المراسلات البريدية أو عبر الإنترنت أو بترجمة الانبعاثات الكهرومغناطيسية الصادرة من الحاسب الآلي وصولا إلى البيانات وذلك بالنقل أو التسجيل باستعمال أي من الأجهزة الفنية للإرسال غير العلني للمحادثات أو البيانات أو الملفات أو المراسلات [2].

الفرع الأول: مفهوم جريمة الاعتراض غير القانوني.

لاحظنا المشرع الجزائري لم يتطرق إلى تحديد المقصود بهذا السلوك شأنه شأن أغلب التشريعات المقارنة، في حين نجد أن بعض الفقه قد تصدى هذه المهمة.

فنجد البعض عرفه على أنه: " قيام الجاني بخلق نظام وسيط وهمي بحيث يكون على المستخدم أن يمر من خلاله ويزود النظام بمعلومات حساسة بشكل طوعي" أو أنه: " رصد إشارات إلكترو مغناطيسية في الأنظمة المعلوماتية أو تحليلها بغية استخراج المعلومات المفهومة أو المقروءة منها."[3]

كما عرفته المادة الثالثة من الاتفاقية الدولية بشأن حماية المعلوماتية على أنه: " التصنت ونقل البيانات التي تتم عبر جهازين عن بعد عبر الشبكات المعلوماتية المختلفة أو بترجمة الانبعاثات الكهرومغناطيسية الصادرة من الحاسب إلى البيانات أو التي تتم عبر الأجهزة اللاسلكية وذلك عن " طريق أي من الوسائل الفنية غير علنية. [4]

[1] هلالي عبد الله أحمد، تم اعتماد الاتفاقية وتقريرها التفسيري من لدن لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة (8 نوفمبر/ 2001 (وفتح باب التوقيع على الاتفاقية في بودابست، في 23 نوفمبر/ 2001، بمناسبة المؤتمر الدولي حول الجريمة الإلكترونية، مرجع سابق، ص 49.

[2] فؤاد حسين العزيزي، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، 2014، ص 305.

[3] محمد سعادي، أثر التكنولوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديدة، الإسكندرية، مصر، 2014، ص، 224-223.

[4] بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات، دار الفكر الجامعي، الإسكندرية، مصر، 2008، ص 306.

وعرفه البعض الآخر على أنه: " انتهاك حق احترام الاتصالات كالتصنت والتسجيل التقليدي للمكالمات الهاتفية بين الأشخاص، والذي تستعمل فيه وسائل تقنية كالأجهزة التقنية التي يتم ربطها بخطوط الارسال وأجهزة تجميع وتسجيل الاتصالات اللاسلكية والبرامج وكلمات السر والشفرة، بالتصنت والمراقبة أو الرقابة لمضمون الاتصالات والحصول على ما يتضمنه سواء بصفة مباشرة «أو عن طريق استخدام أجهزة التصنت «.[1]

ومن هذه التعريفات يمكن لنا أن نشبه اعتراض نظام المعالجة الآلية بالتصنت على المحادثة على سبيل المثال، فهو يعني معرفة محتوى اتصال لكن ما يميزه أنه تم على شكل إلكتروني.

و تعتبر الوسيلة الأساسية لاعتراض نظام الحاسب الآلي هي استخدام الموجات الكهربائية الصادرة عن الحاسب الآلي، فاعتراض الحاسب الآلي كما هو معروف في الولايات المتحدة الأمريكية باسم التقاط الموجات الكهربائية وهو جمع المعلومات عن بعد، فمن الممكن جمع معلومات يتم ارسالها من خلال نظام الحاسب الآلي داخل مبنى وذلك باستعمال شاشة عرض يتم توصيلها بجهاز توصيل خارج المبنى، وتقوم هذه الشاشة بالتقاط الموجات الكهربائية التي تحيط الحاسب الآلي والتي تتحول إلى معلومات مقروءة على الشاشة من ناحية، كما يتم تسجيلها من ناحية أخرى، ففي حالة الاعتراض غير القانوني لا يمكن تحديد الجاني للمعلومات التي سوف يقوم بالتقاطها، حيث يلتقط الجاني المعلومات التي يتم ارسالها دون أن يكون له دور في تحديدها، إلا أن احتمال كون هذه المعلومات مفيدة للجاني نظرا لتحديده للمكان الذي يقوم بالتقاط المعلومات منه والذي ينطوي بالضرورة على أهمية للفاعل، كما أن الجاني في هذه الحالة يقتصر دوره على مجرد التقاط المعلومات دون أن يكون بيده إجراء أي تعديلات عليها فهو يلتقطها كما هي.[2]

الفرع الثاني: أركان جريمة الاعتراض غير القانوني.

تتمحور جريمة الاعتراض غير القانوني في ركنين أساسين سنعرضهما فيما يلي:

[1] رشيدة بوكر، مرجع سابق، ص 205.

[2] نائلة عادل محمد فريد قورة، مرجع سابق، ص 351.

أولا: الركن المادي: ويتمثل في فعل الاعتراض الذي يجب على الجاني أن يقوم به دون وجه حق وباستخدام وسائل غير علنية، ولقيام هذه الجريمة لابد أن يتوافر في الركن المادي شروط معينة لقيامه سنعرضها فيما يلي:

1-أن يكون فعل الاعتراض باستخدام وسائل فنية غير علنية:

باعتبار أن فعل الاعتراض يمثل الركن المادي لجريمة الاعتراض غير القانوني للبيانات يجب أن يكون باستخدام وسائل فنية معينة و غير علنية معدة للتصنت و نقل البيانات وتسجيلها والحصول على المحتويات بصورة مباشرة عن طريق الولوج أو الدخول إلى نظم المعالجة الآلية للمعطيات واستخدامها، أو بصورة غير مباشرة عن طريق استخدام أجهزة التصنت أو بتسجيل البيانات على أي من الأشرطة أو الدعامة المغناطيسية المعدة للتسجيل أو الأوراق، وقد يمتد نطاق هذه الوسائل إلى الأجهزة الفنية المتصلة بخطوط النقل أو الاتصال مثل أجهزة تجميع وتسجيل الاتصالات اللاسلكية، ويمتد أيضا إطارها ليشمل الكيانات المنطقية كالبرامج المعلوماتية وكذلك كلمات المرور.

وتوصف وسائل الاعتراض غير القانوني على أنها غير علنية، وهذه الصفة تلحق الوسيلة نفسها من أجهزة ومعدات وأدوات وطرق معدة للتسجيل أو النقل أو التصنت أو لالتقاط البيانات وليس البيانات المرسلة في حد ذاتها والتي قد تكون متاحة للغير والعامة من الجمهور أي لكل الناس.[1]

2-أن يكون الاعتراض دون وجه حق:

كذلك يشترط أن يكون فعل الاعتراض دون وجه حق، فإذا قام المتهم بالتصنت على المحادثات الشخصية للأطراف المعنية أو بنقل وتسجيل البيانات المعلوماتية أوجد من الأدلة و الأسانيد على أن قيامه بذلك قد تم بناء على ماله من حق استمده من أطراف المحاكمة أو الحديث الشخصي حيث سبق و أن صرح له بذلك أو أنه قد

[1] فؤاد حسين العزيزي، مرجع سابق، ص 307.

تصرف بناء على أمر قد صدر له منهما أو من المعنية بمراقبة الاتصالات و النظم المعلوماتية الخاصة بالمنشأة أو بالشركة أو الإدارة و الذي عن طريقه قد تمكن من الاستماع إلى المكالمات الشخصية أو الاطلاع على البيانات ونقلها لأغراض تتعلق بتجربة واختيار الأجهزة و المعدات لوضع أفضل السبل الأمنية لحماية هذه البيانات والمعلومات من الانتهاكات التي يمكن أن تتعرض إليها .[1]

ثانيا: الركن المعنوي: جريمة الاعتراض غير القانوني من الجرائم العمدية التي تتطلب توافر القصد الجنائي بعنصريه العلم والإرادة[2] . فلا بد أن يعلم الجاني أنه يقوم بالتصنت على المكالمات والأحاديث الشخصية وتسجيل ونقل البيانات المعلوماتية بغير رضا أطراف الاتصال، كذلك لابد أن تتجه إرادته إلى إتيان السلوك المادي الذي يشكل جريمة الاعتراض وهو التصنت أو النقل أو التسجيل للبيانات والمحادثات فإذا ما أكره على ذلك من قبل الآخرين لما لديه من خبرة ومهارة في استعمال أجهزة التصنت أو التسجيل أو لما لديه من تقنية استخدام الحاسبات الآلية و مهارة اختراق الشبكات المعلوماتية وأجهزة الاتصالات اللاسلكية أو كان دخوله غير إرادي أي عن طريق الصدفة أو تحت تأثير أي من وسائل الدفع والإكراه المعنوي والمادي فإنه لا يقوم القصد الجنائي وبالتالي لا تعتبر جريمة .[3]

المطلب الثالث: جريمة سرقة الأسرار معلوماتية

استخدام الحاسبات الآلية والأنظمة المعلوماتية على وجه العموم وترتب على ذلك تغيير في النمط العام للتعامل واختلاف في طريقة تناول المعلومات، ومن ذلك أخذت المعلومات في حد ذاتها أهمية غير مسبوقة وأصبحت مستهدفة، وأصبح أيضا لها سوقها الخاص بها وثمنها المرتفع جدا، وترتب على ذلك أن أصبحت تلك المعلومات هدفا للسرقة [4]، فتم استهداف كل أنواع المعلومات المالية والتجارية والشخصية والعسكرية وغيرها [5] ويعبر البعض

[1] بلال أمين زين الدين، مرجع سابق، ص 308.

[2] محمد كمال محمود الدسوقي، مرجع سابق، ص 102.

[3] فؤاد حسين العزيزي، مرجع سابق، ص 309.

[4] محمد عبد الله أبو بكر سلامة، مرجع سابق، ص 129.

[5] فالمعلومات المالية مثلا المتعلقة بالمركز الأموال، بينما التجارية ما تعلق منها مثلا الدراسات الخاصة بمشروعات التصنيع والإنتاج أما عن الشخصية فتتعلق بالمعلومات الماسة بسرية الحياة الخاصة والمخزنة في الحواسيب وعن العسكرية فمثلا ما تعلق بأسرار الدولة والمشروعات النووية والتصنيع الحديث

عن سرقة المعلومات بقرصنة المعلومات، وهي سرقة المعلومات من برامج وبيانات بصورة غير شرعية وهي مخزونة في ذاكرة الحاسوب أو نسخ برامج معلوماتية بصورة غير قانونية وتتم هذه العملية إما بالحصول على كلمة السر أو بواسطة التقاط موجات كهرومغناطيسية بحاسبة خاصة، ويمكن إجراء عملية القرصنة بواسطة رشوة العاملين في المنظمات المنافسة.

أما عن الهدف من عمليات القرصنة فهو سرقة الأسرار أو المعلومات التجارية أو التسويقية أو التعرف على حسابات المنظمات أو أحيانا بهدف التلاعب بقيود المصارف أو المؤسسات المالية بهدف سرقة الأموال، أو يكون الهدف الكشف عن أسرار صناعية بهدف إعادة تصنيعها دون إجازة قانونية، أو لأهداف سياسية وعسكرية من أجل الحصول على الملفات والخطط السرية العسكرية أو الحكومية، والأمثلة على حالات القرصنة عديدة فقد قامت الشركات الصينية بنقل أسرار تكنولوجيا صناعية من الولايات المتحدة وكندا مستخدمة الحاسوب ومن ثم القيام بإنتاج سلع على ضوء ذلك وتصديرها لهاتين الدولتين لتباع في أسواقها بثلث الأسعار الأصلية [1]. وذلك ما حدث لأكبر شركة أمريكية متخصصة في توفير خدمات الانترنت في عام 2001 والتي تخدم أكثر من 23 مليون مستخدم للأنترنت، عندما قام شاب يبلغ من العمر تسعة عشر عاما يدعى "جاي ستيرو" بإقناع مسؤوليها بأنه مفيد للشركة، فقاموا بتعيينه على الفور وعندما أظهر مهارة في العمل تطورت صلاحياته، وبدأ يطلع على بيانات مهمة خاصة بتلك الشركة، وظل طوال سنتين متواصلتين يجمع معلومات سرية مهمة عن الشركة، وفجأة قرر الاستقالة بحجة الحصول على وظيفة أخرى.

لكنه في الحقيقة كان يجهز لاستخدام ما جمعه من بيانات في شن هجمات شديدة القصوى على موقع الشركة، وبعد فترة من استقالته لاحظ المسؤولون عن تأمين موقع الشركة أن هناك شخصا يهاجم الموقع باحتراف

للأسلحة وغيرها، أنظر عبد العال الديربي، محمد صادق إسماعيل، الجرائم الالكترونية، دراسة قانونية قضائية مقارنة، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 170.

[1] انظر الموقع: http://www.ao-academy.org/docs/45D0، تاريخ الاطلاع على الموقع :2020/05/18 .

شديد، تنهار أمامه جميع إجراءات التأمين ويخترقها بسرعة، ثم يقوم باستبدال البرامج الخاصة بالموقع ببرامج أخرى من عنده تعطل العمل وتسبب مضايقات عديدة للعاملين في الشركة، وبعد فترة طور هذا القرصان عملياته وبدأ يسرق الأرصدة المدفوعة من اشتراكات الخدمات، وقد كلفت هذه العمليات غير المشروعة الشركة خسائر خلال وقت قصير جدا [1] .

الفرع الأول: مدى خضوع برامج الحاسب للنشاط الإجرامي في جريمة السرقة

الاختلاس في جريمة السرقة هو الاستيلاء على الحيازة الكاملة للشيء بدون رضا المالك أو الحائز السابق، ويتحقق هدا الاستيلاء إما بنزع الشيء من مكانه أو بالاستيلاء عليه بعد سبق التسليم بناء على اليد العارضة.

ويفترض الاستيلاء بهذا المعنى أن المالك أو الحائز الشرعي للشيء يفقد حيازته وسيطرته على هدا الشيء أي أن الاستيلاء ينتج عنه خروج الشيء المستولى عليه من ذمة ودخوله في ذمة أخرى وبمعنى آخر إفراغ ذمة وإشغال أخرى، بحيث لا يوجد مجال للتزاحم بين الذمتين في الاستيلاء على الشيء[2] تطبيق هدا المعنى للاختلاس على برامج الحاسب الآلي أو المعلومات المعالجة بصفة عامة يصطدم بعدة عقبات يمكن بلورتها فيما يلي:

العقبة 1: وقوع فعل الاختلاس على برامج وبيانات الحاسب يصطدم لا يعني خروجها من سيطرة حائزها، بينما يقتضي فعل الاختلاس بصدد هده الجريمة خروج المال بصفة كلية من سيطرة المجني عليه.

صحيح أن الجاني يتسبب باختلاسه برامج وبيانات الحاسب في دخولها إلى حوزته إلا إن هدا لا يعني خروجها من سيطرة المجني عليه بصورة كلية, كل ما يحدث أنه يفقد ميزة الاستئثار بها.

العقبة 2: تتمثل العقبة الثانية في حالة وقوع الاختلاس على البرامج والبيانات حال تجسدها في شكل سمعي أو مرئي عن طريق الالتقاط الذهني لها سواء عن طريق السمع أو البصر[3].

[1] محمد عبد الله أبو بكر سلامة، مرجع سابق، ص 13.

[2] علي عبد القادر القهوجي، المرجع السابق، ص 45.

[3] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة الطبعة الأولى، القاهرة، مصر، 1994، ص 232.

العقبة 3: المعلومات التي تحويها البرامج من طبيعة غير مادية، فكيف يتصور أن يرد فعل الاختلاس الذي هو من طبيعة مادية على شيء معنوي؟

أثيرت مشكلة خضوع البرامج لفعل الاختلاس أمام القضاء الفرنسي، ولكنه لم يتصد مباشرة لكيفية تخطي العقبات السابقة، وإنما قدم حلولا عملية يحاول الفقه من خلالها الوصول إلى التأصيل النظري لتجاوز هده العقبات، وموقف الفقه منها أنها في نظر البعض تستعصي على الحل وفي نظر البعض الآخر لا تستعصي على الحل، وأن تجاوزها أمرًا ميسور.

وأول حكم أصدرته محكمة النقض الفرنسية في هذا الشأن هو حكم لوجاباكس [1] LOGAPAX في سنة 1979 وصدر حكم آخر عرف باسم حكمHERBERTAUX وفي سنة 1986[2] وحكم ثالث صدر باسم BOURQUIN في سنة 1989 [3]

[1] Cass. Crim ; 8 janvier 1979. p-509 et note p- Corlay. g.p 1979 II p 501 et observation Roujour de Boubee

تتلخص وقائع قضية لوجاباكس في أن أحد مهندسي شركة لوجاباكس فصل من عمله وفي الدعوى المرفوعة ضد رب العمل قدم -للمحكمة تأييدا لدعواه صورتين كان قد نسخهما لمستندين من مستندات الشركة أمكنه الحصول عليها بمناسبة وظيفته السابقة و قبل فصله من العمل قدم للمحاكمة بتهمة سرقة هده المستندات و برأت محكمة أول درجة ، و تأييد حكم البراءة في الاستئناف على أساس أن المتهم لم يحمل هده المستندات إلى منزله على سبيل التملك و لكن م.ن.ف نقضت الحكم السابق لمخالفته صحيح القانون لأن القانون لم يشترط لتحقق الأخذ أو الاختلاس في جريمة السرقة أخد أو انتزاع الشيء وأن الاختلاس يمكن أن يتحقق و لو كان الشيء بين يدي الجاني قبل الاستيلاء عليه على سبيل اليد العارضة ولأن الجاني استولى على المستندين التابعين للشركة المذكورة التي كان يعمل فيها لمصلحته الشخصية بدون علم وبدون رضا رب العمل المالك لهما أثناء الوقت اللازم لتصويرها.

[2] تتلخص وقائع القضية في أن العامل هيربيرتو دخل بمناسبة وظيفته إلى المكان الذي تحفظ فيه خطط تصميم المنتج الذي تنتجه الشركة التي يعمل بها و حصل على نسخ لهده الخطط أثناء خدمته بتلك الشركة، ثم استقال من وظيفته و أنشأ هو و زملاؤه شركة جديدة تنتج نفس المنتج مستخدمين في دلك الصور التي سبق نسخها، قدم هدا العامل للمحاكمة بتهمة السرقة وقدم زملاؤه بتهمة إخفاء أشياء مسروقة، فأدانهم حكم أول درجة و في الاستئناف ، تأييد هدا الحكم، و رفضت محكمة النقض نقض هدا الحكم لتوافر جريمة السرقة في حق هدا العامل الذي أخد لأغراض شخصية و بدون موافقة رب العمل نسخا من خطط المنتج الذي تنتجه الشركة التي يعمل بها.

وكانت محكمة جنح MONBELLIARD قد أصدرت حكما يتعلق بموظف سابق كان يعمل لدى شركة PEUGEOT للسيارات وأثناء عمله لدى شركة أخرى قام بمساعدة زملائه القدامى بنسخ أو تسجيل البرامج المعلوماتية التي كان قد ساهم فيها قبل تركه العمل على قرص مغناطيسي كان قد حمله معه خصيصا لهدا الغرض وأدانته بجريمة السرقة على أساس أنه اختلس المعلومات المسجلة على قرص مغناطيسي والتي تتضمن برامج معلوماتية تخص شركة بيجو.

[3] Cass Crim. 12 janvier 1989B.C p38 N°14 M.p-lucas de Leyssac : l'arrêt bourquin préaté R.S.C. 1990p507.

نستنتج أن الأحكام السابقة على اختلاف وقائعها تعتبر أن تصوير أو نسخ البرامج أو المعلومات بصفة عامة بدون علم وبدون رضا أصحابها لأغراض شخصية مكونا لجريمة السرقة.

وقد انقسم الفقه الفرنسي بمناسبة تعليقه على هده الأحكام حول الشيء الذي وقعت عليه أفعال الاختلاس، وصلاحية هدا الشيء لوقوع الاختلاس عليه، فمنهم من قال بصلاحية وقوع الاختلاس على المعلومات مباشرة، ومنهم من رفض دلك معتبرا أن هدا الفعل وقع على الأصل الذي تم تصويره أو على الآلة التي قامت بالتصوير.

الفرع الثاني: الفقه القائل بصلاحية المعلومة للاختلاس

بداء أنصار هدا الاتجاه من نقطة أساسية هي أن طبيعة الشيء المختلس تحدد الطريقة التي يتبعها الجاني للقيام بالنشاط الإجرامي المحقق للاختلاس، وهكذا يختلف الأسلوب الذي ينفد به النشاط باختلاف الشيء الذي يقع عليه الاختلاس سواء من حيث طبيعته أو حجمه أو وزنه أو مقاومته أو وظيفته أو قيمته، وهدا ما أكدته محكمة النقض الفرنسية.

