الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليـــــم العالـــي والبحث العلمـــــي

Ministère de L'enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق والعلوم السياسية

المرجع:.....

قسم: القانون العـــــام

مذكرة نهاية الدراسة لنيل شهادة الماستر

آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري

ميدان الحقوق والعلوم السياسية

الشعبة: الحقوق

التخصص: القانون الجنائي والعلوم الجنائية

من إعداد الطالبة:

بوبقرة خيرة

تحت إشراف الأستاذ:

بن عودة نبيل

أعضاء لجنة المناقشة

الأستاذ(ة): درعي العربي	رئيسا
الأستاذ(ة): بن عودة نبيل	مشرفا مقررا
الأستاذ(ة): بن قارة مصطفى عائشة	عضو مناقش

السنة الجامعية: 2020/2019

نوقشت بتاريخ: 2020/09/09

إهداء

إلى من أوصاني بهما ربي برا و إحسانا

والدي العزيزين أمي و أبي

إلى إخوتي و أخواتي و بالأخص إلى حبيباتي كوثر و خروبية زهرة قلبي.

أهدي هذا العمل المتواضع.

شكر و تقدير

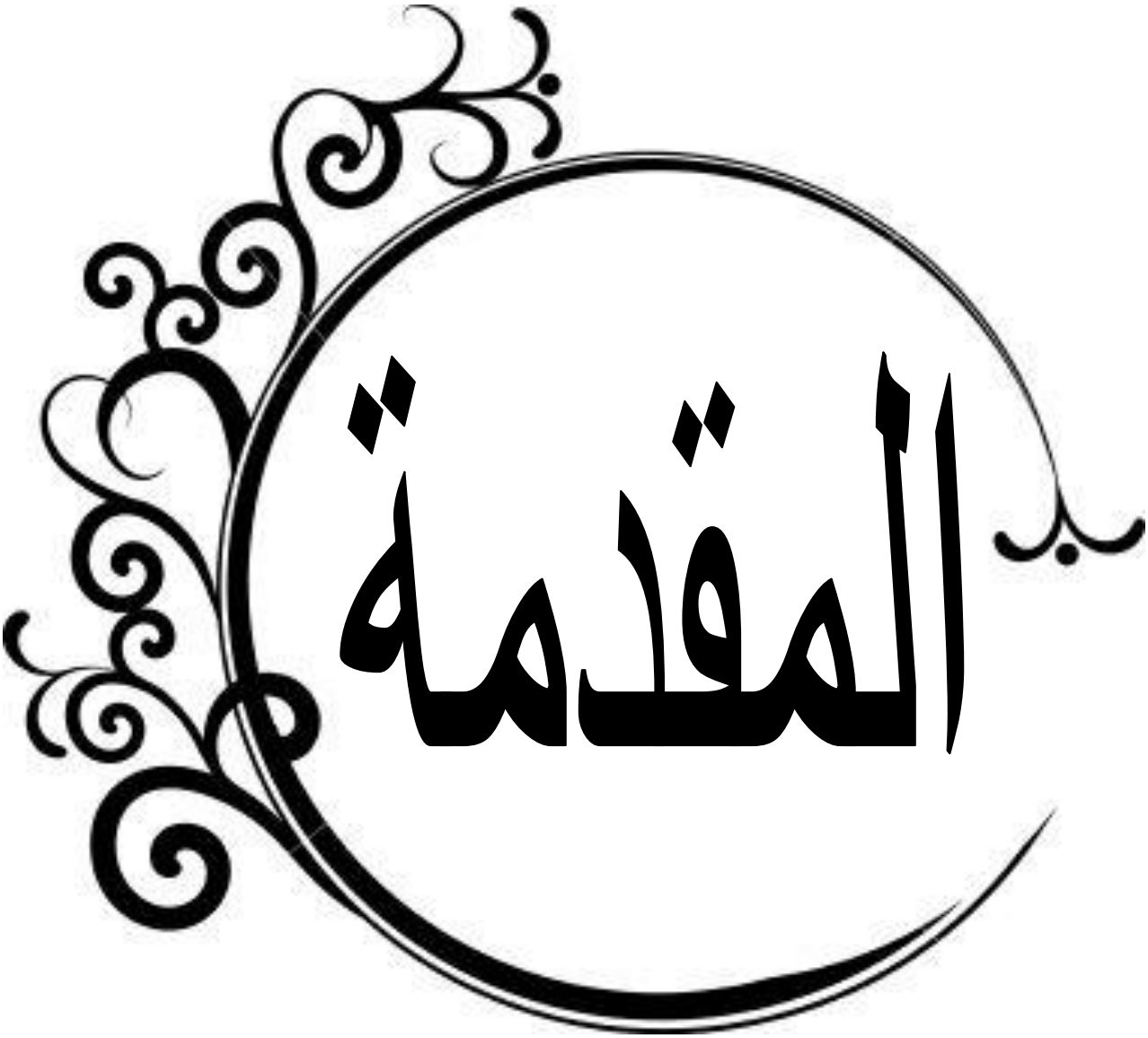
قال رسول الله صلى الله عليه و سلم في معنى الحديث من صنع لكم معروفا فكافئوه فإن لم تجدوا بما تكافئونه فادعوا له..

فأول كلمة أقولها الحمد و الشكر لله تعالى الذي ألهمني و أعانني على إتمام بحثي هذا والذي آمل أن أكون قد حققت الغاية المرجوة منه، كما أخص بالشكر و التقدير و الاهتمام الأستاذ بن عودة نبيل الذي تفضل بالإشراف على هذه المذكرة و تقديم النصح و الإرشاد طوال هذه الفترة إعداد المذكرة فله مني فائق الاحترام و التقدير.

كما أتقدم بالشكر إلى كل أعضاء اللجنة المحترمة الذين قبلوا مناقشة هذه الرسالة رغم كثرة انشغالاتهم و ارتباطاتهم الشخصية.

قائمة المختصرات:

Internet Protocol	**IP**
Internet Crime Complaint Center	**IC3**
Internet Froude Complaint Center	**IFCC**
National White Collar Center	**NWC**
Internet Crime Reporting Online System	**ICROS**
Tram Mission Control Protocol	**TCP**


المقدمة

الجريمة ظاهرة قديمة عرفتها المجتمعات البشرية منذ القدم، وظهرت في هذه المجتمعات السلطة الحاكمة انطلاقا من رب الأسرة إلى شيخ القبيلة، حيث وضعت بعض القيود على تصرفات الأفراد لاستتبات الأمن لدى الفرد والمجتمع، واعتبرت أن كل فعل يمس أمن الجماعة أو حياة الفرد أو ماله وسلامته الجسدية، فعل مجرّم يستحق العقاب عليه.

لكن بعد ظهور فكرة الدولة تولت بنفسها سلطة تجريم الأفعال والعقاب عليها حيث أصدرت تشريعات منها ما هو موضوعي"قانون العقوبات"، والذي يجرم الأفعال ويحدد العقوبات عليها، ومنها ما هو إجرائي"قانون الإجراءات الجزائية" الذي يحدد الإجراءات الواجب إتباعها أمام الهيئات القضائية وكذا الضبطية القضائية، دون أن ننسى أن الشريعة الإسلامية المناسبة لكل زمان ومكان قد حددت الكليات الخمس التي لا تستقيم الحياة إلا بها وهي: حفظ الدين، حفظ النفس، حفظ العقل، حفظ المال وحفظ النسل، وبينت أن مسألة المجرم تكون استنادا لمبدأ حرية الاختيار لقوله تعالى:﴿ إِنَّ الَّذِينَ كَذَّبُوا بِآيَاتِنَا وَاسْتَكْبَرُوا عَنْهَا لَا تُفَتَّحُ لَهُمْ أَبْوَابُ السَّمَاءِ وَلَا يَدْخُلُونَ الْجَنَّةَ حَتَّىٰ يَلِجَ الْجَمَلُ فِي سَمِّ الْخِيَاطِ وَكَذَٰلِكَ نَجْزِي الْمُجْرِمِينَ ﴾ [1]