لدلك فسرقة شيء مادي تختلف عن سرقة شيء معنوي فإذا كانت الأشياء المادية يتم اختلاسها من خلال نشاط مادي يصدر عن الجاني فإن الأمر لن يكون على هده الصورة دائما بالنسبة للأشياء المعنوية، فهده الأخيرة يمكن اختلاسها عن طريق اختلاس الدعامة التي تحتويها، ويمكن أيضا اختلاسها استقلالا عن تلك الدعامة ومقتضى دلك ان برامج الحاسب الآلي والمعلومات يمكن التقاطها ذهنيا دون أي نشاط مادي ملموس وخاصة عن طريق النظر أو السمع.

هدا المنطق يؤدي بنا إلى القول بتوافر جريمة السرقة في حق من يقرأ كتاب ويحفظ ما به دون علم صاحبه، أو من يقرأ برنامجا على شاشة الحاسب الآلي ويحفظه، مثل هدا القول لا يمكن التسليم به ومن غير المسوغ الأخذ به في مجال القانون الجنائي إذ لابد من نشاط مادي يصدر عن الجاني للقول بقيام عنصر الاختلاس، فالقانون الجنائي لا يعاقب على مجرد الأفكار مهما كانت جسامتها.

من أجل الخروج من هدا المأزق، يذهب أصحاب هدا الاتجاه إلى أن اختلاس المعلومة يجب أن يتم بنشاط مادي، وهدا النشاط هو عملية النسخ أو التصوير التي عن طريقها تنتقل المعلومة من الأصل إلى الصورة أما بالنسبة للمعلومة التي تم التقاطها ذهنيا فان الاختلاس لا يتحقق بالنسبة لها إلا إذا وضعت موضع التنفيذ أو تم بيعها أو نقلها إلى الغير على دعامة مادية أو إذاعتها لأن هدا النشاط المادي هو الذي ينتج عنه انتقال المعلومات من ذمة إلى أخرى ويقوم به الاختلاس.

ويقتصر بعض مؤيدي هدا الاتجاه على النشاط الذي يفرغه الجاني في عملية النسخ إذ به يتحقق الاختلاس.

إن أنصار هدا الاتجاه يرون أن اشتراط مادية النشاط الإجرامي الذي يتحقق به الأخذ أو الاختلاس في حالة وقوعه على المعلومات أمر تفرضه طبيعة الأشياء دلك أن التسامح بالنسبة لأحد العناصر المكونة للجريمة يجب أن يقابله تشدد بالنسبة للعناصر الأخرى لتجنب تشويه مفهوم تلك الجريمة، فادا تسامحنا مثلا بعض الشيء في الركن المادي يجب أن يقابل هدا التسامح تشدد في الركن المعنوي.[1]

وهدا هو الحاصل بالنسبة لاختلاس المعلومات، فالموافقة على وقوع الاختلاس على شيء معنوي على خلاف ما هو مستقر عليه في الماضي يجب أن يقابله تشدد في طبيعة الأخذ أو الاختلاس ذاته والقول بضرورة تحققه بنشاط مادي وتتحقق مادية الاختلاس بالنسبة للمعلومات إذا ما تم نقلها على دعامة مادية أيا كانت مادتها أو هيئتها وهو ما يؤكد أن الاستيلاء على الشيء يختلف باختلاف طبيعة هدا الشيء، فأخذ شيء غير مادي مثل المعلومات لا يكون ماديا إلا إذا كان هدا الشيء قد تجسد في هيئة مادية.

وإيضاحا لإمكانية سلب حيازة المعلومة فان الأشياء غير المادية قابلة للحيازة و مادام يمكن حيازتها تصبح سرقتها متصورة في الحالة التي يتم فيها الاختلاس دون تحريك للشيء من مكانه و يرجع الفضل في دلك إلى القضاء الفرنسي والدي قام بتأصيله الفقيه الفرنسيGARCON وأنشأ نظريته في الاختلاس انطلاقا من

[1] Goutal : La protection pénale des logiciels, Le droit commercial face aux technologies nouvelles de la communication. Paris 1986, p 254.

أحكام القضاء حيث أصبح من المسلم به بناء على هده النظرية أن يتحقق الاختلاس وتقوم السرقة إذا كان الشيء يوجد قبل الاستيلاء عليه بين يدي الجاني على سبيل اليد العارضة ولكن القضاء الفرنسي لم يتوقف عند هدا الحل بل اعترف بإمكانية وقوع الاختلاس في الحالة التي يحرم فيها مالك الشيء من حيازته ولو لفترة قصيرة يظهر خلالها الجاني بمظهر السيد المسيطر على الشيء وهده هي سرقة الاستعمال التي يرى القضاء الفرنسي أنها سرقة عادية[1]

يستنتج أنصار الاتجاه القائل بإمكانية وقوع فعل الاختلاس على المعلومة بأن التطور السابق في نظرية الاختلاس يستنتج منه أن جريمة السرقة تقع في كل حالة يحرم فيها مالك أو حائز الشيء – ولو لفترة قصيرة – من مميزات حق الملكية التي له على الشيء، حتى لو لم يتحرك هدا الشيء من مكانه، ويرون أن الاختلاس ما هو إلا إنقاص لذمة فإذا كان الشيء المختلس ماديا فإن إنقاص ذمة المجني عليه لا يكون إلا بخروج الشيء من ذمته بنقله أو تحريكه، أما إذا كان الشيء يحتوي على قيمة اقتصادية معنوية مثل البطارية الجافة التي تحتوي على طاقة تعتبر مالا ، فإننا لا نكون بحاجة إلى نقل للشيء (البطارية) فسحب الطاقة من هده البطارية يعني إنقاصا من الذمة دون نقل الشيء.

قد يقال هنا أن السرقة سرقة استعمال، ولكن هدا غير صحيح لأنها لو كانت كذلك لوقعت على البطارية كلها على هيكل البطارية وما بداخله من كهرباء وفي حالتنا لم يحدث شيء من دلك، فالبطارية مازالت في مكانها لم تتعرض لأي اعتداء من أي نوع أي لا يوجد أي انتقاص للبطارية وبالتالي لا يوجد اختلاس لهيكل البطارية، وإنما الاختلاس وقع على الطاقة فهي التي خرجت من ذمة مالكها.

إذا طبقنا هدا المفهوم في مجال البرامج والمعلومات، فإن نسخ البرامج من دعامتها دون نقل لها ودون خروجها من المكان الذي توجد فيه دون رضا صاحب الحق عليها لا يعني بان فعل الاختلاس في هده الحالة قد وقع على الدعامة

[1] Garçon : Code pénal annoté ; 2eme édition par m. rousselet, N° 47, p.575.

أو الأصل إنما يكون هدا الفعل قد وقع (من خلال عملية التصوير أو النسخ) على المعلومات التي يحتويها الأصل أو الدعامة.

وأدى إلى انتقالها من خلال الأصل أو تلك الدعامة إلى الصورة ولكن يلاحظ هنا – على عكس الطاقة–أن المعلومات (البرنامج) مازالت بين يدي مالكها وتحت سيطرته إلا أن قيمتها نقصت بفعل الاختلاس لان صاحبها يكون في هده الحالة قد فقد حقه في احتكار استغلالها[1]، مما أدى بهذا الاتجاه الفقهي إلى القول بصلاحية وقوع الأخذ على برامج الحاسب والمعلومات بصفة عامة مستقلة عن دعامتها الأصلية التي يتم نسخها وهي في مكانها.

واستطرادا مع هدا الاتجاه الفقهي فإن جريمة السرقة تقع على المعلومات فقط سواء تم النسخ مباشرة أم عن بعد متصلة بالحاسب المركزي وسواء كانت هده الطرفية سلكية أو لاسلكية.

الفرع الثالث: الفقه القائل بعدم صلاحية المعلومة للاختلاس

اصحاب هدا الاتجاه الفقهي يستبعدون أن تقع جريمة السرقة على البرامج والمعلومات مستقلة عن دعامتها نظرا للطبيعة غير المادية للمعلومات وأنها على خلاف الطاقة تبقى بين يدي صاحبها على الرغم من حصول الجاني عليها في حالة نسخها، فعلى الرغم من أن المعلومات مال إلا أنها مال يتميز عن غيره من الأموال بالخصائص الثلاث التالية:

– أنه مال غير قابل للنفاد، بمعنى أنه لا ينفد بالاستعمال ولا يفقد قيمته إلا بالنسيان أو بظهور معارف جديدة.

– أنها مال يمكن استعماله بواسطة أطراف عديدة في نفس الوقت دون أن يفقد قيمته فالمعلومات لا تتغير باتساع نطاق استخدامها.

– نفقة نقل هدا المال من طرف لأخر ضئيلة للغاية ولا تقارن بنفقة إنتاجه[2]

[1] Lucas de leyssac : l'arrêt buorquin…, article précité, p12.

[2] حسام محمد عيسى، نقل التكنولوجيا دراسة في الآليات القانونية للتبعية الدولية، دار المستقبل العربي، القاهرة، مصر، 1987، ص 62.

الإشكال المطروح أن أصحاب هدا الاتجاه لم يكن لهم رأي واحد حول تفسير أحكام النقض السابقة فمنهم من رأى أن السرقة قد وقعت على الأصل، ومنهم من اعتبر أنها قد وقعت على الآلة وفي الحالتين لا تعدو أن تكون سرقة استعمال ومنهم من انتهى إلى أن السرقة وقعت على الكهرباء.

أولا: وقوع فعل الاختلاس على الأصل:

اتجه جانب من الفقه الرافض لفكرة صلاحية المعلومة للاختلاس بأن محل الاختلاس ليس المعلومة وإنما فعل الاختلاس قد تم على الأصل، ومنطقه في دلك أن فعل الاختلاس يتمثل في الاستيلاء على الأصل مدة الوقت اللازم لتصويره، وأن الجاني في هده الحالة يتوافر في حقه سرقة استعمال (vol d'usage) لهدا الأصل حتى ولو كان هدا الاستيلاء لم يستمر فترة طويلة من الزمن.

وصلاحية المعلومة محلا للاختلاس ينكرها البعض بدعوى أن المعلومة لا تؤخذ وإنما تكتسب، وان اكتساب شخص لها لا يعني أنه أخدها ودلك لأنها تظل ولو اكتسبها الغير على حالها.

كما أن اخذ أو حصول الغير على المعلومة ليس من شانه حرمان صاحبها منها وإنما مشاطرته أو مشاركته فيها.[1]

ويستند هدا الرأي إلى ما استقر عليه التطور القضائي بشأن سرقة الاستعمال وبصفة خاصة استعمال السيارات، ففي هدا النوع من السرقة لا يشترط القضاء الفرنسي أن يكون الاستيلاء على السيارة قد تم على سبيل التملك، وإنما يكفي أن يكون لهدا الاستيلاء أحد مظاهر الملكية على الشيء حتى ولو كان لفترة قصيرة يعود الشيء بعدها إلى مالكه لأن الجاني في تلك الفترة كان يبدو مثل المالك الذي يستعمل سيارته. ولقد اضطر القضاء الفرنسي أمام انتشار ظاهرة اخذ السيارات لاستعمالها ثم إعادتها إلى مكانها أو أي مكان آخر أن يعطي مفهوما موسعا للاختلاس والقصد الجنائي في جريمة السرقة حتى يستطيع ملاحقة هده الأفعال التي لم يتدخل

[1] P.Corlay : Reflection sur les récentes controverses relatives au domaine et à la définition De vol. J.C.P 1984 I doct 3160

المشرع لتجريمها بنص خاص[1] وانتهى به هدا التطور إلى التسليم بوقوع هده السرقة (سرقة الاستعمال) على الدعامة التي تحتوي على البرامج والمعلومات الوقت اللازم لتصويرها مهما كان قصيرا وان لم يصل به هدا التطور إلى درجة القول بوقوع السرقة على المعلومات وحدها.

ثانيا: وقوع فعل الاختلاس على الآلة:

توجه جانب من الفقه إلى القول بان السرقة هنا وقعت على الآلة وليس على الأصل وأنها سرقة وقت الآلة أي أن هدا الرأي يعتبر أن فعل الاختلاس وقع على آلة الحاسوب ذاتها وأن هدا (vol du temps machine) الفعل يتمثل في الاستيلاء عليها ولو لوقت قصير جدا هو الوقت اللازم لنسخ صور للبرامج أو المعلومات الأصلية من خلالها[2]

يرى أصحاب هدا الرأي أن السرقة في هذه الحالة هي سرقة استعمال كما ذهب إلى ذلك أصحاب الرأي السابق مع فارق واحد يتعلق بمحل الاختلاس فهو الأصل في الرأي السابق والآلة بالنسبة لهدا الرأي.

الإشكال أن هذين الرأيين يصطدمان بعقبة مؤداها أنه من الممكن أن يتم الحصول على البرنامج أو نسخ صورة منه دون الاستيلاء على الأصل أو الآلة وذلك في حالة ما إذا تم هذا النسخ من خلال طرفية تتصل بالحاسب المركزي سلكيا أو لاسلكيا بحيث لا يحرم صاحب البرنامج أو الآلة ولو لفترة قصيرة من استعمال أي منها.

ولتفادي هذه العقبة، اتجه رأي إلى أن السرقة هنا وقعت على القدر من التيار الكهربائي اللازم لاستخدام الصورة من خلال الومضات التي يترتب عليها فنيا استخراج هذه الصورة.

[1] ويلاحظ ان المشرع المصري أنه تدخل بنص خاص جرم بمقتضاه الاستيلاء على السيارات بغير حق وبدون نية التملك (م 323)

[2] Bertrand : La criminalité informatique, les délits relatifs au matériel. D1984, n° 62, expertise, p 149 /1 مكرر .

ولكن هذا الرأي نفسه لا يرى في هذا التفسير حلا للمشكلة لأن كمية الكهرباء المستهلكة لا تكاد تذكر وهي من البساطة بحيث لا يوجد وجه للمقارنة بينها وبين سرقة التيار الكهربائي المعروفة ويستبعد تبعا لذلك وقوع جريمة السرقة على التيار الكهربائي في هذه الحالة.[1]

ولهذا فقد اتجه الرأي إلى عدم وقوع السرقة في الحالات السابقة لأن طبيعة البرنامج والمعلومات تأبى تحقق الأخذ أو الاختلاس بمعناه الدقيق المسلم به في جريمة السرقة ، والذي يعني الاستيلاء على الحيازة الكاملة للشيء دون رضا صاحبها أو حائزها السابق، لأنه إذا تصورنا وقوع الاختلاس من خلال النسخ أو التصوير على المعلومات، هذه المعلومات الأصلية ذاتها تظل في نفس الوقت كما كانت من قبل تحت سيطرة صاحبها الأصلي ولا تخرج من حيازته[2] وعليه فان الفقه الجنائي انقسم بين مؤيد ومعارض لخضوع برامج الحاسب الآلي لفعل الاختلاس.

[1] Pradel et Feuillard : Les infractions commises au moyen de l'ordinateur.R.dr.pén. crim1985.p307.

[2] **هدى حامد قشقوش، المرجع السابق، ص 63.**

الفصل الثاني

الحماية الجنائية الاجرائية

يعتبر امن اسرار المعلومات, من اهم الامور التي شغلت المجتمع في عصرنا الحالي, نظرا لان الاعتداءات ,اصبحت سهلة التنفيذ, من خلال نقرات بسيطة على فارة الحاسب او على شاشة الهواتف الذكية من خلال التعديل او النسخ واللصق ,لذلك كان لابد من تتبع هؤلاء المجرمين وسن قوانين لردعهم وتنظيم اجراءات لمتابعتهم وتسليط عقوبات في حقهم, من شانها ان تقلص من ارتكاب مثل هذه لجرائم, الامر الذي اوجب اتباع اجراءات صارمة خاصة بخصوصية نوع الجريمة ,موضوع الدراسة وادوات القيام بها, لذلك وجب اتباع طرق تتماشى مع هذه الخصوصية و اعتماد اليات و وسائل تسهل من مهمة الكشف على الجاني المتعدي على اسرار معلوماتية للأشخاص والمؤسسات, لان امن المعلومات ما هو الا جزء لا يتجزأ من الامن العام الذي يفترض ان يتمتع به الافراد وتسهر على تحقيقه الجهات الامنية المختصة وهي يجب ان تتوفر على اجهزة ومتخصصين في المجال التقني ومن تمة تطبيق القانون على المعتدين وتسليط عقوبات مناسبة سواء على الشخص الطبيعي والمعنوي.

المبحث الاول: المتابعة والتحقيق في الجرائم الماسة بإسرار المعلوماتية.

لا شك في أن التطور الحالي الذي لحق ثورة الاتصالات عن بعد وما أفرزته هذه الثورة من وسائل الكترونية متقدمة ومتعددة قد انعكس أثره عن الجرائم التي تمخضت عن ذلك. بحيث يثأر القانون ثأترا بالغا بالتقدم العلمي ولكي تتحقق الفائدة المرجوة من هذا التقدم، فإن القانون يجب ألا ينفصل عن الواقع الذي يفرزه ويطبق عليه، بل يجب أن يكون متجاوبا معه ومتطور بتطوره بحيث تميزت هذه الجرائم بطبيعة خاصة من حيث الوسائل التي ترتكب بها، ومن حيث المحل التي تقع عليه من حيث الجناة الذين يرتكبونها على النحو السابق الإشارة إليه، بحيث يمكن القول إن الأساس في خطر هذه الجرائم يكمن في أنها تجمع بين الذكاء الاصطناعي والذكاء البشري مما جعل إثباتها جنائيا قد يكون في منتهى الصعوبة.

فالتطور الحالي الذي انعكس أثره على قانون العقوبات قد انعكس أثره أيضا على قانون الاجراءات الجزائية، بحيث أن هذا القانون الأخير قد لا يطبق بسبب عجز القانون الأول عن استيعاب الجرائم المستحدثة التي ترتكب بالوسائل الالكترونية.

فالإثبات الجنائي هو أحد الموضوعات الهامة لهذا القانون، فقد تأثر بدوره بالتطور الهائل الذي لحق الأدلة الجنائية بسبب تطور طرق ارتكاب الجريمة، الأمر الذي يتعين معه تغيير النظرة إلى طرق الإثبات الجنائي لكي تقترب الحقيقة العلمية في واقعها الحالي من الحقيقة القضائية.

اما إثبات الجرائم التي تقع على العمليات المعلوماتية باستخدام الوسائل الالكترونية سيتأثر بطبيعة هذه الجرائم، وبالوسائل العلمية التي قد ترتكب بها، مما قد يؤدي إلى عدم اكتشاف العديد من الجرائم في زمن ارتكابها، أو عدم الوصول إلى الجناة الذين يرتكبون هذه الجرائم أو تعذر إقامة الدليل اللازم لإثباتها مما يترتب عليه إلحاق الضرر بالأفراد وبالمجتمع.

المطلب الأول: اجراءات التحري وجمع الأدلة في الجريمة المعلوماتية

فالجريمة المعلوماتية النمطية الواحدة التي تمتاز بها الجرائم التقليدية خالفت في طبيعتها الكلية والتي رصدت التشريعات القانونية الإجرائية.

لا سيما سبل لمحاربتها إلا أن جرائم العصر الرقمي الجديد أحدثت إشكالا عاما يبرز كيفية التعامل مع هاته الجرائم التي أرغمت المشرع القانوني إلى تدارك النقص الهائل ومحاولة ملأه مسايرا في ذلك عدة معايير أهمها التقنية العالية في هاته الجريمة[1].

[1] منتدى شباب طمرة، قسم الكمبيوتر والأنترنت، "جرائم الكمبيوتر والأنترنت": الموقع، www.tamra.com، يوم الاطلاع: 2020/05/30، على الساعة (14:09).

فهي لا تترك أثرا ماديا في مسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية كما أن مرتكبيها يملكون القدرة على اتلاف او تشويه أو إضاعة الدليل في فترة قصيرة، ولا تكفي في هذا النمط من الجرائم إعادة نظام الكمبيوتر وقواعد البيانات وشبكات المعلومات.

الفرع الأول: طرق ووسائل البحث في الجريمة المعلوماتية

خطوات جمع الادلة كما حددها القانون هي: المعاينة، الخبراء، التفتيش، وضبط الأشياء، ومراقبة المحادثات وتسجيلات وسماع الشهود الاستجواب والمواجهة.

وليس على المحقق الالتزام باتباع ترتيب معين مباشرة هذه الاجراءات بل هو غير ملزم أساسا بمباشرتها جميعا وإنما يباشر منها ما تمليه مصلحة التحقيق وظروفه ويرتبها وفقا لما تقضي به المصلحة وما تسمح به هذه الظروف وسوف نوضح في مجال جميع الأدلة ما يلي:

- أولا: معاينة مسرح الجريمة المعلوماتية.
- ثانيا: التفتيش في مجال الجريمة المعلوماتية.
- ثالثا: الشهادة في الجريمة المعلوماتية.
- رابعا: الخبرة في مجال الجريمة المعلوماتية.
- خامسا: الضبط في مجال الجريمة المعلوماتية[1]

أولا: معاينة مسرح الجريمة المعلوماتية

نعني بالمعاينة فحص مكان أو شيء او شخص له علاقة بالجريمة وإثبات حالته، كمعاينة مكان ارتكاب الجريمة أو أداة المعاينة قد تكون إجراء حقيق لإثبات ما بالجسم من جراح أو على الثياب من دماء أو ما بها من مزق أو ثقوب.

[1] منتدى شباب طمرة، قسم الكمبيوتر والأنترنت، "جرائم الكمبيوتر والأنترنت": الموقع، www.tamra.com، يوم الاطلاع: 2020/05/30، على الساعة (14:09

ويلاحظ أن المعاينة قد تكون إجراء تحقيق او استدلال، ولا تتوقف طبيعتها على صفة من يجريها بل على ما يقتضيه إجراؤها من مساس بحقوق الأفراد فإذا جرت المعاينة في مكان عام كانت إجراء استدلال وإذا اقتضت دخول مسكن او له حرمة خاصة كانت إجراء تحقيق[1].

والمعاينة جوازية لمحقق شأنها شأن سائر إجراءات التحقيق فهي متروكة إلى تقديره سواء طلبها الخصوم او لم يطلبوها، ولا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة. من الأهمية التي تلعبها في مجال الجريمة التقليدية، ومرد ذلك إلى الاعتبارات السالف ذكرها[2] وحتى أصبح معاينة مسرح الجريمة المعلوماتية لها فائدة في كشف الحقيقة عنها وعن مرتكبها فإنه ينبغي مراعاة عدة قواعد وإرشادات أهمها ما يلي:

1- تصوير الحاسب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه، مع التركيز بشكل خاص على تصوير الأجزاء الخلفية للحاسب ملحقاته ويراعي تسجيل وقت وتاريخ ومكان التقاط كل الصور

2- المهانة البالغة التي تم بها إعداد النظام الآثار الالكترونية، وبوجه خاص التسجيلات الالكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو النظام أو الموقع أو الدخول معه في الحوار.

3- ملاحظة وإثبات حالة التوصيلات والكبلات المتصلة بالنظام حتى يمكن إجراء عملية المقارنة والتحليل حين عرض فيما بعد على القضاء.

4- عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختيارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجالات لقوى مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة.

[1] شيباني عبد الكريم مذكرة ماستر الحماية الإجرائية والموضوعية للجريمة المعلوماتية، ص28.

[2] ID=148.http://www.arablawinfo.com/research-search.asp?Validate=articles : يوم الاطلاع 2020/05/30 على الساعة (14:14)

5- التحفظ على محتوى سلة المهملات من الأوراق الملقاة والممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة، السليمة وغير السليمة او المحطمة وفحصها ورفع البصمات التي قد كون لها صلة بالجريمة المرتكبة .

6- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليه من بصمات[1].

تحضير خطة للهجوم بحيث تكون الخطة واضحة ومفهومة لدى أعضاء الفريق، على أن تكون الخطة موضحة بالرسومات وتتم مراجعتها مع أعضاء الفريق قبل التحرك، مع الأخذ في الاعتبار قاعدة سماك العسكرية والتي تعني الحالة الرسالة التنفيذية المداخل والمخارج والاتصالات هي ملائمة للأجهزة الأمنية وأجهزة تنفيذ القوانين، فالحالة أو الوضع يعني معرفة حجم القضية التي تقوم بالتحقيق فيه وعدد المتورطين فيه، أما الرسالة فهي تحدد الهدف من الغارة، والتنفيذ يعني كيفية أداء المهمة، أما المداخل والمخارج فإن من المهم معرفتها ضرورية وهي تختلف من جريمة لأخرى وتحسب وفقا لمكونات طريق التحقيق، بينما يأتي عنصر الاتصال لضمان السرية وسلامة لعامل وتبادل المعلومات أثناء الغارة[2] .

- وبعد وصول الفريق إلى مسرح الجريمة يتم التأمين والسيطرة على المكان والبدء في التفتيش على النحو التالي:

1- السيطرة على المناطق المحيطة بمسرح الجريمة أو مكان الإعارة وذلك عن طريق إغلاق الطرق والمداخل.

2- السيطرة على الدائرة المحيطة بمكان الإغارة بوضع حراسات كافية لمراقبة التحركات داخل الدائرة، ورصد الاتصالات الهاتفية من وإلى مكان الإغارة مع إبطال أجهزة الهاتف النقال.

3- تأمين موقع الغارة والسيطرة على جميع أركانها ومنافذها والتحفظ على الأشخاص الموجودين.

---

[1] شيباني عبد الكريم مرجع السابق ص29.

[2] نبيلة **هبة** محمد **هروال**، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الطبعة الأولى، لإسكندرية، مصر، 2007، ص 220.

4- تحديد أجهزة الحاسب الآلي الموجودة في مكان الإغارة وتحديد موقعها بأسرع فرصة ممكنة، وفي حالة وجود شبكة اتصالات يجب البحث عن خادم الملفfile server لتعطيل حركة الاتصالات.

5- يوضع حرس على كل جهاز حتى لا يتمكن أحد المتهمين من اتلاف المعلومات من على البعد أو من جهاز آخر داخل المبنى.

6- اختيار مكان لمقابلة المتهمين والشهود على أن يكون المكان بعيدا عن اجهزة الحاسب الآلي[1].

ثانيا: التفتيش في مجال الجريمة المعلوماتية

يعتبر التفتيش اجراء من اجراءات التحقيق يتطلب أوامر قضائية لمباشرته، ويهدف للبحث عن الأدلة المادية التي ترتبط بالجريمة مدار التحقيق. ولا يشتمل لذلك الأدلة الشفوية أو القولبة للاتصال الأخيرة بعنصر الشخص الشاهد، ويجري التفتيش بخصوص جرم تحقق وقوعه ويوجه إلى مكان يتمتع بالحرمة او يتجه إلى الشخص المشتبه به، ويخضع التفتيش غي وجوده وإجراءاته التنفيذية إلى أحكام القانون التي من أبرزها صدور أمر التفتيش أو مذكراته الكتابية عن الجهة التي حددها القانون، مع بيان الأسباب الموجبة لذلك ومحل التفتيش المخصوص.

وسوف نعالج إجراء التفتيش بالنظر إلى إمكانية تفتيش العالم الرقمي والقيود التي ترد على فرقة التفتيش.

1- مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش:

يتكون الحاسب الآلي من مكونات مادية، مكونات منطقية، كما أن له شبكات اتصال بعدية سلكية ولا سلكية سواء على المستوى المحلي او المستوى الدولي.

1-1- مدى خضوع مكونات الحاسب المادية للتفتيش:

يخضع الولوج في المكونات المادية للحاسب بحثا عن شيء يتصل بجريمة معلوماتية وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبيها للإجراءات القانونية الخاصة بالتفتيش، وبعبارة أخرى فإن جواز التفتيش تلك

[1] منتدى جامعة قطر "كلية القانون": " مراحل إثبات الجريمة الإلكترونية" عن موقع:
Heard PHP?t=20845http://www.quatar.com/VB/show يوم الاطلاع (2020/05/29) على الساعة (11:37)

المكونات يتوقف على طبيعة المكان الموجودة فيه وهل هو مكان عام أم مكان خاص إذ أن لصفة المكان أهمية خاصة في مجال التفتيش فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيه تفتيش مسكنه وبنفس الضمانات المقررة قانونا في التشريعات المختلفة.[1]

ويجب التمييز داخل المكان الخاص بينما إذا كانت مكونات الحاسب منعزلة عن غيرها من الحياسب الأخرى ام انها متصلة بحاسب أو بنهاية طرفية terminal في مكان آخر كمسكن لا يخص مسكن المتهم فإذا كانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن، أما بالنسبة للاماكن العامة فإذا وجد شخص وهو يحمل مكونات الحاسب الآلي المادية او كان مسيطر عليها او حائز عليها، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص بنفس الضمانات والقيود المنصوص عليها في هذا المجال[2].

1-2-مدى خضوع مكونات الحاسب المعنوية للتفتيش:

اما عن تفتيش مكونات الحاسب المعنوية فقد ثار الخلاف بشأن جواز تفتيشها حيث يذهب رأي أنه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن المفهوم يمتد ليشمل البيانات الالكترونية بمختلف أشكالها.

وفي هذا المعنى نجد أن المادة 251 من قانون الاجراءات الجنائي اليوناني تعطى سلطات التحقيق إمكانية القيام (بأي شيء يكون ضروري لجمع وحماية الدليل) ويفسر الفقه اليوناني عبارة أي شيء بأنها تشمل بالضبط البيانات المخزنة أو المعالجة الكترونيا، ولذلك فإن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسب الآلي لا تشكل أي

[1] منتدى جامعة قطر، الموقع نفسه.

[2] شيباني مرجع سابق ص.31

مشكلة في اليونان إذ بمقدور المحقق أن يعطي أمرا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل في المحاكمة الجنائية[1].

وتمنح المادة 487 من القانون الجنائي الكندي سلطة إصدار إذن لضبط أي شيء طالما تتوفر الأسس معقولة للاعتقاد بأن الجريمة ارتكبت أو يشتبه بارتكابها أو ان هناك نية بأن يستخدم في. ارتكاب الجريمة أو أنه سوف ينتج دليلا على وقوع الجريمة.[2]

1-3-مدى خضوع شبكات الحاسب للتفتيش:

ويمكن في الفرض التمييز بين ثلاثة احتمالات:

الاحتمال الأول: اتصال حاسب المتهم بحاسب او نهاية طرفية موجودة في مكان آخر داخل الدولة:

يرى الفقه الألماني بشأن مدى امكانية امتداد الحق في التفتيش إذا تبين أن الحاسب أو النهاية الطرفية في جهاز المتهم متصلة بجهاز أو طرفية في مكان آخر مملوك لشخص غير المتهم، إنه يمكن أن يمتد التفتيش في هذه الحالة إلى سجلات البيانات التي تكون في موقع آخر استنادا إلى مقتضيات القسم 103 من قانون الاجراءات الجنائية الألماني[3].

كما نص مشروع قانون جرائم الحاسب الآلي في هولندا على جواز أن يمتد التفتيش إلى نظم المعلومات الموجودة في موقع آخر بشرط أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة (القسم الخامس من المادة 125) وذلك بمراعاة بعض القيود[4].

---

[1] Vassilaki (Irini) : computer crimes and other crimes against information techenologye in greece RI.D.P.1993, P, 371.

مشار اليه د. هلالي عبد الله احمد، تفتيش الحاسب الالي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة 1997، ص74.

[2] أمين فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية لكلية حقوق مصرية، الإسكندرية، مصر، 2008، ص 219، 224.

[3] KASPERSEN(W.K.Henrik) : computer crimes and other crimes against information technology in the netherlands .R.I.D.P.1993, p, 479.

[4] د. احمد هلالي، مرجع سابق، ص77.

الاحتمال الثاني: اتصال حاسب المتهم بحاسب او نهاية طرفية موجودة في مكان آخر خارج الدولة.

من المتصور طبقا لهذا الاحتمال أن يقوم مرتكبو الجرائم بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكات الاتصال البعيدة بهدف عرقلة سلطات الادعاء في جميع الأدلة، ولمواجهة هذا الاحتمال نص مشروع قانون جريمة الحاسب الآلي بهولندا أنه يجوز لجهات التحقيق مباشرة التفتيش داخل الاماكن وبما ينطوي عليه تفتيش نظم الحاسب المرتبطة حتى إذا كانت موجودة في دولة أخرى، ويشترط أن يكون هذا التدخل مؤقتا وان تكون البيانات التي يتم التفتيش عنها لازمة لإظهار الحقيقة (المادة 125)[1] .

الاحتمال الثالث: يسمح بالتصنت والأشكال الخاصة للمراقبة التليفونية في العديد من الدول.

حيث يجيز القانون الفرنسي الصادر في 10 يوليو 1991 اعتراض الاتصالات البعيدة بما في ذلك شبكات تبادل المعلومات، ويجوز لقاضي التحقيق في هولندا أن يأمر بالتصنت على شبكات اتصالات الحاسب إذا كانت هناك جرائم خطيرة متورطا فيها المتهم وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات، وفي الولايات المتحدة الأمريكية يجوز اعتراض الاتصالات الالكترونية بما فيها شبكات الحاسب بشرط الحصول على إذن تفتيش صادر من القاضي.

2-ضوابط تفتيش نظم الحاسب الآلي:

يمكن تقسيم ضوابط تفتيش نظم الحاسب الآلي إلى نوعين موضوعية شكلية:

2-1-الضوابط الموضوعية لتفتيش نظم الحاسب الآلي: وتنحصر هذه الضوابط في:

وقوع جريمة الكترونية: والجريمة الالكترونية هي كما سبق القول وبشكل عام كل فعل غير مشروع مرتبط باستخدام الحاسب الآلي لتحقيق أغراض غير مشروعة. وهناك العديد من التشريعات التي حرصت على

[1]DURHAM(COLO) : the emergin structures of criminal information law :tracing the contours of new pardigm geenral report for the a.i.d.pcollwuiumR.I.D.P1993.P115.

استحداث نص خاص كما هو الحال بالنسبة للأنظمة القانونية التي تم التطرق سابق في إطار الجهود الدولية، سواء المنفردة منها أو الجماعية في مواجهة هاته الجريمة العصرية.

– تورط شخص او أشخاص معينين في ارتكاب الجريمة المعلوماتية أو الاشتراك فيه:

ينبغي أن تتوفر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة الالكترونية، سواء بوصفه فاعلا لها أو شريكا فيها وفي مجال الحاسب الآلي يمكن القول بأن تعبير الدلائل الكافية يقصد به مجموعة من المظاهر أو الأمارات المعنية التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة، كذلك على خبرة وحرفية القائم بالتفتيش والتي تؤيد مسبة الجريمة المعلوماتية إلى شخص معين سواء بوصفه فاعلا أو شريكا .[1]

وتشمل المكونات المادية للحاسب وحدة الإدخال ووحدة الذاكرة الرئيسية ووحدة الحساب والمنطق ووحدات الإخراج وأخيرا وحدات التخزين الثانوي.

وتنقسم المكونات المعنوية للحاسب الآلي إلى الكيانات المنطقية الأساسية أو برامج النظام والكيانات المنطقية التطبيقية أو برامج التطبيقات بنوعيها برامج التطبيقات سابقة التجهيز وبرامج التطبيقات طبقا لاحتياجات العميل، ويستلزم الحاسب بمكوناته سالفة الذكر مجموعة من الأشخاص لديهم خبرة ومهارة في تقنية نظم المعلومات وهم مشغلو الحاسب وخبراء البرامج، سواء كانوا مخططي برامج تطبيقات أم كانوا مخططي برامج نظم ومحليين ومهندي الصيانة ومديري النظم المعلوماتية[2].

[1] عبد الله حسين محمود، " إجراءات جمع الادلة في مجال جريمة سرقة المعلومات" عن موقع:
ID=148.http://www.arablawinfo.com/research-search.asp?Validate=articles ، يوم الاطلاع :
2020/05/28 ، على الساعة (10:39)

[2] أسامة أحمد المناعسة، جلال محمد الزغبي، صايل فاضل الهواوشة، " جرائم الحاسب الآلي والانترنت"، دار وائل للنشر والتوزيع، الطبعة الأولى، عمان، الاردن ،2001، ص، ص272-276.

2-2-الضوابط الشكلية لتفتيش نظم الحاسب الآلي:

ويمكن إجمال مثل هاته الضوابط فيما يلي:

الأسلوب الآلي لتنفيذ التفتيش في نظم الحاسب الآلي حيث الريادة في ذلك كانت للنظام الأمريكي وذلك على النحو التالي:

تقتحم قوات الشرطة القضائية المكان بصورة سريعة ومن كافة منافذه في آن واحد وذلك باستخدام القدر الأعظم من القوة، بافتراض أن هذا التكتيك يقلل من احتمالية وقوع إصابات بين صفوف رجال الشرطة.

يتم إبعاد سائر المشتبه فيهم عن كافة أنظمة ومعدات الكمبيوتر المتواجدة في المكان على الفور حتى لا يتمكنوا من تشويه أو تدمير أي دليل الكتروني، ويتم إدخال سائر المشتبه فيهم إلى غرفة لا توجد بها أية أجهزة كمبيوتر، ودائما ما تكون غرفة المعيشة ويوضعوا تحت حراسة مشددة، وفي هذه الخطوة يتم تقديم التفتيش الصادر من النيابة إليهم ويتم تحذيرهم بأن كافة أقوالهم ستحسب عليهم منذ هذه اللحظة وقد تؤخذ بمثابة دليل إدانة ضدهم، ودائما ما سنجد لدى العديد منهم الكثير من الحديث وخاصة إذا ما كانوا أولياء أمور غافلين عن حقيقة ما يحدث بمنزلهم، وفي مكان ما من المنزل سنجد النقطة الساخنة جهاز كمبيوتر متصل بخط تلفون أو ربما نجد أكثر من جهاز وأكثر من خط في المنزل الواحد، وعادة ما تكون هذه النقطة الساخنة داخل غرف النوم الخاصة بأحد الأبناء المراهقين.

تعهد النقطة الساخنة لفريق يضم إثنين من العملاء (مكتشف ومسجل)، ويجب أن يكون المكتشف من بين العملاء الذين تم تدريبهم تدريبا متقدما على نظم المعلومات، وغالبا ما يقوم بهذا الدور العميل المعني بالقضية والذي عاصرها منذ البداية واستصدار إذن التفتيش الخاص بها من القاضي، فهذا الشخص يعرف تماما الشيء او الأشياء التي يبحث عنها ويتفهم طبيعتها تماما ولن نتجاوز إذا ما قلنا إنه هو الذي يقوم بفتح الأدراج والبحث عن الديسكات والملفات وحاويات الأسطوانات ...الخ.

– **فريق التفتيش:** هد الفريق هو المعني بإجراءات التحقيق، وهو جزء داخل فريق الإغارة الذي يضم بجانب فريق التفتيش والضبط رجال الحراسات والأمن وقوات الحماية والتأمين ورجال المباحث والمراقبة السرية والمعاونين من العمال والسائقين وخبراء مسرح لجريمة العادية الملائمين لجريمة موضوع التحقيق.

ثالثا: الشهادة في مجال الجريمة المعلوماتية

الشهادة هي الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى متهم او براءته منها، وللشهادة في مجال الاجراءات أهمية بالغة لأن الجريمة ليست تصرفا قانونيا ولكنها عمل غير مشروع يجتهد الجاني في التكتم عند ارتكابه وبحرص على إخفائه عن الناس[1].

كما أن سماع الشهود هو كسائر إجراءات التحقيق من الأمور التقليدية للمحقق فله ان يسمع الشهود او يستغني عنهم فإذا قرر سماعهم فهو الذي يحدد من يجب الاستماع إليه ومن يمكن الاستغناء عنه، والأمر متروك إلى فطنة المحقق والأصل أن يطلب الخصوم سماع من يرون من الشهود، غير أن للمحقق أن يجيبهم إلى طلبهم أو يرفضه وله أن يدعو لشهادة من يقدر أن لشهادته أهمية بل له أن يسمع شهادة أي شاهد يتقدم من تلقاء نفسه، ومن المبادئ المستقرة أن الشاهد لا يرد ولو غلب على الظن انه لن يتحرى الصدق في شهادته سواء كان ذلك راجعا لانحطاط في خلقه أو لوجود صلة مودة أو لعداوة بينه وبين المتهم تجعله يميل له او ضده.

1– المقصود بالشاهد في الجريمة المعلوماتية:

يعتبر الشاهد في الجريمة المعلوماتية هو الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي، الذي تكون لديه معلومات جوهرية او هامة لازمة للولوج في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن ادلة الجريمة داخله، ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي وذلك تمييزا عن الشاهد التقليدي ويشمل الشاهد المعلوماتي بهذا المفهوم عدة طوائف من اهمها:

[1] منتدى جامعة قطر "كلية القانون"، " مراحل إثبات الجريمة الإلكترونية"، الموقع السابق.

1-1-القائم على تشغيل الحاسب الآلي:

وهو المسؤول عن تشغيل جهاز الحاسب الآلي والمعدات المتصلة به، ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز واستخدام لوحة المفاتيح في إدخال البيانات كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج.

1-2-المبرمجون :وهم الأشخاص المتخصصون في كتابة البرامج ويمكن تقسيمهم إلى فئتين:

- الفئة الأولى : وهم مخططو برامج التطبيقات.
- الفئة الثانية : هو مخططو برامج النظم.