غير أنه بتطور الإنسان في شتى الميادين، خصوصا في مجال التقنية إذ ظهر الحاسب الآلي وشبكة الأنترنت وغزت هذه الوسيلتين جميع المجالات نظرا لما تتسم به من الدقة والسرعة وأصبحت في متناول الجميع، كل ذلك أدى إلى بروز طائفة جديدة من الجرائم ونوع جديد من المجرمين وهو الانعكاس السلبي لهذه الثورة العلمية، حيث تطورت الجريمة بدورها وأصبحت تمس المعلومات وهو ما يسمى بالجريمة الالكترونية، فهذه التقنية تسمح بنقل المعلومة صوتا وصورة عبر الأنترنت، وفي أي مكان من العالم مما يسمح للبعض استغلال هذه الشبكة في ارتكاب جرائمهم، وهذا يعتبر خطر يهدد المجتمع والعالم ككل، وهذا ما يعطي أهمية كبيرة للموضوع تستدعي دراسة هذه الظاهرة المستجدة باعتبارها كانت غير معروفة في

[1] سورة الأعراف الآية 40.

القانون الجنائي، لذا كان اهتمامي بالبحث في موضوع الجريمة الالكترونية، بغية شرح وتحليل المفاهيم القانونية المتعلقة بها.

وهدفي من دراسة الموضوع هو إثراء المكتبة وسد النقص في المراجع المتخصصة في هذا المجال، ومحاولة دراسة الظاهرة وتحليلها وبيان كيفية مكافحتها، غير أنه قد واجهتني بعض الصعوبات في إنجاز البحث، كون أن الموضوع له علاقة بالجانب التقني والفني، وهذا ما يستدعي المتخصص الإلمام أكثر بالموضوع.

وإذ نحن بصدد البحث في هذه الإشكالية الجوهرية تصادفنا تساؤلات يعتبر البحث فيها أمر ضروري الإجابة عند جوهر موضوع الدراسة والتي منها:

- ما مدى فاعلية الآليات القانونية في التحقيق الجنائي في الجريمة المعلوماتية؟
- ما هي خصائص الجريمة المعلوماتية وكذا خصائص المجرم المعلوماتي؟ وما مدى تأثيرها على إثبات الجريمة وإسنادها للمتهم؟
- ما هي طبيعة الدليل المناسب لإثبات الجريمة المعلوماتية؟
- كيف تكون طريقة البحث والتحري في استخلاف الدليل الرقمي؟
- ما موقف المشرع الجزائري من ذلك؟

وعلى هذا الأساس يمكن أن نحصر نطاق هذه الدراسة ضمن خطة تتكون من فصلين:

الفصل الأول: الجوانب القانونية للجريمة المعلوماتية.

الفصل الثاني: الجوانب القانونية للتحقيق في لجريمة المعلوماتية.


الفصل الأول

تمهيد

بالرغم من المزايا الهائلة التي تحققت والتي تتحقق كل يوم بفضل تقنية المعلومات على جميع الأصعدة وفي شتى ميادين الحياة المعاصرة، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة جراء استخدام هذه التقنية المتطورة والانحراف عن الأغراض المتوخاة منها، تبدت في تفشي طائفة من الظواهر الإجرامية المستحدثة، ألا وهي ظاهرة الجرائم المعلوماتية، ليس هذا فحسب بل سهلت هذه التقنية ارتكاب بعض الجرائم التقليدية وشكلت أرضا خصبة لكثير من الأنشطة غير المشروعة المرتبطة بالحاسبات الآلية، هذه الحاسبات التي أصبحت توفر للجناة وسيلة هامة لارتكاب العديد من الجرائم المرتبطة بالمعلوماتية ما كانت لتظهر لولا وجود هذه الحاسبات الآلية وارتباطها بالتقنية المعلوماتية.

ولما كانت الجريمة المعلوماتية ظاهرة إجرامية حديثة نظرا لارتباطها بالتكنولوجيا الحديثة، فقد ترتب على ذلك إحاطة هذه الظاهرة بكثير من الغموض، لأجل ذلك فقد بدا لي أنه وقبل الخوض في المسائل الشكلية والإجرائية التي تنطبق على الجريمة المعلوماتية أن أنوه على جانب من القواعد الموضوعية لهذه الظاهرة الإجرامية، إذ يجب الإلمام بماهية الجرائم المعلوماتية وطبيعتها وإظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجمة عنها ودوافع مرتكبيها، وهذا حتما في منظورنا يتخذ أهمية استثنائية لسلامة التعامل مع هذه الظاهرة من طرف القائمين على مكافحتها، وعلى ضوء ذلك سأتناول في هذا الفصل تحديد مفهوم الجريمة المعلوماتية وأوجه الحماية الجزائية الموضوعية للنظم المعلوماتية.

المبحث الأول: ماهية الجريمة المعلوماتية.

إنه منذ شيوع استخدام الحاسب الآلي أو الكمبيوتر في الستينات ثم السبعينات بدأ الحديث عن بعض الأفعال والسلوكات المرتبطة بالاستخدام غير المشروع للبيانات المخزنة في أنظمة الكمبيوتر والتلاعب بهذه البيانات وتدميرها، وقد رافق ذلك نقاشات وتساؤلات حول ما إذا كانت هذه السلوكات مجرد شيء عابر أم أنها ظاهرة جرمية مستجدة.

ولقد شهد العالم في الفترة الراهنة ازديادا مطردا في نطاق استخدام تقنية المعلومات وتطورا بالغا في الاعتماد عليها في تسيير شؤونه، وهو الأمر الذي صاحبه في المقابل ازدياد مواز للإجرام المعلوماتي.

وتعد الجريمة المعلوماتية من الظواهر الإجرامية الحديثة، وتحديد مفهومها يعد الخطوة الأولى للتعرف على هذه الظاهرة الجرمية من جميع جوانبها القانونية، خاصة إذا علمنا أنه لا يوجد مصطلح قانوني موحد للدلالة على هذه الظاهرة الإجرامية الناشئة في بيئة الكمبيوتر بسبب ذاتيتها وتميزها عن غيرها من الجرائم التقليدية، سواء في محلها أو خصائصها، ومما لا شك فيه فإن أي محاولة من أجل اختيار وتحديد المصطلح الملائم لهذه الظاهرة ينبغي أن يكون مبنيا ومؤسسا على عدة ضوابط تقنية وقانونية، أولها إدماج البعدين التقني والقانوني، ذلك أن تقنية المعلومات في أصلها هي نتاج اندماج الحوسبة والاتصال، فأما الحوسبة فتقوم على استخدام وسائل التقنية لإدارة وتنظيم ومعالجة المعطيات في إطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق، وأما الاتصال فهو قائم على وسائل تقنية لنقل المعلومات، والضابط الثاني يقوم على أساس البحث بشأن الحدود التي ينتهي عندها العبث وتلك التي تبدأ عندها المسؤولية عن أفعال تعد مجرمة، والضابط الثالث أن يكون اختيار المصطلح شاملا لما يعبر عنه ملما بحدود محله، فلا ينبغي أن يقتصر على الجزء ليعني الكل ولا ينصرف إلى ما لا يجب أن ينطوي تحت نطاقه.

لذلك فلقد بذل المهتمون بدراسة هذا النمط الجديد من الإجرام جهدا كبيرا من أجل الوصول إلى تعريف مناسب يتلاءم مع طبيعة الجريمة المعلوماتية، ذلك أن عدم الاتفاق على تعريف هذه الظاهرة الإجرامية إنما يؤدي إلى إثارة عدد من المشكلات العملية يتمثل أهمها في صعوبة تقدير حجم هذه الظاهرة وتعذر إيجاد الحلول اللازمة لمواجهتها، وكذا صعوبة تحقيق التعاون الدولي لمكافحتها.[1]

إلا أن المتفق عليه أن فكرة المعلوماتية هي الفكرة الجوهرية والمركزية في دراسة هذه الظاهرة الإجرامية، ذلك أن المعلوماتية هي شرط مفترض لقيام هذا النوع من الجرائم.

المطلب الأول: تعريف الجريمة المعلوماتية:

إن الجرائم الناشئة في البيئة الرقمية جرائم حديثة، ارتبط مفهومها ولا يزال يرتبط بتكنولوجيا الحاسبات وتطوراتها المستخدمة في تشغيل وتخزين و نقل المعلومات في شكل الكتروني، و كذا بتكنولوجيات وسائل الاتصال وشبكات الربط، لذلك فإنه من الضروري أن يكون أي تعريف لهذا النمط من الجرائم متسما بالمرونة مما يسمح باستيعابه وتواكبه مع سائر التقنيات المبتكرة الراهنة والمستقبلية في مجال تكنولوجيا التعامل مع المعلومات.