حيث يقوم مخططو برامج التطبيقات بالحصول على خصائص ومواصفات النظام من محلل النظم ثم يقوم بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات، أما مخططو برامج النظم فيقومون باختبار وتعديل وتصحيح برامج نظام الحاسب الداخلية أي أنه يقوم بالوظائف الخاصة بتجهيز الحاسب بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والإخراج ووسائط التخزين بالإضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج .[1]

1-3-المحللون :المحلل وهو الشخص الذي يحلل ويقوم بتجميع البيانات ويقوم بتجميع بيانات نظام معين، ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية من هذه الوحدات، كما يقوم بتتبع البيانات داخل النظام عن طريق ما سمي بمخطط تدفق البيانات واستنتاج الاماكن التي يمكن ميكنتها بواسطة الحاسب.

[1] منتدى قانون نت، منتدى القضايا الجنائية، خصوصية جرائم الحاسوب والأنترنت، عن موقع https://democraticac.de/?p=35426 يوم الاطلاع: 2020/05/30 على الساعة (16:36).

2 منتدى قانون نت، منتدى القضايا الجنائية، خصوصية جرائم الحاسوب والأنترنت، نفس الموقع.

2- التزامات الشاهد المعلوماتي:

يتوجب على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله، والسؤال الذي يطرح نفسه هل يلتزم الشاهد بطبع الملفات والإفصاح عن كلمات المرور والشفرات؟

هناك اتجاهان بهذا الصدد:

- **الاتجاه الأول:** ويرى أنه ليس من واجب الشاهد وفقا للالتزامات التقليدية للشهادة أن يقوم بطبع ملف البيانات او الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة، ويميل إلى هذا الاتجاه الفقه الألماني حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب .

وكذلك لا يجوز في تركيا إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية او كشف شفرات تشغيل البرامج المختلفة.

- **الاتجاه الثاني** : ويرى أنصار هذا الاتجاه أن من بين الالتزامات التي يتحمل بها الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة، حيث يرى اتجاه في الفقه الفرنسي أن القواعد العامة في مجال الإجراءات تحتفظ بسلطاتها في مجال الإجراءات المعلوماتية، ومن ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهاداتهم (المواد 62،109،138) من قانون الاجراءات الجنائية الفرنسية، ومن ثم يجب عليهم الإفصاح عن كلمات المرور السرية التي يعلمونها، ولكن رفض إعطاء المعلومات المطلوبة غير معاقب عليه جنائيا إلا في مرحلة التحقيق والمحاكمة[1].

[1] منتدى قانون نت، منتدى القضايا الجنائية، خصوصية جرائم الحاسوب والأنترنت، نفس الموقع.

[2] منتدى قانون نت، منتدى القضايا الجنائية، نفس المنتدى.

رابعا: الخبرة في مجال الجريمة المعلوماتية

– ندب الخبير أو مبررات ندب الخبير وإجراءاته : يستلزم على المحقق في بعض الأحيان الاستعانة بالخبير لإيضاح مسألة تستعصي ثقافته العامة عن فهمها، كتحديد سبب الوفاة أو ساعتها أو رفع بصمة وجدت في مكان الجريمة أو فحص سيارة لبيان ما فيها من خلل وتكتسب الخبرة أهمية بالغة في مجال الجريمة المعلوماتية نظرا لأن الحاسبات وشبكات الاتصال بينها على أنواع ونماذج متعددة، كذلك فإن العلوم والتقنيات المتصلة بها تنتمي إلى تخصصات عملية وفنية دقيقة ومتنوعة والتطورات في مجالها سريعة ومتلاحقة، لدرجة قد يصعب معها على المتخصص تتبعها واستيعابها، ويمكن القول بصفة عامة بأنه لا يوجد حتى الآن خبير لديه معرفة متعمقة في سائر أنواع الحسابات وبرامجها وشبكتها، كذلك لا يوجد خبير قادر على التعامل مع كافة انماط الجرائم التي تقع عليها أو ترتكب بواسطتها[1].

لذا ترك المشرع للمحقق الحرية الكاملة في هذا الشأن ليمكنه من كشف الحقيقة بالسرعة اللازمة وبالطريقة التي يراها مناسبة، وللمحقق في أي وقت إلى أن ينتهي التحقيق أن يندب من يأنس فيه الكفاءة الفنية اللازمة للاستعانة بخبرته.

وندب الخبير من سلطات المحقق فليس في القانون ما يلزمه بالاستجابة للمتهم ولا لغيره من الخصوم إذا طلبوا ندب خبير، كما أنه يحدد للخبير مهمته والميعاد الذي يقدم فيه تقريره وعليه أن يحلفه اليمين على أن يبدي رأيه بالذمة وهذا الإجراء جوهري يترتب على إغفاله بطلان عمل الخبير، والأصل أن يباشر الخبير عمله في حضور المحقق وتحت إشرافه والاستثناء يتم ذلك في غيابه.

[1] PHILIP M, stanely computer crime invetigation and investigators computer & security North Holland1986, pp.310-311.

. مشار اليه في: د محمد فريد رستم، مرجع سابق.

وللخصوم حق الحضور أثناء عمل الخبير ويجوز مع ذلك أن يباشر الخبير عمله في غياب الخصوم وأن يمنعهم كذلك من الحضور إذا كان للمنع سبب، ويعد الحصول على المستندات خلال عملية التفتيش أمرا سهلا حيث يمكن التعرف عليها بالرؤية ولن يحتاج المحقق لأي مساعدة من قبل الخبراء، وهذه المستندات مثل :

أدلة عمل النظام، سجلات إدارة الكمبيوتر، وثائق البرامج، السجلات، صيغ مدخلات البيانات والبرامج، وكذلك صيغ مخرجات الكمبيوتر المطبوعة ويتم التخطيط على هذه المستندات ويمكن تحديدها ما إذا كانت كاملة، أصلية، او صورا من خلال استجواب القائمين على حفظها .[1]

وبالطبع فإن البحث عن المعلومات داخل جهاز الكمبيوتر ذاته يعد أمرا بالغ التعقيد ويحتاج إلى وجود خبير، وأهم المسائل التي يستعان فيها بالخبرة في مجال الجرائم المعلوماتية هي:

1- تحديد وصف الحاسوب:

- تركيب الحاسوب وصناعته وطرازه ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها، بالإضافة إلى الأجهزة الطرفية الملحقة به وكلمات المرور أو السر ونظام التشفير ... الخ.

- طبيعة بيئة الحاسب او الشبكة من حيث تنظيم ومدى تركيز او توزيع عمل المعالجة الآلية ونمط وسائط الاتصالات وتردد موجات البث وامكنة اختزانها.

- الموضع المحتمل لأدلة الإثبات والشكل أو الهيئة التي تكون عليها.

- أثر التحقيق من الوجهة الاقتصادية والمالية على المشاركين في استخدام النظام[2].

[1] عبد الله حسين محمود، "إجراءات جمع الادلة في مجال جريمة سرقة المعلومات" عن موقع:
ID=148.http://www.arablawinfo.com/research-search.asp?Validate=articles الموقع السابق.

[2] عبد الفتاح البيومي الحجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي (دراسة قانونية متعمقة في القانون المعلوماتي)، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، مصر، 2006، ص، 304 ،305.

2- بيان طرق استخدامه:

-كيف يمكن عند الاقتضاء عزل النظام المعلوماتي دون إتلاف الأدلة او تدميرها أو إلحاق ضرر بالأجهزة ؟

-كيف يمكن عند الاقتضاء نقل أدلة الإثباتات إلى أوعية ملائمة بغير أن يلحقها تلف ؟

-كيفية تجسيد الأدلة في صورة مادية بنقلها إذا امكن إلى أوعية ورقية يتاح للقاضي مطالعتها وفهمها، مع إثبات أن المسطور على الورق مطابق للمسجل على الحاسب او النظام أو الشبكة أو الدعامة الممغنطة ؟

خامسا: الضبط في مجال الجريمة الالكترونية

المقصود بالضبط في قانون الاجراءات وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو التحقيق، وتتحد طبيعته بحسب الطريقة التي يتم بها وضع اليد على الشيء المضبوط فإذا كان الشيء وقت ضبطه في حيازة شخص واقتضى الأمر تجريده من حيازته كان الضبط بمثابة إجراء تحقيق أما إذا كان الاستيلاء عليها دون الاعتداء على حيازة قائمة فإنه يكون بمثابة إجراء استدلال[1].

1- محل الضبط:[2]

فالضبط بطبيعته وبحسب تنظيمه القانوني وغايته لا يرد إلا على الأشياء أما الأشخاص فلا يصلحون محلا للضبط بالمعنى الدقيق، وإذا كان قانون الاجراءات يتحدث في بعض التصرف عن ضبط الأشخاص وإحضارهم فإنه يعني القبض عليهم وإحضارهم، والقبض نظام قانوني يختلف عن ضبط الأشياء.

ولا يفرق القانون في مجال الضبط بين المنقول والعقار فكلاهما يمكن ضبطه كذلك يستوي أن يكون الشيء المضبوط مملوكا للمتهم او لغيره، والقاعدة أن الضبط لا يرد إلا على شيء مادي أما الأشياء المعنوية فلا تصلح بطبيعتها محلا للضبط والشرط اللازم لصحته ان يكون مفيدا في كشف الحقيقة فكل ما يحقق هذه الغاية يصح ضبطه.

[1] عبد العال الديربي، مرجع سابق، ص320.
[2] عبد الفتاح البيومي الحجازي، المرجع السابق، ص 305.

والأدلة المادية التي يجوز ضبطها في الجريمة المعلوماتية والتي لها قيمة خاصة في إثبات الجرائم الحاسب الآلي ونسبتها إلى المتهم هي:

1-1- الورق : اغلب الجرائم الواقعة على المال او على جسم الإنسان تترك خلفها قدرا كبيرا من الأوراق والمستندات الرسمية منها والخاصة، إلا أن وجود أجهزة الحاسب يجعل كثيرا من المعلومات يتم حفظها غي الحاسب الآلي، مما قلل حجم الأوراق والملفات ومع ذلك نجد أن الكثيرين يقومون بطباعة المعلومات لأغراض المراجعة او التأكد من الشكل العام للمستند أو الرسالة أو الرسومات موضوع الجريمة، وأجهزة الحاسب الآلي والطابعات المتطورة ذات السرعة الفائقة تطبق قدرا كبيرا من الأوراق في وقت قصير، عليه يعتبر الورق من الادلة التي ينبغي الاهتمام بها في البحث وتفتيش مسرح الجريمة والورق أربعة أنواع:

- اوراق تحضيرية يتم إعدادها بخط اليد كمسودة او تصور للعملية التي يتم برمجتها.
- أوراق تالفة تتم طباعتها للتأكد ومن ثم إلقاؤها في سلة المهملات.
- أوراق أصلية تتم طباعتها والاحتفاظ بها كمرجع أو لأغراض تنفيذ الجريمة.
- أوراق أساسية وقانونية محفوظة في الملفات العادية او دفاتر الحسابات وتكون لها علاقة بالجريمة، خاصة عند تلقيها أو تزوير بياناتها لتنفيذ جريمة الحاسب الآلي.

1-2-جهاز الحاسب الآلي: للقول بأن هناك جريمة معلوماتية يجب ان تقع على حاسب آلي، ولأجهزة الحاسب الآلي أشكال وأحجام وألوان مختلفة، وخبير الحاسب الآلي يستطيع أن يتعرف على الحاسب الآلي ومواصفاته بسرعة فائقة، كما يستطيع تمييزه عن الأجهزة الالكترونية الأخرى وتحديد أسلوب التعامل معه في حالة الضبط والتحرير.[1]

[1] عبد الفتاح البيومي الحجازي، المرجع السابق، ص 306.

1-3-ملحقات الحاسب الآلي: من السهل التعرف على جهاز الحاسب الشخصي الذي أصبح مألوفا اليوم فهو يتكون من وحدة المعالجة المركزية، لوحة المفاتيح، والشاشة، ومع التطورات السريعة التي يمر بها الحاسب الآبي نجد إضافات جديدة مثل المودم والماوس والسماعات و "السير فر"، وإذا كنا بصدد الحديث عن الأجهزة الكبير فإننا نجد أن أشكالها تتغير باستمرار خاصة من حيث الحجم والهيكل، ومن الضروري إطلاع العاملين في مجال التحقيق على مختلف أجهزة الحاسب الآلي فور ظهورها.

1-4-أقراص الليزر: مع جهاز الحاسب الآلي للشخص الطبيعي والشخص المعنوي نجد قدرا كبيرا من أقراص الليزر، علاوة على أن مراكز الحاسب الآلي في الأشخاص المعنوية نجد فيها الآلاف من الأقراص قد تكون على غلاف القرص بيانات توضح محتويات كل قرص وبمعرفة خبير يقدم الدليل أمام المحكمة، وقد تجد في مكان ما أقراص الليزر ولا تجد معها أجهزة حاسب آلي ومع ذلك يعد جزءا من جريمة الحاسب الآلي متى كانت محتوياتها عنصرا من عناصر الجريمة.

1-5-الشرائط الممغنطة: وتستعمل الشرائط الممغنطة عادة للحفظ الاحتياطي وقد تكون في مكان بعيد آمن، كما يقوم البعض بإيداعها في خزائن البنوك التجارية او مراكز التوثيق الحكومية الآمنة[1] .

الفرع الثاني: الدليل الرقمي في الجريمة المعلوماتية.

يتميز الدليل الرقمي بصفة الحداثة، فهو من الأدلة الحديثة التي أفادها التطور التقني وهو ايضا ذو طبيعة خاصة من حيث الوسط الذي ينشأ فيه والطبيعة التي يبدو عليها، ولذي فإننا سنتطلع في هذا المطلب إلى التعريف بالدليل الرقمي.

[1] عبد الفتاح البومي الحجازي، المرجع السابق، ص 306-307 .

– التعريف بالدليل الجنائي بشكل عام :

في اللغة: هو المرشد، وما يتم به للإرشاد، وما يستدل به، والدليل هو الدال وجمع الأدلة [1] و كذلك يعني تأكيد الحق بالبينة والبينة هي الدليل أو الحجية.

في المصطلح القانوني: هو الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها وما المقصود بالحقيقية بهذا الصدد: هو كل ما يتعلق بالإجراءات والوقائع المعروضة عليه بإعمال حكم القانون عليها.[2]

أولا: ماهية الدليل الرقمي

يقصد الدليل المأخوذ من أجهزة الكمبيوتر و هو يكون في شكل مجالات ونبضات مغناطيسية أو كهربائية ممكن تجميعها و تحليلها باستخدام برامج التطبيقات و تكنولوجيا و هي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة نفاذ و تطبيق القانون [3] ويعرف الدليل الرقمي بأنه:

مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها لاستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية.

---

[1] جميل صليبا، المعجم الفلسفي، دار الكتاب اللبناني، ط 1، بيروت، لبنان، 1980، ص 23،

[2] ناصر إبراهيم محمد زكي، سلطة القاضي الجنائي في تقدير الأدلة "دراسة مقارنة"، رسالة دكتوراه جامعة الأزهر، كلية الشريعة والقانون، مصر، 1978، ص 211.

[3] ممدوح عبد الحميد عبد المطلب، وزبيدة محمد قاصي، عبد الله عبد العزيز، النموذج المقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، منشور ضمن أعمال مؤتمر «الأعمال المصرفة والإلكترونية" نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة التجارة والصناعة دبي في الفترة من 10-2003/05/12، المجلد الخامس، ص 2273.

وترجع تسمية الدليل الرقمي لأن البيانات داخل الوسط الافتراضي سواء كانت صور أو تسجيلات أو نصوص تأخذ شكل أرقام على هيئة الرقمين (1 أو 0) و يتم تحويل هذه الأرقام عند عرضها لتكون في شكل صور أو مستند أو تسجيل[1] .

ثانيا: خصائص ومميزات الدليل الرقمي.

– خصائص الدليل الرقمي:

1-يعتبر الدليل الرقمي دليلا غير ملموس أي هو ليس دليلا ماديا (فهو يكون في مجالات مغناطيسية أو كهربائية)

2-يعتبر الدليل الرقمي من قبيل الأدلة الفنية أو العلمية[2]

3-إن فهم مضمون الدليل الرقمي يعتمد على استخدام أجهزة خاصة بتجميع وتحليل محتواه ولذلك ما لا يمكن تحديد وتحليل محتواه بواسطة تلك الأجهزة ويمكن اعتباره دليلا رقميا.

– مميزات الدليل الرقمي:

1-يتصف الدليل الرقمي بصعوبة محوه او تحطيمه، اد حتى في حالة محاولة اصدار امر بإزالة دليل فمن الممكن اظهاره من خلال ذاكرة الالة التي تحتوي دلك الدليل.

2-ان محاولة الجاني محو الدليل الرقمي بدأتها تسجل عليه كدلك، حيث ان قيامه بدلك يتم تسجيله بذاكرة الالة وهو ما يمكن استخراجه واستخدامه كدليل ضده.

3-ان الطبيعة الفنية دليل رقمي تمكن اخضاعه لبعض البرامج والتطبيقات للتعرف على ما اذا كان قد تعرض للعبث والتحريف.

[1] عبد الفتاح بيومي الحجازي، دليل الرقمي والتزوير في جرائم الكمبيوتر والأنترنت، دراسة معمقة في جرائم الحاسب الآلي والأنترنت، بهجات للطباعة والتجليد، مصر، 2010، ص 278.

[2] علي محمود عي حمودة، الأدلة المتحصلة للوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مقدم ضمن أعمال مؤتمر العلمي الأول حول جوانب القانونية والأمنية والعمليات الإلكترونية نضمته أكاديمية شرطة دبي، في الفترة من 26 إلى 2003/04/28 دبي، ص 22.

ثالثا: مشروعية الدليل الرقمي

المراد بمشروعية الدليل الرقمي هو ان يكون الدليل معترف به، بمعنى ان يكون القانون يجيز للقاضي الاستناد اليه لتكوين عقيدته للحكم بالإدانة، فهناك اتجاهان رئيسان، الاول نظام الادلة القانونية، والثاني نظام الاثبات الحر.

1 –نظام الادلة القانونية.

حسب هدا النظام فان المشرع هو الدي يحدد حصرا للأدلة التي يجوز للقاضي اللجوء اليها في الاثبات ، كما حدد القيمة الاقناعية لكل دليل بحيث يقتصر دور القاضي على مجرد فحص دليل للتأكد من توافر الشروط التي حددها القانون[1] ، فلا سبيل للقاضي في تقدير القيمة الاقناعية للدليل ، و لدا سمي هدا النظام بنظام الاثبات القانوني او المقيد حيث ان القانون قيد القاضي بقائمة من الادلة التي حددت قيمتها الاثباتية ، و هدا النظام ينتمي للنظم دات الثقافة الانجلوساكصونية ، مثل المملكة المتحدة " بريطانيا" و الولايات المتحدة الامريكية ، ولدا فان النظم التي تتبنى هدا النظام لا يمكن في ظلها الاعتراف بالدليل الرقمي بأية قيمة اثباتية ما لم ينص القانون عليه صراحة ضمن قائمة ادلة الاثبات.

وتطبيقا لهدا الفهم نص قانون الاثبات في المواد الجنائية البريطاني على قبول الدليل الرقمي و حدد قيمته الاثباتية اتفاقا و طبيعة النظام القانوني في بريطانيا .[2]

و يعاب على نظام الاثبات القانوني ان من شانه تقييد القاضي على نحو يفقده سلطته في الحكم مما يتفق مع الواقع ، فيحكم في الكثير من الاحيان مما يخالف قناعته التي تكونت لديه من ادلة لا يعترف بها دلك فيصبح القاضي كالألة في اطاعته لنصوص القانون و لذلك فإن هذا النظام بدا ينحصر نطاقه حتى في الدول التي تعتبر أكثر إقناعا لها، فنجد بريطانيا مثلا قد بدأ تخفف من علوائه، حيث ظهر فيها ما يعرف بقاعدة الإدارة دون أدنى

[1] هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر ،1999، ص 49.

[2] علي محمود علي حمودة، مرجع سابق ذكره، ص 30.