لكن التطور المستمر ولا متناهي للتكنولوجيا المعلومات والاتصالات حال دون وضع تعريف فقهي جامع وشامل لمفهوم الجريمة المعلوماتية،[2] خشيةً من حصر نطاقها داخل إطار تجريمي محدد قد يضر بها خاصة في ظل التطور المستمر للتقنية المعلوماتية، فما يتم تجريمه اليوم قد يصبح غير ذي أهمية بالنسبة لصور مستحدثة أخرى تظهر نتيجة استخدام تقنيات جديدة.

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، الطبعة الأولى، 2005، ص28.

[2] خالد ممدوح إبراهيم، الجرائم المعلوماتية، الدار الجامعية، ص73.

وإذا كان التطور المتجدد والمستمر للمعلوماتية يمنع صور التجريم الحالية عن مواكبة ما يطرأ من صور إجرامية مستحدثة في مجال المعلوماتية إلا أن وضع قواعد قانونية تنظم أوجه الحماية الجنائية أفضل بكثير من ترك ما يستجد على الساحة الجنائية دون حماية، وهذا ما يقع على عاتق الفقه بداية بوضع تعريف لهذه الظاهرة الإجرامية، والذي قد يسهم في صياغة المشرع للنصوص القانونية ويساعد القضاء في تفسير هذه النصوص وتكييف الوقائع.

ولقد ذهب الفقهاء في تعريف الجريمة المعلوماتية مذاهب شتى ووصفوا تعريفات مختلفة تتمايز وتتباين تبعا لموضوع العلم المنتمية إليه وتبعا لمعيار التعريف ذاته، فاختلفت بين أولئك الباحثين في الظاهرة الإجرامية الناشئة عن تقنية المعلوماتية من الوجهة التقنية، وأولئك الباحثين في ذات الظاهرة من الوجهة القانونية، وحتى من الوجهة القانونية تعددت التعريفات واختلفت بحسب الدراسة القانونية التي تناولتها.[1]

وفي سبيل ذلك فإن الفقه الجنائي قد بذل محاولات عديدة لتعريف الجريمة المعلوماتية، ولعل جميع المحاولات التي بذلت من أجل تعريف الجريمة المعلوماتية لا تخرج عن أحد الاتجاهين أولها يضيق من مفهومها و الثاني يوسعه.

[1] ذلك أن الجريمة المرتكبة بواسطة تقنية المعلومات تدخل في نطاق دراسات القانون الجنائي الوطني والتي تقع في صميم القسم الخاص لقانون العقوبات، وأنها من الجرائم التي تتخطى حدود الدولة الواحدة فهي تدخل أيضا في نطاق دراسات القانون الجنائي الدولي، ونظرا لنمو وتزايد التجارة الإلكترونية من خلال المبادلات والمراسلات التجارية الالكترونية فإن الجرائم المرتكبة بواسطة تقنية المعلومات لصيقة الصلة بالقانون التجاري وبحركة التجارة العالمية الحديثة، كما أن الاستعمال الواسع لتقنية المعلومات في المجتمع مكنت من تخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية فخلقت بذلك سلسلة من التحديات الجديدة والتهديدات الخاصة بالحياة الشخصية وأدى ذلك إلى تزايد انتهاك الحقوق الأساسية والحريات الفردية التي كفلتها القوانين الدستورية مما يدل على ارتباط الموضوع أيضا بالقانون الدستوري وارتباطه في نفس الوقت بالقانون الإداري خاصة في ظل ظهور وبروز الحكومات الإلكترونية.

الفرع الأول: الاتجاه الذي يضيق مفهوم الجريمة المعلوماتية:

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

ومن التعريفات التي وضعها أنصار هذا الاتجاه أن الجريمة المعلوماتية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية ولملاحقته وتحقيقه من ناحية أخرى،[2] وفي هذا الاتجاه أيضا عرفها الفقيه David Thomson(دافيد تومسون)،[3] أنها:" أي جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب".

وحسب هذا التعريف فإنه يشترط أن يكون مرتكب الجريمة المعلوماتية على درجة كبيرة من العلم بتكنولوجيات الحاسبات، وهذا المفهوم قد أخذت به وزارة العدل الأمريكية في تقريها الصادر عام 1989 بعد تبنيها لدراسة وضعها معهد ستانفورد الدولي للأبحاث حينما عرف الجرائم المعلوماتية بأنها أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها.

وفي هذا الاتجاه أيضا عرفها جانب من الفقه بالنظر إلى معيار نتيجة الاعتداء، إذ يرى الأستاذ MASS أن المقصود بالجريمة المعلوماتية هي تلك الاعتداءات التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح، كما عرف الأستاذ PARKER الجريمة المعلوماتية بأنها كل

[1] نائلة محمد فريد قورة، المرجع السابق، ص30.

[2] المرجع نفسه، ص28.

[3] رشيدة بوكر، المرجع السابق، ص40.

فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنها خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل.

وهناك جانب آخر أخذ في تعريفه للجريمة المعلوماتية بمعيار موضوع الجريمة وذلك كما ذهب إليه الفقيه (Posenblatt)،[1] على أنها:" نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخلا لحاسوب أو تغييرها أو حذفها".

والملاحظ أن التعريفات المتقدمة تضيق على نحو كبير من الجريمة المعلوماتية، حتى أن البعض يرى أن الجريمة المعلوماتية في ظل هذا الاتجاه سوف تصبح أشبه بالخرافة فحصرها مثلا في الحالات التي تتطلب أن يكون مقترف هذه الجريمة متمتعا بقدر كبير من المعرفة التقنية لارتكابها و هو أن ما تحقق في بعض الأحوال قد لا يتوفر في كثير منها، إذ قد يرتكب الفعل الغير مشروع في البيئة الرقمية دون أن يكون فاعله بحاجة إلى هذا القدر من المعرفة، ورغم ذلك فإنه لا يمكن إنكار أن هذه الأفعال تدخل في عداد جرائم المعلوماتية، فالقيام مثلا بإتلاف البيانات المخزنة داخل نظام الكمبيوتر لا يتطلب من فاعله قدرا كبيرا من العلم بتكنولوجيات الحاسبات الآلية، و على الرغم من ذلك فقد جرمته الكثير من التشريعات العقابية.

لذلك فإنه يؤخذ على هذه التعريفات السابقة أنها جاءت قاصرة عن الإحاطة بأوجه ظاهرة الإجرام المعلوماتي، فالبعض من فقهاء هذا الاتجاه ركز على معيار موضوع الجريمة و البعض الآخر على وسيلة ارتكابها و البعض الآخر ركز على معيار النتيجة.

[1] نهلا عبد القادر المومني، الجريمة المعلوماتية، الطبعة الثانية، 2010، دار الثقافة للنشر والتوزيع، ص48.

الفرع الثاني: الاتجاه الموسع لمفهوم الجريمة المعلوماتية.

إزاء الانتقادات التي وجهت للاتجاه الأول حاول بعض الفقه تعريف الجريمة المعلوماتية على نحو واسع لتفادي أوجه القصور التي شابت تعريفات الاتجاه الضيق في التصدي لظاهرة الإجرام المعلوماتي.

فعلى عكسٍ من الاتجاه السابق فإن أنصار هذا الاتجاه يذهبون إلى التوسيع من مفهوم الجريمة المعلوماتية باعتبار أن مجرد مشاركة الحاسب الآلي في النشاط الإجرامي يصبغ عليه وصف الجريمة المعلوماتية، وقد تباينت مواقف أنصار هذا الاتجاه في تعريف الجريمة المعلوماتية بحسب المعايير التي اعتمد عليها كل فريق في تعريف الجريمة المعلوماتية، فيذهب فريق من الفقهاء إلى تعريف الجريمة المعلوماتية بأنها كل سلوك إجرامي يتم بمحاسبة الحاسب الآي وفريق آخر يعتبرها أنها كل جريمة تتم في محيط الحاسبات الآلية، ومن هذه التعريفات ما جاء به الفقيه (MERWE) الذي يرى أن الجريمة المعلوماتية تتمثل في الفعل الغير مشروع الذي يتورط في ارتكابه الحاسب الآلي.[1]

كما ذهب البعض إلى القول بأن الجريمة المعلوماتية هي كل عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها.