شك و التي مفادها أن القاضي يستطيع أن يكون عقيدته من اي دليل إن لم يكن من ضمن الأدلة المنصوص عليها متى كان هذا الدليل قاطعا في دلالته .[1]

2-نظام الإثبات الحر:

استعملت الأنظمة اللاتينية نظام الإثبات الحر، و وفق لهذا النظام يتمتع القاضي الجنائي في تكوين قناعته فله أن يبني هذه القناعة على اي دليل و إن لم يكن منصوص عليه بل إن المشرع في هذا النظام لا يحفل بالنص على أدلة الإثبات، فكل الأدلة تتساوى قيمتها الإثباتية في نظر المشرع، و القاضي هو الذي يختار من بين ما يطرح عليه و ما يراه صالحا للوصول إلى الحقيقة و هو في ذلك يتمتع بمنطلق الحرية لقبول الدليل أو رفضه إذا لم يطمأن إليه، فالمشرع في هذا النظام لا يتدخل في تحديث القيمة الإقناعية للدليل فعلى الرغم من توفر شروط الصحة في الدليل إلا أن القاضي يملك أن يرده تحت مبرر عدم الاقتناع، و لذلك فالقاضي في مثل هذا النظام يتمتع بدور إيجابي في مجال الإثبات في مقابل انحصار دور المشرع .[2]

في هذا النظام لا تثور مشكلة مشروعية الدليل الرقمي من حيث الوجود، على اعتبار أن المشرع لا يعهد عنه سياسة النص على قائمة أدلة الإثبات ولذلك فإن مسألة قبول الدليل الرقمي لا ينال منها سوى مدى اقتناع القاضي به إذا كان هذا النوع من الأدلة يمكن إخضاعه بالتقدير القضائي.

رابعا: حجية الدليل الرقمي أمام القضاء الجنائي.

لا يكفي مجرد الحصول على الدليل الرقمي وتقديمه للقضاء لاعتماده كدليل للإدانة إن الطبيعة الخاصة بالدليل الرقمي تمكن من العبث بمضمونه على نحو يحرف الحقيقة دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث، فضلا عن ذلك فإن نسبة الخطأ في إجراءات الحصول على الدليل صادقة في الإخبار عن الحقيقة تبدو

[1] هلالي عبد الإله أحمد، حجية المخرجات، مرجع سابق، ص 91.

[2] هلالي عبد الإله أحمد، حجية المخرجات، مرجع سابق، ص 29 وما بعدها.

عالية في مثل هذا النوع من الأدلة، ولذلك تثور فكرة الشك في مصداقياتها كأدلة الإثبات الجنائي، فهل من شأن ذلك فاستبعاد الدليل الرقمي من دائرة الإثبات الجنائي لتعارضه وقرينة البراءة؟

في ضل النظم القانونية التي تعتمد النظام اللاتيني في الإثبات –كالنظام القانون الليبي – فإن القاضي يملك سلطة واسعة في تقديم الدليل من حيث قسمته التدليلة، فللقاضي قبول الدليل أو رفضه وهو يعتمد في ذلك على مدى اقتناعه الشخصي بذلك الدليل وهذا المعنى هو ما نصت عليه المادة 275 من قانون الإجراءات الجنائية الليبي.[1]

سلطة القاضي الجنائي في تقدير الدليل لا يمكن ان يتوسع في شانها بحيث يقال إن هذه السلطة تمتد لتشمل الأدلة العلمية، فالقاضي بثقافته القانونية لا يمكن إدراك الحقائق المتعلقة بأصالة الدليل الرقمي فضلا عن ذلك فإن هذا الليل يتمتع من حيث قوته التدليلية بقيمة غثباتية قد تصل إلى اليقين، فهذا هو شأن الأدلة العلمية عموما ولكن هذا لا يناقض ما سبق أن قدمناه من أن الدليل الرقمي هو موضع شك من حيث سلامته من العبث ومن ناحية صحة الإجراءات المتعبة في الحصول عليها من ناحية أخرى حيث يشك في سلامة الدليل الرقمي من ناحيتين:

1–الدليل الرقمي من الممكن خضوعه للعبث للخروج به من نحو يخالف الحقيقة ومن ثم فقد يقدم هذا الدليل معبرا عن واقعة معينة صنع اساسا لأجل التعبير عنها خلافا للحقيقة، وذلك دون أن يكون في استطاعة غير المتخصص إدراك ذلك العبث فالتقنية الحديثة تمكن من العبث بالدليل الرقمي بسهولة ويسر بحيث يظهر وكأنه نسخة أصلية في تعبيرها عن الحقيقة.

[1] أحمد الصادق الجهاني، محاضرات ألقيت على طلبة الدراسات العليا، كلية القانون، جامعة قار يونس، 2003–2004، غير منشور –تنص المادة 275 على أنه: "يحكم القاضي في الدعوة حسب العقيدة التي تكونت لديه بكامل حريته، ومع ذلك لا يجوز له أن يبلي حكمه على إي دليل لم يطرح أمامه في الجلسة «.

2-إذا كانت نسبة الخطأ الفني في الحصول على الدليل الرقمي نادرة للغاية إلا أنها تضل ممكنة، ويرجع الخطأ في الحصول على الدليل الرقمي لسببين:

- الخطأ في استخدام الأداة المناسبة في الحصول على الدليل الرقمي ويرجع ذلك الخلل في الشفرة المستخدمة أو بسبب استخدام مواصفات خاطئة.

- الخطأ في استخلاص الدليل، ويرجع ذلك إلى اتخاذ قرارات لاستخدام الأداة تقل نسبة صوابها عن 100 % ويحدث هذا غالبا بسبب وسائل الاختزال البيانات أو بسبب معالجة البيانات بطريقة تختلف عن الطريقة الأصلية التي تم تقيمها.

ومن ذلك فإننا نخلص إلى أن الشك في الدليل الرقمي لا يتعلق بمضمونه كدليل، وإنما بعوامل مستقلة عنه ولاكنها تؤثر في مصداقيته

المطلب الثاني: المكافحة الإجرائية في القانون الجزائري

اقتدى المشرع الجزائري بالمشرعين الذين سبقوه، فسارع لمواكبة هذا التطور الذي لحق الجريمة بمكافحتها من الناحية الإجرائية وذلك بتعديل بعض المواد في قانون الإجراءات الجزائية وإصدار قوانين خاصة وجديدة في مجال الإجراءات.

الفرع الأول: المكافحة الإجرائية في القانون 04/09

نظم المشرع الجزائري في القانون رقم 04/09 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]، أحكاما جديدة وخاصة بمعالجة الجريمة المعلوماتية تتماشى والتطور الذي لحق بهذه الجريمة، من هذه القواعد ما نص عليه في المادة الثالثة منه التي تضمنت الإجراءات الجديدة التي تتطلبها التحريات والتحقيقات القضائية من ترتيبات تقنية،[1] الهدف منها هو:

[1] قانون رقم 09-04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 اوت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته ومكافحتها.

– مراقبة الاتصالات الإلكترونية وتجميعها، حيث نجد أن المشرع الجزائري قد تبنى هذا الإجراء رغم ضمانه لسرية المراسلات والاتصالات بكل أشكالها بنص المادة39 من الدستور الجزائري نظرا لخطورة بعض الجرائم المعلوماتية المحددة حصرا [2].

– تسجيل الاتصالات الإلكترونية في حينها .

– القيام بإجراءات التفتيش والحجز للمنظومة المعلوماتية .

كما يبين القانون 04/09 في مادته الرابعة الحالات التي تسمح بتطبيق الإجراء الجديد المتمثل في مراقبة الاتصالات الإلكترونية وذلك على سبيل الحصر وهذه الحالات هي:

– الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

– في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني[3].

– مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الالكترونية.

– في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة تنص المادة 16 من القانون 09/ 04 على إمكانية تبادل المساعدات القضائية على المستوى الدولي لنجاح عمليات التحقيق والتحريات لمكافحة الجرائم المعلوماتية.[4]

---

[1] هلالي عبد الله أحمد، تفتيش نظام الحاسب الآلي وضمانات متهم المعلومات، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، ص 121.

[2] المادة 39 من دستور الجزائري 1996.

[3] مادة 4 من قانون رقم 09-04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 اوت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته ومكافحتها، جريدة الرسمية، عدد47.

[4] طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير، في القانون الجنائي، جامعة الجزائر 1، كلية الحقوق، 2012/2011، ص130.

كما أن المادة 18 من القانون 04/09 [1]قد بينت الحالات التي لا تجوز فيها عملية المساعدة القضائية الدولية وحددتها بالحالات التالية:

- إذا كان فيها مساس بالسيادة الوطنية .

- إذا كان فيها مساس بالنظام العام.

أما المادة الخامسة من القانون 04/09 [2]فهي تبين إجراءات التفتيش للمنظومة المعلوماتية يقصد بالتفتيش في مجال الجرائم المعلوماتية هو التفتيش المنصوص عليه في قانون الإجراءات الجزائية، وحتى وان اختلف مضمونه عن التفتيش العادي بحيث يجب توفر شروط التفتيش المنصوص عليها في المادة 45 من قانون الإجراءات الجزائية مع مراعاة أحكام الفقرة الأخيرة منها لأننا بصدد جرائم معلوماتية.

غير أن القانون 04/09 أجاز إجراء التفتيش على المنظومة المعلوماتية عن بعد وهذا إجراء جديد بحيث يمكن الدخول إليها دون إذن صاحبها بالدخول في الكيان المنطقي للحاسوب، للتفتيش عن أدلة في المعلومات التي يحتوي عليه هذا الأخير، وهي شيء معنوي غير محسوس، كما أجاز إفراغ هذه المعلومات على دعامة مادية أو نسخها للبحث عن الدليل فيها.[3]

كما نص المشرع الجزائري في الفقرة الأخيرة من المادة الخامسة من القانون 04/09 [4]على إجراء أخر يسهل عملية التفتيش وهذا الإجراء يتمثل في اللجوء إلى الأشخاص المؤهلين كالخبراء والتقنيين المختصين في الإعلام الآلي وفن الحاسبات لإجراء عمليات التفتيش على المنظومة المعلوماتية، وجمع المعطيات المتحصل عليها والحفاظ عليها وتزويد السلطات المكلفة بالتفتيش بهذه المعلومات.

---

[1]مادة 18 من قانون رقم 09-04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 اوت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته ومكافحتها، جريدة الرسمية، عدد47.

[2]مادة 5 من قانون رقم 09-04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 اوت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته ومكافحتها، جريدة الرسمية، عدد47.

[3] طرشي نورة، المرجع السابق، ص 131.

[4]مادة 5 مرجع سابق.

كما ألزمت المادة العاشرة من القانون 04/09 مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية والتفتيش وحفظ المعلومات طبقا للمادة 11 من نفس القانون التي من شأنها تمكين سلطات التحقيق من التعرف على مستعملي الخدمة[1].

وقد حدد هذا القانون المدة اللازمة لحفظ المعطيات بسنة واحدة من تاريخ التسجيل كما أوجب في المادة 12 على مقدمي الخدمات التزامات خاصة هي:

– واجب التدخل الفوري لسحب المعطيات المخالفة للقانون وتخزينها أو منع الدخول إليها باستعمال وسائل فنية وتقنية.

– وضع الترتيبات التقنية لحصر إمكانيات الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام وأن يخبروا المشتركين لديهم بوجودها.[2]

الفرع الثاني: المكافحة الإجرائية في قانون الإجراءات الجزائية.

سارع المشرع الجزائري بتعديل قانون الإجراءات الجزائية تماشيا مع التطور المعلوماتي الذي لحق بالجريمة، محاولة منه الحد من انتشارها، وذلك في إطار المكافحة الإجرائية لهذا النوع من الإجرام، حيث أنه بتعديلي 09/01 و14/04 وضع قواعد وأحكام خاصة لسلطة المتابعة والاختصاص، الغرض منها هو مواجهتها،[3] وهذه الأحكام هي:

– جواز تمديد الاختصاص المحلي للمحكمة: حيث نصت المادة 329 من قانون الإجراءات الجزائية في فقرتها الأخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[1].

[1] مادة 10 و11 من قانون رقم 09-04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 اوت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، جريدة الرسمية، عدد47.

[2] ربيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011، ص 155.

[3] طرشي نورة، مرجع سابق، ص 134.

– **توسيع مجال اختصاص النيابة العامة:** حيث أنه بموجب المادة 37 من قانون الإجراءات الجزائية تم توسيع مجال اختصاص النيابة العامة ليشمل نطاقات أخرى لم يكن مرخصا لها من قبل حيث نصت هذه المادة على تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف[2].

– **العمل بنظام المشروعية في تحريك الدعوى العمومية:** حيث سحب نظام الملائمة من النيابة العامة في مجال متابعة بعض الجرائم، حيث يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون بحيث لا يتمتع بشأنها بسلطة الملائمة بين تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد 144 مكرر، 144 مكرر 1و 2 من قانون العقوبات المعدل والمتمم بالقانون 09/01 المؤرخ في 26 يونيو 2001 [3].

– إضافة لما سبق ودائما في إطار المكافحة الإجرائية للجرائم المعلوماتية تم توسيع مجال اختصاص النيابة العامة في مجال البحث والتحري عن هذه الجرائم بمنح الإذن بالتفتيش والقيام باعتراض المراسلات وتسجيل الأصوات والتقاط الصور حسب نص المادة 65 مكرر 5 في إطار تعديل قانون الإجراءات الجزائية بالقانون 22/06 المؤرخ في 2006/12/20[4].

– **التسرب:** إضافة لما سبق تجدر الإشارة إلى الإجراء الجديد الخاص بمكافحة الجرائم المعلوماتية والمنصوص عليه في المادة 65 مكرر 11 من قانون الإجراءات الجزائية، وهو إجراء التسرب فتنص المادة 65 مكرر 11 على أنه "عندما تنقضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 ، يجوز لوكيل الجمهورية أو لقاضي

[1] مادة 329 من قانون الاجراءات الجزائية، المرسوم تنفيذي رقم 348/06 المؤرخ في 2006/10/05.
[2] مادة 37 من القانون الإجراءات الجزائية" عدلت بالقانون رقم 04-14 المؤرخ في 10نوفمبر 2004. (ج.ر..71ص.5)
[3] مادة 144مكرر و144 مكرر1 و2 من قانون العقوبات المعدل والمتمم بالقانون 09/01 المؤرخ في 26 يونيو 2001وعدلت بالقانون رقم 01-09 المؤرخ في 26 يونيو 2001). ج.ر34 ص.17) وكذا عدلت بالقانون رقم 88-26 المؤرخ في 12 يوليو 1988)، ج.ر 28 ص.1034) كما أضيفت بالقانون رقم 01-09 المؤرخ في 26 يونيو 2001). ج.ر34 ص.18.)
[4] مادة رقم65 مكرر5 في إطار التعديل قانون الاجراءات الجزائية بالقانون 22/06 المؤرخ في 20ديسمبر 2006(ج.ر.84.ص.8).

التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد 65 مكرر 12 و 65 مكرر 18 من قانون الإجراءات الجزائية".

وقد عرفت المادة 65 مكرر 12 التسرب على أنه "قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة، بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف"

كما سمحت الفقرة الثانية من المادة 65 مكرر 12 أن يستعمل لغرض إجراء التسرب هوية مستعارة أو أن يرتكب عند الضرورة الأفعال المنصوص عليها في المادة 65 مكرر 14 وهذه الأفعال هي:

– اقتناء أو نقل أو حيازة أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها[1].

– استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.

ويمكن للمتسرب بإتيان هذه الأفعال دون أن تترتب عليه المسؤولية الجزائية لأنه مرخص له بهذه الأفعال بهدف الوصول إلى مرتكبي الجريمة.[2]

وقد بينت المادة 65 مكرر 15 الشروط الواجب توفرها في الإذن بالتسرب، وهي أن يكون مكتوبا ومسببا وأن يذكر فيه الجريمة التي تبرر اللجوء إلى هذا الإجراء، وهوية ضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته[3].

[1] تمم الباب الثاني من الكتاب الأول بالقانون رقم 22/06المؤرخ في 20 ديسمبر 2006. (ج.ر.84ص.8) بفصل الرابع بعنوان في التسرب ويشمل المواد من 65مكرر11الى 65 مكرر18.

[2] طرشي نورة، المرجع السابق، ص 135

[3] المرجع السابق ص32.

كما يجب أن يحدد في الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة أشهر كما أجازت المادة 65 مكرر 15 كإجراء جديد في مكافحة الجريمة المعلوماتية اعتبار ضابط الشرطة القضائية الذي جرت عملية التسرب تحت مسؤوليته كشاهد عن العملية في إجراءات التحقيق فيها.[1]

المطلب الثالث: التحقيق في الجرائم الماسة بإسرار المعلوماتية.

الفرع الأول: ماهية التحقيق في الجرائم الماسة بسرية المعلومات الالكترونية

أداء ظهور الجريمة المعلوماتية إلى فرض على جهات التحقيق تحديات عظيمة لم يسبق لها مثيل، فما تتميز به هاته الجرائم من حيث السهولة والسرعة الفائقة في تنفيذ الجريمة، وانعدام الآثار المادية للجريمة، وغياب الدليل المرئي، وصعوبة الوصول إلى الدليل بالوسائل الفنية التقليدية، وكذلك سهولة إتلاف الدليل المادي وتدميره في زمن قياسي، كل ذلك استوجب إعادة النظر بوسائل المكافحة التقليدية للجريمة وأساليبها وطرق الوقاية منها،

وأصبح من الضرورة بمكان وضع الخطط والبرامج الاستراتيجية لتحديث أجهزة العدالة الجنائية وتطويرها من حيث بنيتها المؤسسية وكوادرها البشرية لتصبح قادرة من الناحية التقنية على التصدي لهذا النوع من الجرائم ومواجهة مرتكبيها وضبطهم وتقديمهم للعدالة، فضلا عن إشكالية توفر المعرفة القانونية لدى الجهات المختصة بمواجهة هذا النوع من الجرائم، ومنه تطورت وسائل التحقيق الجنائي في عصر المعلوماتية تطوراً ملموساً يواكب حركة الجريمة وتطور أساليب ارتكابها.[2]

معنى ذلك أن ظهور أنماط جديدة من الجرائم لم تكن مألوفة من السابق ونحن لا نزال في بداية عصر الانفجار المعلوماتي ويمكن أن نتوقع ظهور المزيد والمزيد من هذه الأنماط الجديدة، كان يتوجب معها تحديث

[1] طرشي نورة، مرجع نفسه، ص 137.

[2] بالنسبة للتشريع الفرنسي فإن المشرع سعى إلى ملاءمة قانون الإجراءات الجزائية مع الآليات والقواعد الإجرائية التي جاءت بها اتفاقية بودابست في مجال البحث عن الجريمة الإلكترونية باعتبار أن فرنسا كانت من الدول السباقة للتوقيع على. اتفاقية بودابست وذلك بتاريخ 23 نوفمبر 2001 هذه إذن كانت نظرة على بعض القوانين المقارنة وحدود ملاءمتها مع مختلف الآليات الإجرائية التي أرساها المنتظم الدولي.

الأنظمة والتعليمات والجهات الأمنية المختصة بمعالجة القضايا الناتجة عن ظهور هذه الأنماط الجديدة، وهو ما يستتبع تطوير أسلوب التحقيق فيها.

كما أن الطبيعة الفنية والتقنية الناجمة عن الجرائم المعلوماتية نتج عنها في مجال الإثبات الجنائي نوع جديد من الأدلة يطلق عليه الدليل الرقمي أو الدليل الإلكتروني، وقد اعتدت به المحاكم في بعض النظم القانونية المقارنة، سواء من حيث قيمته القانونية أي الدليل الرقمي وبين حجيته في الإثبات حيث ساوت هذه الأنظمة القانونية في الإثبات الدليل التقليدي والدليل الإلكتروني لهما نفس الحجية في الإثبات، ويعرف الدليل الإلكتروني بأنه "هو الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهي مكون رقمي

لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون [1]

اولا: تعريف التحقيق الجنائي الالكتروني

عملية التحقيق الجنائي الالكتروني هي استخدام الطرق المثبتة علمياً لحفظ، جمع، عرض، تحديد، تحليل ترجمة، توثيق، والتحقق من صحة الأدلة الرقمية المستخرجة من المصادر الرقمية بهدف تسهيل أو تعزيز بناء الأحداث الجنائية، أو المساعدة في إحباط العمليات غير الشرعية المرتقبة. [2]

[1] إشكاليات الدستور والبرلمان، بواسطة د. علي السامي، نشره Sama For Publishing & Distributiom. http://www.f-law.net/law/threads الاطلاع يوم 2020/05/20،على الساعة19:40.

[2] محمد عسكر، مقال بعنوان مقدمة لمراحل التحقيق الجنائي وخطواته، في 7 ديسمبر 2013، عن. http://www.isecur1ty.org/ يوم الاطلاع: 2020/05/22 على الساعة (16:30).

ويعرف أنه "عمل قانوني يقوم به مأمور الضبط القضائي المختص والمتخصص 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]

ثانيا: عناصر التحقيق الجنائي الالكتروني

يلتزم المحقق باستظهار الركن المادي والمعنوي للجريمة محل التحقيق، وتحديد وقت ومكان ارتكاب الجريمة المعلوماتية بالإضافة إلى علانية التحقيق.

1-إظهار الركن المادي للجرائم المعلوماتية

حيت إن النشاط أو السلوك المادي في الجرائم الالكترونية يتطلب وجود بيئة رقمية واتصال بالأنترنت ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته.[2]

2-إظهار الركن المعنوي للجرائم المعلوماتية

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني [3].

3-تحديد وقت ومكان ارتكاب الجريمة المعلوماتية

تثير مسألة النتيجة الإجرامية في جرائم الالكترونية مشاكل عدة، فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية، فلقوام أحد المجرمين في أمريكا اللاتينية باختراق أحد البنوك في الإمارات، وهذا الخادم موجود في الصين فكيف يمكن Server جهاز خادم معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين، وهذا بالتالي يثير مشكلة أخري وهي مكان ارتكاب الجريمة المعلوماتية،

[1] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، مطابع الشرطة القاهرة، مصر، 2008، ص 166.

[2] محمد حسن السراء، الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الالكترونية، الفكر الشرطي، المجلد الحادي والعشرون، العدد 81 ،2012، ص 36.

[3] محمد حسن السراء، مرجع نفسه، ص 36.

ويثور أيضا إشكاليات القانون الواجب التطبيق في هذا الشأن. حيث أن هناك بعد دولي في هذا المجال ذلك أن الجريمة المعلوماتية جريمة عابرة للحدود[1].

4-علانية التحقيق

فعلانية التحقيق من الضمانات اللازمة لتوافر العدالة، ولهذا قيل إن العلانية في مرحلة المحاكمة لا يقصر فيها الأمر علي وضع الاطمئنان في قلب المتهم، بل أن فيها بذاتها حماية لأحكام القاضي من أن تكون محلا للشك أو الخضوع تحت التأثير، كما أن فيها اطمئنانا للجمهور على أن الإجراءات تسير في طريق طبيعية [2].

الفرع الثاني: التحقيق في الجريمة المعلوماتية

إن طبيعة الجرائم المعلوماتية بعناصرها ووسائل ارتكابها قد تدفع المشرع الجزائي إلى ان يعيد النظر في كثير من المسائل الإجرائية، خاصة يتعلق فيما يتعلق بمسألة الإثبات باعتبارها أهم موضوعات هذا القانون. ذلك أن الدليل الذي قد يقوى على إثبات هذا النوع من الجرائم لابد أن يكون من ذات طبيعتها التقنية، وهو الأمر الذي لا تكون فيه القواعد الإجرائية التقليدية لاستخلاص الدليل قادرة على القيام به. مما يستوجب تدخل المشرع لتكريس قواعد إجرائية يمكن للجهات المكلفة بالبحث والتحري عن الجريمة المعلوماتية الاعتماد عليها في الوصول إلى الدليل المناسب في إثبات الجريمة المعلوماتية.

ولا شك أن هذا الدليل سيتم استخلاصه من البيئة الرقمية، والتي تعتبر مسرح الجريمة المعلوماتية مما يجعله يتميز بخصائصها (خصائص البيئة الرقمية).وهو الأمر الذي يقودنا الى الحديث عن مسالة قبول هذا الدليل أمام القضاء و مدى تعبيره عن الحقيقة نظرا لما يمكن أن يخضع له من التزييف والتحريف و الأخطاء، بل وحتى مع ضمان مصداقية هذا الدليل وكذا مشروعيته فإن الأمر لا يتوقف عند هذا الحد، بل يتجاوزه إلى مسألة أكبر أهمية

[1] محمد حسن السراء، المرجع نفسه، ص 37 .

[2] محمد حسن السراء، المرجع السابق ، ص 37.

تتعلق بمدى خضوع هذا الدليل ذو الأصالة العلمية للسلطة التقديرية للقاضي إعمالا لمبدأ الاقتناع الشخصي للقاضي الجزائي الذي يشكل جوهر أي حكم. وسوف أحاول أن أتناول هذه المسائل بنوع من التفصيل.[1]

اولا: التحقيق في الجريمة المعلوماتية

هذا الاخير هو إجراء من أهم الإجراءات التي تُتخذ بعد وقوع الجريمة، لما له من أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها، وهو كما يدل اسمه عليه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة.والثابت أن الدعوى الجزائية تمر بمرحلتين، مرحلة التحقيق ومرحلة المحاكمة، وتمر عملية التحقيق بمرحلتين أيضا، مرحلة التحقيق الأولي ومرحلة التحقيق الابتدائي، فالمرحلة الأولى وهي مرحلة جمع الاستدلالات التي يباشرها أعضاء الضبط القضائي[2] ، والمرحلة الثانية تدخل في اختصاص قاضي التحقيق[3].

وإننا نؤيد الرأي أو الاتجاه [4] الذي يقسم التحقيق إلى:

- تحقيق أولي و الذي يناط به رجال الضبطية القضائية.

- تحقيق قضائي ويناط به رجال القضاء، وهذا الأخير يقسم إلى تحقيق ابتدائي من اختصاص قاضي التحقيق وتحقيق نهائي ويكون في مرحلة المحاكمة من طرف قضاة الحكم.

---

[1] القانون رقم 15/04 المؤرخ في 10 /11/ 2004 المتضمن قانون العقوبات الجزائري المعدل والمتمم للأمر 66 / 156 المؤرخ في 8 جوان 1966.

[2] حسب المرجع السابق "يتمتع بصفة ضابط الشرطة القضائية: رؤساء البلديات، ضباط الدرك الوطني، محافظو الشرطة، ضباط الشرطة، ذوو الرتب في الدرك الوطني، ورجال الدرك الذين أمضوا في سلك الدرك أكثر من ثلاث سنوات ويتم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع. مفتشو الأمن الوطني الذين قضوا في خدمتهم بهذه الصفة ثلاث سنوات على الأقل وعينوا بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية وكذا ضباط الصف التابعين للمصالح العسكرية.

[3] يبدو لنا أن المشرع لا يفرق بين التحقيق الأولي والتحقيق الابتدائي وذلك من خلال نص المادة 63 من قانون الإجراءات الجزائية التي تنص على أن ضباط الشرطة القضائية يقومون بالتحقيقات الابتدائية ..." وفي نفس الوقت تنص المادة 66 الواردة في الباب المتعلق بالأحكام الخاصة بقاضي التحقيق على أن التحقيق الابتدائي في الجنيات وجوبي وهو بذلك يعتبر أن التحقيق الذي يمارسه سواء رجال الضبطية القضائية أم قضاة التحقيق يعد تحقيقا ابتدائيا على حد السواء.

[4] زهير كاظم عبود، بحث مقدم للأكاديمية العربية المفتوحة في الدنمارك، كلية القانون والسياسة قسم القانون الدراسات العليا 2007 بدون ترقيم.

[2] جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترانت، المرجع السابق. ص 76.

وفي كل جميع أنواع التحقيق هذه، يكون للقائمين عليه من ضبطية قضائية وقضاة صلاحية ممارسة إجراءات البحث والتحري المحددة وفقا لقانون الإجراءات الجزائية. وهو الأمر الذي يفهم صراحة من خلال استقراء نص المادتين 12 و38 من قانون الإجراءات الجزائية الواردتين في الباب الأول من هذا القانون تحت عنوان" في البحث والتحري عن الجرائم" حيث تنص المادة 12 الفقرة الثالثة أنه "يناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات..." وتنص في نفس الوقت المادة 38 من نفس القانون أنه "يناط بقاضي التحقيق إجراءات البحث والتحري ..."[1]

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

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

ثانيا: الأجهزة المكلفة بالبحث والتحري عن الجريمة المعلوماتية.[2]

التزايد المستمر للجرائم المعلوماتية أثر الأثر البالغ في ضرورة تطوير أجهزة الضبط القضائي لتواكب التطور الحاصل في مجال الجريمة، ونتيجة لهذا التحدي قامت معظم الدول بإحداث أجهزة متخصصة بمكافحة هذا النوع من الإجرام المستحدث تتولى مهمة التحري عن جرائم العالم الافتراضي وكشف النقاب عنها، وقد حملت هذه

[1] مادة 12و38 من قانون الإجراءات الجزائية المرجع نفسه ص4و16.

الاجهزة تسميات مختلفة منها مثلا شرطة الانترنت أو فرقة التحري عن جرائم المعلوماتية إلى غير ذلك من التسميات.

ولا يقتصر دور هذه الأجهزة على المستوى الوطني فقط، بل هناك أجهزة متخصصة على المستوى الدولي أيضا.

ثالثا: الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الداخلي:

ظهرت العديد من الأجهزة والهيئات المختصة في مجال الجريمة المعلوماتية في إطار مكافحتها والبحث والتحري عنها وعن مرتكبيها سواء على المستوى الوطني أم على صعيد الدول الأجنبية.

الكفاءة والتدريب والوسائل البشرية والمادية ما يؤهلها للتعامل مع هذا النوع المستحدث من الإجرام، وسوف نحاول أن نلقي الضوء على هذه الأجهزة الموجودة في بعض الدول ثم نعرج على الوضع في بلادنا.

إنه بالنظر إلى الطبيعة التقنية التي تتميز بها الجريمة المعلوماتية ذهبت أغلب الأنظمة القانونية الإجرائية في التشريعات المقارنة ألي أن تعهد بمسألة البحث والتحري عن هذا النوع من الجرائم لأجهزة متخصصة، لها.

1-الأجهزة المختصة في الدول الأجنبية: الدول المتقدمة دائما سباقة بإحداث هذه الأجهزة إذ أن مكافحة الجرائم المعلوماتية مرتبط بمدى تقدم الدول من الناحية التقنية وبمدى توفر الإمكانات المادية اللازمة لإنشاء هذه الأجهزة ونذكر على سبيل المثال في هذا الصدد الدول التالية:

1-1-الولايات المتحدة الأمريكية: قامت بإنشاء عدة أجهزة لمكافحة الجريمة المعلوماتية ومنها:

شرطة الواب webpolice: هي بمثابة نقطة مراقبة على الأنترانت إضافة إلى أنها تتلقى الشكاوى من مستخدمي الشبكة وملاحقة الجناة والقراصنة، والبحث عن الأدلة ضدهم وتقديمهم إلى المحاكمة[1] .

[1] جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترانت، المرجع السابق، ص 77 .

– **مركز تلقي شكاوى جرائم الأنترانت IC3**: وتم إنشاؤه من طرف مكتب التحقيقات الفدرالي FBI في سنة 2000.

ثم في عام 2003 تم دمج مركز شكاوى الاحتيال عبر الأنترانت المعروف ب IFCC مع هذا المركز. ويعمل مركز IC3 بصورة تشاركية مع مكتب التحقيقات الفدرالي والمركز الوطني لجرائم الياقات البيضاء NWC، ويقوم هذا المركز بتلقي الشكاوى عبر موقعه على الأنترانت أين يقوم الشاكي بمليء استمارة إلكترونية ثم يقوم المختصون في هذا المركز بتحليل الشكاوي وربطها بالشكاوي الأخرى المستلمة من قبل.

– **قسم جرائم الحاسوب والعدوان على حقوق الملكية الفكرية:** هذا القسم يختص بالتعريف بهذه الجرائم والكشف عنها وملاحقة مرتكبيها.

نيابة جرائم الحاسوب والاتصالات(CTC) تتألف هده الاخيرة من مجموعة من قضاة النيابة العامة ممن تلقوا تدريبات مكثفة على نظم المعالجة الآلية للبيانات وتم منحهم صلاحيات واسعة في مجال الجرائم المعلوماتية والعدوان على حقوق الملكية الفكرية.

المركز الوطني لحماية البنية التحتية التابع للمباحث الفدرالية الأمريكية وقد حدد هذا المركز البنى التحتية التي تعتبر هدفا للهجومات والاعتداءات عبر الأنترانت وعلى رأسها شبكات الاتصالات.

وإضافة إلى هذه الأجهزة يوجد أيضا في الولايات المتحدة الأمريكية وحدة متخصصة بمكافحة الإجرام المعلوماتي تابعة لقسم العدالة الأمريكي تتكون من خبراء في نظام الحوسبة والأنترانت ومن مستشارين قانونيين[1] .

[1] نبيلة هبة محمد هروال، مرجع سابق، ص 108.

1-2-في بريطانيا: السلطات البريطانية خصصه وحدة تضم نخبة من رجال الشرطة المتخصصين في البحث والتحري عن الجرائم المعلوماتية وتضم هذه الوحدة نحو ثمانين عنصرا على درجة عالية من الكفاءة في المجال التقني، وقد بدأت هذه الوحدة نشاطها عام 2001

1-3-في فرنسا: أجهزة الامن الفرنسية إنشاءات لمكافحة الجرائم المعلوماتية ونذكر من هذه الأجهزة:

القسم الوطني لقمع جرائم المساس بالأموال والأشخاص ويتكون هذا القسم من محققين مختصين في التحقيق بجرائم العالم الافتراضي وقد بدأ هذا القسم مهامه عام 1997

المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات ويعد هذا المكتب سلاح الدولة الفرنسية في مكافحة الجرائم المعلوماتية، وقد تم إنشاؤه في 2000/05/15.

1-4-في الصين: إنشاءات السلطات الصينية وحدة متخصصة على مستوى جهاز الشرطة تعرف باسم" القوة المضادة للهكرة" وهي تختص برقابة المعلومات التي يسمح لمواطنيها الدخول إليها عبر الأنترانت.[1]

وأما على مستوى الدول العربية فنجدها لم تقف مكتوفة الأيدي أمام خطر الجرائم المعلوماتية، فقد قامت بعض الدول منها بإنشاء أجهزة متخصصة لمكافحة هذه الجرائم ونذكر على سبيل المثال:

2-الأجهزة المتخصصة في مصر: أنشاءات وزارة الداخلية في مصر عدة أجهزة أوكلت لها مهمة ضبط ما يقع من جرائم من خلال الشبكة المعلوماتية نعرض لها على النحو التالي:

2-1-إدارة مكافحة جرائم الحسابات وشبكات المعلومات: أنشئت هذه الإدارة بموجب قرار وزاري[1] وهي تابعة للإدارة العامة للمعلومات والتوثيق وتخضع للإشراف المباشر لمدير الإدارة العامة وتشرف عليها فنيا مصلحة الأمن العام التابعة لوزارة الداخلية، وتضم ثلاث أقسام رئيسية:

[1] عمر محمد ابو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترانت، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2004، ص 812.

هي قسم العمليات، قسم التأمين وقسم البحوث والمساعدات الفنية. وتعتبر هذه الإدارة من أكبر الإدارات تعاملا مع الجرائم المعلوماتية، فهي تتكون من ضباط متخصصين في مجال تكنولوجيا الحسابات والشبكات وتختص بمكافحة جرائم الأنترانت على مختلف أنواعها.[2]

2-2-قسم مكافحة جرائم الحاسبات وشبكات المعلومات: وقد أنشئ هذا القسم بالإدارة العامة للبحث الجنائي بمديرية أمن القاهرة، ويتبع إدارة المعلومات والحاسب الآلي ويخضع من حيث الإشراف الفني لإدارة مكافحة جرائم الحاسبات وشبكات المعلومات ويختص بعمليات تأمين ورقابة نظم وشبكات المعلومات لمنع وقوع أية جرائم عليها باستخدام الأساليب والتقنيات العلمية الحديثة، ورصد ومكافحة وضبط الجرائم التي تقع باستخدام الحاسبات على نظم وشبكات المعلومات وقواعد البيانات.

3-الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الوطني:

الوضع في بلادنا فإنه وبالنظر إلى الخصوصية التي تتميز بها الجريمة المعلوماتية كان الأمر محتما لتوفير كوادر وأجهزة متخصصة تعنى بعملية البحث والتحري عن الجريمة المعلوماتية وكان ذلك إما على مستوى جهاز الشرطة أو الدرك الوطني.

فعلى مستوى جهاز الشرطة فقد أنشات المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة ومخبرين جهويين بكل من قسنطينة ووهران، تحتوي هذه المخابر على فروع تقنية من بينها خلية الإعلام الآلي، بالإضافة إلى أنه يوجد على مستوى مراكز الأمن الولائي فرق متخصصة مهمتها التحقيق في الجريمة المعلوماتية تعمل بالتنسيق مع هذه المخابر.

أما على مستوى الدرك الوطني فإنه يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام ولإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية. بالإضافة إلى مركز

[1] قرار وزير الداخلية المصري رقم 13507 لسنة 2002 الصادر بتاريخ 2002/07/07.

[2] نبيلة هبة محمد هروال، المرجع السابق، ص 141.

الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومي للدرك الوطني وهو قيد الانشاء.

رابعا: الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الدولي والإقليمي:

أسلفنا الذكر بأن الجرائم المعلوماتية تتميز بأنها عابرة للحدود الوطنية يمكن أن يتعدى أثرها عدة دول، لذلك كان لابد من وجود تعاون دولي من أجل مكافحة هذا النوع من الإجرام.

ومن أساليب التعاون الدولي التعاون الأمني الذي يمكن أن يحقق أهدافه لا قبل للشرطة الإقليمية بتحقيقها، ومن أبرز هذه الأجهزة في مجال مكافحة الجرائم المعلوماتية على هذا الصعيد نذكر ما يلي:

1-على المستوى الدولي: المنظمة الدولية للشرطة الجنائية (الأنتربول)[1] من أهم الأجهزة على المستوى الدولي لمكافحة الإجرام بصفة عامة ومنها الجرائم المعلوماتية، وبهدف هذه المنظمة الدولية إلى تشجيع التعاون بين أجهزة الشرطة في الدول الأطراف على نحو فعال من أجل مكافحة الجريمة ذات الطابع العالمي بما في ذلك الإجرام المرتبط بالمعلوماتية. وتستخدم هذه المنظمة لتحقيق أهدافها وسيلتين:

أ-تجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم عن طريق المكاتب المركزية الوطنية الموجودة في أقاليم الدول الأطراف.

ب-التعاون في ملاحقة المجرمين الفارين وإلقاء القبض عليهم وتسليمهم للدول التي تطالب بتسليمهم.

وتعمل المنظمة الدولية للشرطة الجنائية في مجال الجرائم المعلوماتية بوضع قائمة إسمية لضباط متخصصين يمكن الاستعانة بهم في مجال البحث والتحري في قضايا الجرائم المعلوماتية، كما توفر هذه المنظمة للدول الأطراف المعلومات اللازمة عن الطرق العملية في مجال الجريمة المعلوماتية من خلال خلق فرق عمل وورشات تكوين [2] ولقد

[1] بعد انتهاء الحرب العالمية الثانية عقد في بروكسل (بلجيكا) مؤتمر دولي في الفترة من6 -9/9 عام 1946 انتهى إلى إحياء اللجنة الدولية للشرطة الجنائية (ICPO) ونقل مقرها إلى باريس وغير اسمها ليصبح المنظمة الدولية للشرطة الجنائية الإنتربول ووضع ميثاق هذه المنظمة في الفترة 13 /06/ 1956 واعتبر نافذا اعتبارا من 07/13 / 1956.

[2] Myriam QUEMENER.Cyebrcrininalité droit pénel apliqué.econonica Septembre2010p208.

أنشأت هذه المنظمة وحدة متخصصة في مكافحة الجرائم المعلوماتية تقوم بتزويد أجهزة الشرطة التابعة للدول الأعضاء بإرشادات حول التحقيق في هذا النوع من الإجرام وكيفية التدريب على مكافحته.

2-الأجهزة على المستوى الإقليمي:

الشرطة الأوروبية أو الأوروبول: هو أحد الاجهزة على مستوى الاتحاد الأوروبي تم إنشاؤه في لكسنبورغ عام 1992 ومقره في مدينة لاهاي بهلندا ليكون حلقة وصل بين أجهزة الشرطة الوطنية للدول الأعضاء في مجال الجرائم الإرهابية والمخدرات والجريمة المنظمة وكذا الإجرام المعلوماتي ويهدف هذا الجهاز إلى تسهيل تبادل المعلومات بين أجهزة الشرطة لمختلف الدول الأعضاء، وكذا تجميع وتحليل المعلومات بغرض المساعدة في التحقيقات المفتوحة في أي دولة عضو بخصوص جريمة من الجرائم المذكورة ومنها الجريمة المعلوماتية.

وبمبادرة من الشرطة القضائية الفرنسية تم إنشاء جهاز على مستوى الأوروبول أطلق عليه إسم" ICROS (Internet Crime Repporting online System) في سنة 2010 بغرض التنسيق أكثر في مجال مكافحة الجريمة المعلوماتية على مستوى الدول الأعضاء.

الأوروجست :Eurojust :وهو جهاز يعمل على المستوى الأوروبي إلى جانب الأوروبول في مجال مكافحة جميع أنواع الجرائم، تم إنشاؤه عام 2002 وينعقد إختصاصه عندما تمس الجريمة دولتين على الأقل من الدول الأعضاء في الاتحاد الأوروبي أو دولة عضو مع دولة أخرى من غير الاتحاد الأوروبي. ويعد الأروجيست وحدة للتعاون القضائي، مهمتها الأساسية هي التنسيق بين السلطات القضائية المكلفة بالتحقيقات ولها من الصلاحيات ما يؤهلها لفتح تحقيقات ومباشرة متابعات جزائية [1]

[1] Myrian QUEMENER.YES CHOR PENAL Cybescviminalité Droit pénal appliqué p 209.

المبحث الثاني: آليات البحث في الجرائم الماسة بإسرار المعلوماتية.

تطرقنا في الفصل الأول الى تجريم الأفعال الماسة بحق الأشخاص في حرمة أحاديثهم ومكالماتهم الخاصة وحقهم في حرمة صورهم، بموجب المواد من 303 مكرر إلى 303 مكرر 3 من قانون العقوبات الجزائري، من خلال إبراز أهم الجوانب القانونية والفقهية للتجريم والجزاء، فقانون العقوبات كرس حماية الحياة الخاصة للأشخاص وأحاطها بالنصوص العقابية الواردة أعلاه[1].

ولكن تطبيق تلك النصوص ليس مطلقا، فقد أباح المشرع الجزائري كاستثناء عن القاعدة العامة المساس بحرمة الحياة الخاصة للأشخاص في قانون الإجراءات الجزائية. إذ أباح اختراقها حماية للمصلحة العامة في إطار التحري والتحقيق في الجرائم الخطيرة [2]، من خلال اعتراض المراسلات و تسجيل الأصوات و التقاط الصور، المنصوص عليها بالمواد 65 مكرر 5 إلى 65 مكرر 10 من قانون العقوبات الجزائية الجزائري، و هي الإجراءات التي تحد من الحق في الخصوصية، فتجعل منه حقا مقيدا بضوابط شرعت للمصلحة العامة في إطار احترام القانون[3] .

[1] مادة 303 مكرر الى مكرر3 من قانون العقوبات الجزائري في الجريدة الرسمية للجمهورية الجزائرية الدمقراطية الشعبية رقم 76المؤرخه في 8ديسمبر 1996معدل بالقانون رقم 02-03المؤرخ في 10افريل 2002الجريدة الرسمية للجمهورية الجزائرية الدمقراطية الشعبية المؤرخة في14 افريل 2002والقانون رقم 08-19المؤرخ في 15 نوفمبر 2008 جريدة الرسمية للجمهورية الجزائرية الجمهورية الديموقراطية الشعبية رقم63الموؤرخه في 16نوفمبر2008.

[2] نصت المادة 65 مكرر 5 فقرة 1 من ق ع ج على أنه: << 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 بتبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد يجوز لوكيل الجمهورية المختص أن يأذن .....>>.

[3] عبد المالك بن ذياب، المرجع السابق، ص 130.

ودالك بالنسبة للجرائم الواردة حصرا بالمادة 65 مكرر 5 فقرة أولى الواردة أعلاه، كون هذه الجرائم غزت العالم، غير معترفة بالحدود الجغرافية، إذ أنه ليس من السهل التنصت أو التتبع لفئة خطيرة وهدامة في المجتمع من دون المساس بحرياتهم الفردية التي حمتها وكفلتها كل القوانين والدساتير العالمية، فشرعت أساليب التحري الخاصة.

لاعتبارات المصلحة العامة، ولكن الملاحظ في هذا الشأن أن هذه النصوص تتعارض مع أحكام الدستور الجزائري لعام 1996تم تعديل الدستور 3 مرات، إذ نصت المادة 39 منه: <<لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، يحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة >>. فهذا النص لم يشر مطلقا إلى ايراد أي استثناء على تلك الحماية ما يفيد ترك المجال للقانون، بل أن الدستور وقف على أن: حرمة الحياة الخاصة لا يجوز انتهاكها وأنها محمية بموجب القانون، وبرجوعنا إلى هذا الأخير نجد أن القانون صدر لتلك الحماية من خلال نصوص تجريم المحددة بالمواد 303 مكرر إلى 303 مكرر من ق ع ج المحددة للجرائم المعاقب عليها السالف.

المطلب الأول: تسجيل الأصوات واعتراض المراسلات والتقاط الصور.

انطلاقا من كون أساليب التحري الخاصة ومنها اعتراض المراسلات وتسجيل الأصوات والتقاط الصور[1] الواردة في الفصل الرابع من الباب الثاني، ضمن المواد من 65 مكرر 5 إلى 65 مكرر 10 من ق ع ج. هي استثناء على قاعدة التجريم الواردة بنصوص قانون العقوبات بموجب المواد من 303 مكرر إلى 303 مكرر 3 من قانون العقوبات الجزائري[2]، فلابد من تحديد طبيعتها ونطاقها. من خلال تحديد مفهومها على النحو التالي:

أولا: مفهوم تسجيل الأصوات.

إن الحديث عن مفهوم وطبيعة تسجيل الأصوات يقتضي التطرق إلى التعريفات الواردة في هذا الشأن، ثم إلى بيان الجانب الفني والتقني لعملية تسجيل الأصوات من خلال إبراز الأجهزة والتقنيات المستعملة في دالك.

ومن خلال استقراء نص المادة 65 مكرر 5 من قانون العقوبات الجزائري فقرة ثانية، يظهر أن مفهوم التنصت على المكالمات يشمل اعتراض المراسلات وتسجيل الأصوات، وعلى هذا الأساس سنتطرق إلى مفهوم كل منهما وتحديد طبيعتها ونطاقها من خلال الفرعين المواليين.

ثانيا: مفهوم اعتراض المراسلات.

إن الحديث عن مفهوم وطبيعة اعتراض المكالمات يقتضي التطرق إلى التعريفات المختلفة، الواردة بشأنها سواء من ناحية التشريع أو الفقه أو القضاء مع بيان الجانب الفني والتقني المستخدم لإجراء عملية اعتراض المراسلات.

---

[1] تعتبر مسألة إدماج التقنيات الحديثة بصفة عامة وأجهزة التنصت والتصوير بصفة خاصة في مجال التحري من أهم المسائل التي أثارت اهتمام العديد من الفقهاء، فتباينت أراءهم، فيرى البعض أن استخدام هذه التقنيات الحديثة يعتبر باطلا باعتباره يجافي قواعد الأخلاق ويخالف المبادئ العامة للقانون، إضافة إلى أن الاعتماد على هذه =الوسائل تتوطى على اعتداء حقيقي على خصوصية الإنسان، عادل عبد العالي خرشي، ضوابط التحري عن. الجرائم في الفقه الإسلامي والقانون الوضعي، دون طبعة، دار الجامعة الجديدة الإسكندرية، مصر، ص 360. أما البعض الآخر فيرى أن استخدام هذه الاساليب الحديثة في التحري يعتبر من الأساليب الفعالة في مكافحة الجريمة، فليس هناك ما يحول دون استخدام هذه الوسائل، ونظرا للزيادة المطردة في معدلات الجريمة، فإنه يجب اختيار الأساليب المناسبة لمكافحتها والقول بغير دالك سوف يؤدي إلى الجمود في مواجهة الإجرام، ياسر الأمير، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، مصر، 2009، ص 30.

[2] مرجع سابق ص18.

ثالثا: مفهوم التقاط الصور.

اعتبر المشرع الجزائري أسلوب التقاط الصور كأسلوب من أساليب التحري الخاصة بموجب المادة 65 مكرر 5 الفقرة الثالثة من قانون الإجراءات الجزائية، إلى جانب اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات. وعليه لتحديد مفهوم أسلوب التقاط الصور، وجب التطرق إلى تعريفه من خلال إبراز مضمونه ثم بيان التقنيات والوسائل المستخدمة في دالك من خلال الفرعين المواليين.[1]

الفرع الثاني: التحقيق في الجرائم الماسة بالأسرار المعلوماتية

من الواضح أن مسألة إثبات الجرائم المعلوماتية من أهم المواضيع القانونية ذلك بالنظر إلى المشكلات الإجرائية التي أثارتها هذه الجرائم المستحدثة والمتمثلة في سرعة ودقة تنفيذ الجريمة وإمكانية نفاذ المجرمين المتمرسين إلى الأجهزة وتخريب أو إخفاء الملفات التي الباب الثاني: الجرائم الواقعة على السرية المعلوماتية في إطار القانون الجنائي وآليات مكافحتها تدينهم أو تجرمهم وهو ما يصعب عملية جمع الأدلة. كما أن الدليل الذي يقوى على إثبات هذا النوع من الجرائم لابد أن يكون من طبيعتها.

فنظرا للطابع الخاص الذي تتميز به هذه الجرائم، فإن إثباتها يحيط به الكثير من الصعاب والتي تتمثل في صعوبة اكتشاف هذه الجرائم لأنها لا تترك أثرا خارجيا[2]، فلا يوجد جثث قتلى وأثار للدماء، وإذا اكتشفت الجريمة

[1] عبد المالك بن ذياب، المرجع السابق، ص 141، نقلا عن، عبد القادر مصطفاوي، أساليب البحث والتحري، الخاصة، مجلة المحكمة العليا، قسم الوثائق، العدد 2 ،2009، ص 71.

[2] ومرد ذلك إلى مجموعة من العوامل تتمثل في: عدم وجود أثر كتابي، إذ يتم نقل المعلومات بالنبضات الإلكترونية، يستطيع الجاني تدمير دليل الإدانة في زمن متناه القصر، إعاقة الوصول إلى الدليل بوسائل الحماية الفنية، حيث أنه في كبرى المواقع العالمية على شبكة تحاط البيانات المخزنة على صفحاته بسياج من الحماية الفنية لإعاقة المحاولات الرامية للوصول غير المشروع إليها لتدميرها وتبديلها أو الاطلاع عليها أو نسخها، فإذا تمكن الجاني من اختراق تلك المواقع وقام بالعبث بها، فإنه قد يقوم بوضع وسائل حماية فنية خاصة به لكي يمنع الغير من الدخول على ذلك الموقع الذي قام بالعبث به ومن ثم يصعب الوصول إليه كما يصعب الكشف عن دليل يدينه. مثل قيام الجاني باستخدام كلمات مرور بعد تخريب الموقع مثلا، ويشكل استخدام تقنيات التشفير أحد أكبر العقبات التي تعوق جهات التحري.

غالبا يكون ذلك بمحض الصدفة[1].ناهيك عن ارتكاب الجريمة يتم غالبا من مسافات بعيدة باستخدام وحدات طرفية أو بأساليب أخرى مشابهة.

عموما بالنسبة لهذا النوع من الجرائم فإن رجال التحقيق يواجهون صعوبات شديدة في ضبط وتوصيف الجرائم المعلوماتية وأيضا لتعقب مرتكبيها، ويعود ذلك بالطبع إلى كونها جرائم ترتكب في فضاء الكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود.

وهذه الصعوبات تعود عموما لما تتميز به الجريمة المعلوماتية من مميزات سبق التفصيل فيها كسهولة إخفاء الجريمة، غياب الدليل المرئي، صعوبة الاهتداء إلى مرتكب الجريمة، إعاقة الوصول إلى الدليل بواسطة الحماية الفنية[2]، سهولة محو الدليل، الضخامة البالغة لكم البيانات المتعين فحصها، نقص خبرة رجال التحقيق.

فصعوبة الاهتداء إلى مرتكبي الجرائم الواقعة في ذلك السياق فإذا أراد شخص إلحاق الضرر بشخص لآخر وقام باختراق جهازه الحاسب الآلي وتمكن من الحصول على بعض البيانات والمعلومات الشخصية الخاصة بالمجني عليه، فإنه وإن أمكن تحديد الحاسب الذي اخترق تلك البيانات فإنه يصعب تحديد شخص المستخدم لذلك الحاسب في ذلك الوقت.

ولا شك أن التعامل في مسرح الجريمة سواء أكان مسرحا ماديا أو الكترونيا يتطلب، إجراءات روتينية معينة متفق عليها لحماية الدليل وإبراز قيمته الاستدلالية إلا أن طرق حفظ الأدلة واستخلاصها تختلف من مسرح الجريمة المادي إلى مسرح الجريمة الالكتروني.

[1] غالبا ما تكتشف تلك الجرائم بمحض الصدفة وذلك للإحجام عن الإبلاغ من طرف المجني عليهم يحاولون درء الأثر السلبي للإبلاغ عما وقع خاصة إذا كان المجني عليه من المؤسسات التي لديها عملاء.

[2] منى فتحي أحمد، مرجع سابق، ص 143 والدكتور عبد الفتاح بيومي حجازي، الجوانب الإجرائية، الأعمال الإجرائية لإعمال التحقيق الابتدائي في الجرائم المعلوماتية، ص 57.

المطلب الثاني: الجزاءات المترتبة على المساس بإسرار المعلوماتية

استدعى تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية استدعى تدخلا تشريعيا صريحا سواء على المستوى الدولي أو الإقليمي أو الداخلي فدوليا وضعت أول اتفاقية تضمنت مختلف الإجرام المعلوماتي حول الإجرام المعلوماتي بتاريخ 11/08/ 2001[1]، أما على المستوى الوطني فقد استدرك المشرع الجزائري الفراغ القانوني في مجال الإجرام المعلوماتي و ذلك باستحداث نصوص تجريميه لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون 15/04 المتضمن تعديل قانون العقوبات الجزائري المعدل و المتمم للأمر 156/66 و يجدر الإشارة مرة أخرى أن الجرائم الماسة بالأنظمة المعلوماتية و إن كانت تختلف في أركانها و عقوبتها إلا أن ما يجمعها أنها تحقق حماية جزائية لنظم المعالجة الآلي.

الفرع الأول: الحماية القانونية في التشريع الجزائري.

الجزائر قبل 2004 لم تعرف قوانين تطبق بشكل خاص على حماية نظام المعلوماتية أو على تكنولوجيا الإعلام والاتصال، و الواقع أن هناك العديد من التشريعات الوطنية التي كانت تطبق في مجال المعلوماتية، منها الأمر 66/ 156 المؤرخ في 08 جوان 1966 والمتضمن قانون العقوبات المعدل و المتمم، والأمر 66- 155 المؤرخ في 08 جوان المتضمن قانون الإجراءات الجزائية والأمر 75- 58 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون المدني، وكذلك الأمر رقم 03 - 05 المؤرخ في 19 جوان 2003 المتعلق بحقوق المؤلف المجاور[2] و لمسايرة التطور التكنولوجي كان لابد للجزائر على غرار الدول المتقدمة من إيجاد الإطار القانوني المناسب لحماية المنظومة المعلوماتية من السلوكيات الإجرامية المستحدثة، فصدر القانون رقم 15/04

[1] الاتفاقية الدولية حول الإجرام المعلوماتي أبرمت في 2001/11/08، من طرف المجلس الأروبي تم توقيعها في 2001/11/23

[2] انظر الموقع الإليكتروني www.startimes.com، في 2020/06/05 على الساعة (09:22)

المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات، إلا أن المشرع الجزائري قرر الحماية القانونية لجريمة الدخول أو البقاء غير المصرح بهما فقط دون جريمة الاعتراض غير القانوني.

الفرع الثاني: الجزاءات المترتبة على الشخص الطبيعي:

عندم نطلع على نصوص قانون العقوبات الجزائري والفرنسي نجدهما ينصان أساسا على العقوبات الأصلية المطبقة على مختلف الجرائم المرتكبة في مجال الجنوح التقني، وطبقا للمبادئ والاتجاهات الحديثة المتعلقة بالعقوبات يتضمنان إضافة للعقوبات الأصلية قائمة العقوبات التكميلية[1]

أولا: العقوبات الأصلية:

وضع القانون لكل جريمة عقوبة أو أكثر أصلية، وهذا شأن جرائم الاعتداء على نظم المعالجة الآلية وهذه العقوبة قد تكون بسيطة عندما لا تقترن بأي ظرف من ظروف التشديد، كما تكون مشددة عندما تقترن بظرف من ظروف التشديد[2]

1-العقوبات البسيطة:

1-1-عقوبة جريمة الدخول أو البقاء غير المصرح بهما في صورتها البسيطة: إذا لم ينجم على الدخول والبقاء غير المصرح بهما إعاقة أو إفساد أو إزالة أو تعديل للمعلومات فإن العقوبة تكون:

الحبس من ثلاثة أشهر إلى سنة و الغرامة من 50.000 دج إلى 100.000 دج، (المادة 394مكرر من القانون رقم 15/04 الفقرة الأولى)[3] .

[1] انظر الموقع الإلكتروني: www.startimes.com، الموقع السابق.

[2] رشيدة بوكر، المرجع السابق، ص 317.

[3] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة، الجزائر، 2006، ص 127.

أما المادة 323 الفقرة الأولى من القانون الفرنسي فإن العقوبة المقررة لجريمة الدخول أو البقاء غير المصرح بهما في صورتها البسيطة الحبس لمدة سنتين وغرامة مالية 30.000 أورو[1].

1-2-عقوبة جريمة الدخول والبقاء غير المصرح بهما في صورتها المشددة: تشدد عقوبة جريمة الدخول أو البقاء غير المصرح بهما في حالتين:

الحالة الأولى: في حالة ما نتج عن الدخول أو البقاء غير المصرح بهما حذف أو تغيير لمعطيات المنظومة ترفع العقوبة إلى ضعف تلك المقررة في الصورة البسيطة سواء في حدها الأدنى الذي يضاعف إلى ستة أشهر أو في حدها الأقصى الذي يضاعف إلى سنتين أما الغرامة فترفع للضعف أي تتراوح من 100.00دج إلى 200.000 دج. (المادة 394 مكرر الفقرة الثانية)

الحالة الثانية: كذاك إدا نتج عن الدخول أو البقاء غير المصرح بهما تخرب لنظام اشتغال المنظومة: فترفع عقوبة الحبس من 6 أشهر إلى سنتين أما الغرامة فيثبت الأدنى حدها عند 50.000 دج في حين يرتفع الحد الأقصى إلى 150.000 دج. (المادة 394 مكرر الفقرة الثالثة)[2]

إلى جانب المشرع الجزائري نجد أن المشرع الفرنسي بدوره جعل من جسامة النتيجة ظرفا مشددا لجريمة الدخول أو البقاء غير المصرح بهما إذ ترتفع العقوبة متى نجم عن الدخول أو البقاء حذف أو تعيير أو تخريب اشتغال المنظومة وهذا ما نصت عليه الفقرة الثانية من المادة 1/323 كما يلي:

---

[1] **Art 323-1 le fait d'accéder ou de maintenir, frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni « deux ans [ancienne rédaction ; d'un an] » d'emprisonnement et de « 30.000 € [ancienne rédaction ; 15.000 euros] » d'amende.**
1- **Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de « trois ans [ancienne rédaction ; deux ans » d'emprisonnement et deux « 45.000 € [ancienne rédaction ; 30.000 euros]» d'amende.riov**
Yeves Mayaud. Code pénal. Edition dalloz : paris. 2010. p 1057.

[2] أمال قارة، مرجع سابق، ص 127.

...»أذا ترتب على الأفعال المذكورة أعلاه حذف أو تغيير لمعطيات المنظومة أو تخريب اشتغال هذا النظام تصل العقوبة إلى 3 سنوات حبس و 45.000 يورو غرامة 137[1]

2العقوبات المشددة:

تنص المادة 394 مكرر في فقرتيها الثانية والثالثة عن ظرف تشدد به عقوبة جريمة الدخول أو البقاء غير المصرح بهما والذي سبق ذكره وما نلاحظه على هذا الظرف المشدد أنه ظرف مادي يكفي أن تقوم بينه وبين الجريمة الأساسية علاقة سببية للقول بتوافره.

كما نصت المادة 394 مكرر 3 على أن تضاعف العقوبات المقررة للج ا رئم الماسة بالأنظمة المعلوماتية و ذلك إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام .[2]

ثانيا: العقوبات التكميلية: وتتمثل في المصادرة والغلق.

1– المصادرة: فتجريم السلوك الذي يهدد نظم المعالجة الآلية في سريتها ليس كافيا لمعاقبة و ردع الجناة، فبض هؤلاء المجرمين حتى و إن تم توقيفهم و إدانتهم سوف يكون بوسعهم حيازة الأشياء التي استخدموها في ارتكاب جرائمهم لاستخدامها في أغراض أخرى، لذلك من الضروري اتخاذ تدابير و آليات الحيلولة دون إفادة المجرمين من الأشياء التي استخدموها في تحقيق سلوكياتهم الإجرامية، ومن أهم الوسائل للقيام بذلك هو ضمان توافر أنظمة تقتضي بمصادرة الأشياء التي استخدمت في ارتكاب الجريمة، و هذا ما نصت عليه المادة 394 مكرر 6 بقولها: " مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة " و هذا مسلك حسن لأثره الشخصي والموضوعي في فعالية مواجهة هذا النوع من الجرائم .[3]

[1] مرجع سابق، ص 318.

[2] أمال قارة، مرجع نفسه، ص 128 .

[3] رشيدة بوكر، مرجع سابق، ص ،327 – 328 .

و نستخلص من خلال عبارة " يحكم بمصادرة " الواردة في المادة أعلاه أن المصادر وجوبية متى تعلق الأمر بالأجهزة و البرامج و الوسائل المستخدمة في ارتكاب الجريمة من الجرائم الماسة بالأنظمة المعلوماتية مع مراعاة الغير حسن النية[1] .

2-الغلق: المشرع الجزائري نص على عقوبة تكميلية أخرى الى جانب عقوبة المصادرة وفي الغلق وذلك بموجب المادة 394 مكرر 6 كما يلي: " ...مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على إغلاق المحل مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها."

وما نلاحظه من هذه المادة أن المشرع الجزائري قد جعل لعقوبة الغلق محلين:

2-1-إغلاق المواقع: والأمر يتعلق بالمواقع التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.

2-2-إغلاق المحل أو مكان الاستغلال: إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك إغلاق المقهى الإلكتروني الذي ترتكب فيه مثل هذه الجرائم بشرط توافر عنصر العلم لدى مالكها .[2]

الفرع الثالث: الجزاءات المترتبة على الشخص المعنوي.

تطرقت المادة 12 من الاتفاقية الدولية للإجرام المعلوماتي، مبدأ مساءلة الشخص المعنوي بحيث يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا، كما يسأل عن الجريمة التامة أو الشروع فيها، كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه، هذا مع ملاحظة أن المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة[3] .

[1] أمال قارة، مرجع سابق، ص 128.
[2] أمال قارة، مرجع نفسه، ص 128.
[3] أمال قارة، المرجع نفسه، ص 129.

كما تجدر الإشارة إلى أن المشرع الجزائري قد أقر المسؤولية الجزائية للشخص المعنوي وذلك في نص المادة 18 مكرر من قانون العقوبات الذي ينص على أن: " العقوبات المطبقة على الشخص المعنوي في مواد الجنايات و الجنح هي[1]:

1-الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

2-واحدة أو أكثر من العقوبات التكميلية الآتية:

- حل الشخص المعنوي.

- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات.

- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر، نهائيا أو لمدة لا تتجاوز 5 سنوات.

- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.

- نشر و تعليق حكم الإدانة.

- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات و تنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكب الجريمة بمناسبته.

بالنسبة لعقوبة الغرامة المطبقة على الشخص المعنوي عند ارتكابه إحدى الجرائم الماسة بالأنظمة المعلوماتية فهي تعادل طبقا للمادة 394 مكرر 4 من القانون 15/04خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي[2]

[1] المادة 18 مكرر من القانون رقم 04/ 15 المتضمن قانون العقوبات المعدل و المتمم لأمر 66 /156 .

[2] انظر المادة 394 مكرر 4 من قانون 15/04 .

الخاتمة

الخاتمة:

الجريمة المعلوماتية سلوك غير سوي وهي وليدة التقدم والتكنولوجيا وسهولة التواصل ونشر المعلومات وتعدد طرق الاطلاع ومعالجة المعلومات ولا شك ان اصحاب هذا السلوك غير السوي اي المجرمين قد استغلوا الوسائط واوعية المعلومات ووسائل التكنولوجيا الحديثة من اجل تحقيق اثار اكبر وارباح بأضعاف ما كان عليه في السابق وعطفا على هدا فقد اصبح من الطبيعي ان تظهر انماط جديدة من الجرائم التي لم تكن معروفة في السابق وذلك بسبب النمو الهائل الدي حصل في مجالات المعلوماتية وتقنيات الاتصال التي كان لها الفضل في تقديم الرخاء والراحة للإنسان في حياته ولكن كما ان حياة الانسان في عصرنا هذا اصبحت بالسرعة والسهولة والجودة في القيام بالأعمال الا ان تعرض الانسان للجريمة اصبح اكثر مما سبق واثار هده الجرائم اكثر وقعا وتكليفا لان المجرم عمل على استغلال هذه التقنيات والبرامج وانظمة البحث والعالجة وغيرها من اجل القيام بجرمه بسهولة وانسيابية ولهذا فقد استعرضنا في هده الدارسة الخصائص التي تتميز بها الجريمة المعلوماتية عن الجريمة التقليدية وكدا الجهود المبذولة وطنيا ودوليا هده الجريمة كما قمنا باستعراض كيفية المتابعة والتحقيق في هده الجريمة للحد منها وكبح جماح المجرمين وفي الاخير استخلصنا من بحثنا العناصر التالية:

1-ان المشرع الجزائري قام بتعديل قانون العقوبات وأدرج القسم السابع مكرر تناول جرائم المساس بأنظمة المعالجة الالية للمعطيات وتبين ان المشرع قد اعتمد فرضية الادماج في النصوص التقليدية ودلك ما نص عليها في فصله الثالث وكدا الباب الثالث وحلت محل الجرائم التعدي على الملكية الفكرية والفنية والتي تم الغاؤها بموجب الامر 10-97.

2-عدم استقرار المجتمع الدولي على وضع نصوص قانونية دولية موحدة تردع من تسول له نفسه القيام بهده الجرائم التي يعد العالم الافتراضي مسرح لها بما يوفر الحماية الجنائية من الجرائم الماسة بسرية المعلومات الالكترونية.

3-استنتجنا ان الجرائم الماسة بسرية لمعلومات الالكترونية هي جرائم دات خطورة كبيرة على امن المجتمع واقتصادات الدول وسياستها نظرا لاعتمادها على انظمة الكترونية وهدا راجع الى سهولة الوصول الى المعلومات والتعامل معها واهمية المعلومات في تلك الجرائم.

4-المتابعة والتحقيق والتحري في هده الجرائم يتطلب وسائل مادية ومؤهلات بشرية فنية وتقنية عالية المستوى سواء المحققين او القضاة الدين يحددون العقوبات

5-ان الجهات المخول لها تامين الشبكات المعلوماتية مراقبة والحفاظ على الامن القانوني هي من تحقيق امن المعلومات بفرض وضمان الامن التقني والفني اي ما يعرف بأمن الشبكات

6-الجرائم الماسة بسرية المعلومات تتوفر على النصر الدولي بحيث يمكن في بضع لحظات نشر عدد لا حصر له من المعلومات في جهاز شخص اخر موجود في اي مكان في العالم وهدا ما يثير اشكالا في القانون الواجب التطبيق مع التنازع في تحديد المحكمة التي لها اختصاص النظر في النزاع او الواقعة الناشئة.

في الاخير لا يمكننا الا ان نقول ان انه ادا اصاب بحثنا وكشف الحقيقة فهدا ما نصبوا اليه في بحثنا هدا وان اخطانا او قصرنا في بعض جوانبه فحسبنا اننا سعينا وبدلنا جهد ولم نبخل بما نقدر عليه في سبيل نجاحنا لتحقيق هدفنا الدي قمنا من اجله بهده الدراسة.

قائمة المراجع

قائمة المراجع: المصادر

أولا: القرآن الكريم

- سورة طه.

- سورة التحريم.

-سورة مريم.

ثانيا النصوص القانونية

- الدستور الجزائري سنة 1996.
- قانون العقوبات المعدل والمتمم.
- قانون الإجراءات الجزائية المعدل والمتمم.
- كالنظام الأساسي لسلطنة عمان الصادر بالمرسوم السلطاني رقم 96/101 في المواد ،18،27،30 منه والمواد 57 ،45، من الدستور المصري، والمواد 7، 10، 15 من الدستور الأردني 1952 م، والمواد 11، 29، 30، 31، 39 من الدستور الكويتي وغيرها.
- قانون 04/09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها - .قانون 03/2000 المؤرخ في 5 جمادى الأولى 1421 الموافق لـ 5 أوت 2000 محدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.
- الاتفاقية الدولية حول الإجرام المعلوماتي أبرمت في 2001/11/08، من طرف المجلس الأوربي تم توقيعها في 2001/11/23.
- القانون رقم 15/04 المؤرخ في 10 /11/ 2004 المتضمن قانون العقوبات الجزائري المعدل والمتمم للأمر 66 /156 الصادر في الجريدة الرسمية للجمهورية الجزائرية، العدد 71المؤرخ في 8 جوان 1966.
- الدستور الجزائري لسنة 2016 بموجب القانون رقم 01/16 المؤرخ في 6 مارس 2016، جريدة رسمية رقم 14 مؤرخة في 7 مارس 2016.

- قانون رقم 2000-03 مؤرخ في 5جمادى الأولى عام 1421 الموافق ل 5 غشت سنة 2000، تحدد القواعد العامة المتعلقة بالبريد الموصلات السلكية ولاسلكية ج. رسمية عدد المؤرخة في 6 جمادى الأولى عام 1421، الموافق ل 6 غشت سنة 2000.
- الامر رقم 66-156 المؤرخ في 18 صفر عام 1936 الموافق ل 8 يونيو سنة 1966المتضمن قانون العقوبات المعدل والمتمم ج. رسمية، عدد49 المؤرخة في 11 يونيو 1966.
- قانون العقوبات الجزائري صدر تعديل بشأنه بموجب القانون 06/ 23 المؤرخ في 20 ديسمبر 2006 جريدة عدد 84 صادر بتاريخ 24 ديسمبر 2006 الذي عدل وتمم الأمر 156/66 المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات الجزائري.
- مرسوم رئاسي 183/04مؤرخ في 8 جمادى الأولى 1425 الموافق لـ 26 يونيو 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد القانوني الأساسي.

ثالثا: الاتفاقيات والقرارات

✓ **الاتفاقيات**

1-الاتفاقية الدولية حول الاجرام المعلوماتي ابرمت في 2011/11/18 من طرف المجلس الأوروبي تم توقيعها في 2011/11/23.

2-اتفاقية الرياض العربية للتعاون الدولي وافق عليها مجلس الوزراء العدل العرب بموجب قراره رقم (1) المؤرخ في 1983/4/6 في دورة انعقاده العادي الأول، وقعت الاتفاقية من قبل جميع الدول الأعضاء عدا (جمهورية مصر العربية –جمهورية القمر الاتحادية الإسلامية)، دخلت الاتفاقية حيز النفاد ابتداء من تاريخ1985/10/30 ذالك طبقا لنص مادة 67.

3- اتفاقية بودابست المبرمة في 23 نوفمبر 2001.

رابعا: الكتب

❖ الكتب الخاصة

1. امال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة، الجزائر، 2006.

2. شيماء عبد المغني عطاءالله، الحماية الجنائية للتعاملات الإلكترونية، دون طبعة، دار الجامعة الجديدة، الأزرايطية، مصر،2007

❖ الكتب العامة

3. أحمد أمين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، 2004

4. أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دار النهضة العربية، الطبعة الأولى، القاهرة، مصر،2010.

5. أسامة أحمد المناعسة، جلال محمد الزغبي، صايل فاضل الهواوشة: " جرائم الحاسب الآلي والانترنت" دار وائل للنشر والتوزيع، الطبعة الأولى، عمان، الاردن ،2001.

6. أمين فرج يوسف الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعة لكلية حقوق مصرية، الإسكندرية، مصر، 2008، ص 219 ،224.

7. بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات، دار الفكر الجامعي، الإسكندرية، مصر، 2008.

8. جمال الدين أبي الفضل محمد بن مكرم ابن منظور الأنصاري الإفريقي المصري، راجعه عبد المنعم خليل ابراهيم، المجلد الثالث، الطبعة الأولى دار الكتب العلمية بيروت لبنان، 2005.

9. حسام محمد عيسى نقل التكنولوجيا دراسة في الآليات القانونية للتبعية الدولية، دار المستقبل العربي، القاهرة، مصر. 1987.

10. خالد ممدوح إبراهيم:

-أمن الجريمة الالكترونية، دار الفكر الجامعي، الطبعة الأولي، الإسكندرية، مصر، 2008.

- الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2009.

11. رشيدة بوكر. جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن. الطبعة الأولى. منشورات حلي. الحقوقية: لبنان. 2012.

12. سامي منصور. الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية، دون طبعة، المنشورات الحقوقية صادر، لبنان، 2006.

13. سهيل محمد العزام، الوجيز في جرائم الإنترنت، الطبعة الأولى، دائرة مكتبة الجامعة، الأردنية،2009.

14. طارق عفيفي صادق أحمد، الجرائم الالكترونية جرائم الهاتف المحمول، الطبعة الأولى، المركز القومي للإصدارات. القانونية، القاهرة، مصر، 2015.

15. عبد الفتاح البيومي الحجازي:

-الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الكتب القانونية، القاهرة، مصر، 2002.

-الحكومة الإلكترونية، دون طبعة، دار الفكر الجامعي، الإسكندرية، مصر، 2004.

- مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي (دراسة قانونية متعمقة في القانون المعلوماتي)، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، مصر،2006.

-دليل الرقمي و التزوير في جرائم الكمبيوتر و الأنترنت، دراسة معمقة في جرائم الحاسب الآلي و الأنترنت، بهجات للطباعة و التجليد، مصر، 2010.

16. عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، الإسكندرية، مصر، 1999.

17. عصام أحمد البهجي، حماية الحق في الحياة الخاصة، في ضوء حقوق الإنسان والمسؤولية المدنية، دار الجامعة الجديدة، للنشر الإسكندرية، مصر ،2005.

18. علي أحمد عبد الزغبي، حق الخصوصية في القانون الجنائي، دراسة مقارنة، الطبعة الأولى، المؤسسة الحديثة للكتاب، طرابلس، لبنان، 2006.

19. عمر أبوبكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة، مصر ،2004.

20. فريد هكيت، الخصوصية في عصر المعلومات، ترجمة محمد محمود شهاب، الطبعة الأولى، مركز الأهرام للترجمة. والنشر، القاهرة، مصر، 1999.

21. فؤاد حسين العزيزي، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، 2014.

22. ماجد أحمد عبد الرحيم الحيارى، مسؤولية الصحفي المدنية دراسة مقارنة بين القانونين الأردني والمصري، الطبعة. الأولى، دار يافا العلمية للنشر والتوزيع، عمان، الاردن ،2008.

23. محمد حسن السراء، الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الالكترونية، الفكر الشرطي المجلد الحادي والعشرون، العدد 81 ،2012.

24. محمد سعادي، أثر التكنوبوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديدة، الإسكندرية، مصر، 2014.

25. محمد عبد المحسن المقاطع، نحو صياغة جديدة لمفهوم الحياة الخاصة للأفراد وضماناتها في مواجهة تهديدات الكمبيوتر. بحث مقدم لمؤتمر الكويت الأول للقانون والحاسب الآلي، كلية الحقوق، جامعة الكويت، الطبعة الأولى 1994.

26. محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية، الطبعة الأولى، دار الفكر والقانون للنشر والتوزيع، المنصورة، مصر، 2017.

27. محمد مصطفى الشقيري، السرية المعلوماتية، ضوابطها وأحكامها الشرعية، الطبعة الأولى، دار البشائر الإسلامية. للطباعة والنشر بيروت لبنان، 2008.

28. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، مطابع الشرطة القاهرة، مصر، 2008.

29. منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية. مصر، 2006.

30. نادية محمد معوض، أتر المعلومات على الحق في سرية الاعمال، كلية الحقوق، جامعة حلوان، الشارقة، بدون سنة.

31. نائلة محمد فريد قورة، جرائم ابغاسب الاقتصادية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 2003.

32. نبيلة هبة محمد هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات – دراسة مقارنة – دار الفكر الجامعي، الطبعة الأولى، لإسكندرية، مصر، 2007.

33. ناصر إبراهيم محمد زكي، سلطة القاضي الجنائي في تقدير الأدلة "دراسة مقارنة"، رسالة دكتوراه جامعة الأزهر، كلية الشريعة والقانون، مصر، 1978.

34. هدى حامد قشقوش، الجريمة المنظمة، القواعد الموضوعية والإجرائية والتعاون. الدولي، دار النهضة العربية، القاهرة، مصر، 200.

35. هشام محمد فريد رستم: هشام محمد فريد رستم الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة الطبعة الأولى، القاهرة، مصر، 1994.

36. هلالي عبد الإله أحمد:

-تفتيش الحاسب الالي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة 1997، ص74.

-حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر ،1999 .

-اتفاقية بودابست لمكافحة الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر،2007.

37. يونس عرب دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي، ورقة عمل مقدمة إلى ندوة أخلاق المعلومات 17 أكتوبر 2002، عمان، الأردن، نادي المعلومات العربي 16.

المراجع الاجنبية:

38. Bertrand : La criminalité informatique, les délits relatifs au matériel. D1984, n° 62, expertise, p 149.

39. DURHAM(COLO) : the emergin structures of criminal information law : tracing the contours of new pardigm geenral report for the a.i.d.pcollwuiumr.I.D.P1993.P115.

40. Garçon : Code pénal annoté ; 2eme édition par m. Rousselet, N° 47, p.575.

41. Goutal : La protection pénale des logiciels, Le droit commercial face aux technologies nouvelles de la communication. Paris 1986, p 254.

42. KASPERSEN(W.K.Henrik) : computer crimes and other crimes against information technology in the netherlands .R.I.D.P.1993, p, 479.

43. Lucas de leyssac : l'arrêt buorquin…, article précité, p12.

44. Myriam QUEMENER.Cyebrcrininalité droit pénel apliqué.econonica Septembre2010.

45. P.Corlay : Reflection sur les récentes controverses relatives au domaine et à la définition De vol. J.C.P 1984 I doct 3160.

46. PHILIP M, stanely computer crime invetigation and investigators computer & security North Holland1986, pp.310-311.

47. Pradel et Feuillard : Les infractions commises au moyen de l'ordinateur.R.dr.pén. Crim1985.p307.

48. SIMMEL (G.), La Sociéte Seréte, Novelle revue Psychanalyse, 1976, n° 14, P.2 .24

49. Vassilaki (Irini) : computer crimes and other crimes against information techenologye in greece RI.D.P.1993, P, 371.

50. ZEMPLENI (A.), La Chàine du secret, Novelle revue Psychanalyse, 1976, N° 14, P .316 ance.

51. ZICRY Laure, Enjeux et maitrise des cyber-risques, largus, edition, 2014, Fr1 SIMMEL (G.), La Sociéte Seréte, Novelle revue Psychanalyse, 1976, n° 14, P.281 .

أطروحات الدكتوراه:

1. رابحي عزيزة، الاسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بلقايد، تلمسان، الجزائر ،2017-2018.

2. ناصر إبراهيم محمد زكي، سلطة القاضي الجنائي في تقدير الأدلة "دراسة مقارنة"، رسالة دكتوراه جامعة الأزهر، كلية الشريعة والقانون، مصر، 1978.

مذكرات الماجستير:

1. طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة. الماجستير، في القانون الجنائي، جامعة الجزائر 1، كلية الحقوق، 2012/2011.

مذكرات الماستر:

.1ريم ساسي، الحماية الجزائية لسرية المعلومات الإلكترونية، مذكرة تكميلية لنيل شهادة الماستر، قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن المهيدي، أم البواقي، الجزائر، 2015-2016.

– المداخلات:

بن بادة عبد الحليم:

1. الملتقى الدولي الأول الموسوم بـ: أمن المعلومات في الفضاء الإلكتروني: الرهانات والتحديات في شمال إفريقيا المنعقد يومي: 17و18 فيفري 2020، كلية الحقوق والعلوم السياسية، جامعة غرداية.

2. بن بادة عبد الحليم، المراقبة الإلكترونية كإجراء لاستخلاص الدليل الإلكتروني، بين الحق في الخصوصية ومشروعية الدليل الإلكتروني، المجلة الأكاديمية للبحث القانوني، 2019/12/31.

المواقع الإلكترونية:

1. الموقع الالكتروني http://ar.wikipedia.org/wiki ، يوم الاطلاع 2020/05/7، الساعة (12:20.
2. الموقع الالكتروني، http://www.mohamah.net/law ، يوم الاطلاع: 2020/05/17 الساعة (13:17.
3. الموقع http://www.ao-academy.org/docs/45D0 :، تاريخ الاطلاع على الموقع :2020/05/18.
4. منتدى شباب طمرة، قسم الكمبيوتر والأنترنت – "جرائم الكمبيوتر والأنترنت": الموقع، www.tamra.com، يوم الاطلاع: 2020/05/30، على الساعة (14:09
5. search.asp ? ID=148.http://www.arablawinfo.com/research Validate=articles يوم الاطلاع : 2020/05/30 على الساعة 14:14
6. منتدى جامعة قطر "كلية القانون": " مراحل إثبات الجريمة الإلكترونية" عن موقع: Heard PHP?t=20845http://www.quatar.com/VB/show يوم الاطلاع : 2020/05/29 على الساعة (11:37).
7. إشكاليات الدستور والبرلمان، بواسطة د. علي السامي، نشره Sama For Publishing & Distributiom. http://www.f-law.net/law/threads الاطلاع يوم 2020/05/20،على الساعة19:40.

قائمة المحتويات