وفي ذات الاتجاه يرى كل منMichel et credo أن الجريمة المعلوماتية تسهل استخدام الحاسب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به

[1] محمد أمين الشوابكة، جرائم الحاسوب والانترنيت (الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2009، ص08.

الحاسوب المجني عليه أو بياناته، كما تمتد لتشمل الاعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدات المتصلة به.[1]

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

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

كما عرفها الفقيهين(Richard totty) و (Anthony Hardcastle) على أنها الجرائم التي يكون للحاسب فيها دورا إيجابيا أكثر منه سلبيا.[4]

ولا شك أن الاتجاه المتقدم ينطوي على توسيع كبير لمفهوم الجريمة المعلوماتية، إذ يؤخذ عليه هذا التوسع الذي من شأنه أن يصبغ وصف الجريمة المعلوماتية على أفعال قد لا تكون كذلك لمجرد مشاركة الحاسب الآلي في النشاط الإجرامي، ولا يمكن القبول بهذا التوجه فقد لا يعدوا أن يكون الحاسب الآلي محلا تقليديا في بعض الجرائم كسرقة الحاسب ذاته أو الأقراص أو الأسطوانات المغنطة مثلا، فلا يمكن إعطاء وصف الجريمة المعلوماتية على سلوك الفاعل لمجرد أن الحاسب أو إحدى مكوناته المادية كانت محلا لفعل الاختلاس.[5]

---

[1] هلال عبد الإله أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية(دراسة مقارنة) الطبعة الأولى، دار النهضة العربية، 2000، ص14.

[2] خالد عباد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة، 2001، ص30.

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

[4] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994، ص06.

[5] نائلة محمد فريد قورة، المرجع السابق، ص31.

ولم يسلم هذا الاتجاه من سهام النقد أيضا حين وسع من نطاق هذه الجريمة إلى درجة التسوية بين السلوك غير المشروع قانونا والسلوك الذي يستحسن اللوم أخلاقيا واستهجان الكافة له، كما في التعريف الذي أورده خبراء منظمة التعاون الاقتصادي والتنمية OECD، ذلك أنه ليس بالضرورة أن يكون الانحراف عن الأخلاق والسلوك المؤثم معاقب عليه قانونا.[1]

المطلب الثاني: خصائص الجريمة المرتكبة على الانترنت.

تعتبر الجريمة المرتكبة عبر الأنترنت من بين الجرائم المستحدثة التي أتى بها التطور في مجال الاتصالات، فهي تختلف عن الجريمة التقليدية والتي ترتكب في العالم المادي، ولذلك فهي تتميز بخصائص وسمات جعلت منها ظاهرة إجرامية جديدة لم يعرفها العالم من قبل وهي على النحو التالي:

أ) الجريمة المعلوماتية متعدية للحدود (عابرة للوطنية):

إنه وبعد ظهور شبكة المعلوماتية لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينهما آلاف الأميال قد أدت إلى نتيجة مؤدّاها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد، حيث يمكن أن ترتكب الجريمة من المجرم في دولة على المجني عليه في دولة أخرى في وقت يسير جدا.

فالجريمة المعلوماتية بهذا الشكل لا تعرف بالحدود بين الدول وهي بذلك شكل جديد من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة،[2] ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمال

[1] محمد أمين الشوابكة، جرائم الحاسوب والانترنت(الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع الطبعة الأولى، 2009، ص08.

[2] خالد ممدوح إبراهيم، الجرائم المعلوماتية، الدار الفكر الجامعي، الطبعة الأولى، ص88.

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،[1] أو القيام بإعداد أحد البرامج الخبيثة(virus) في بلد ما ثم يتم نسخ هذه البرامج وترسل إلى دول مختلفة من العالم.[2] وتظهر هذه المشكلة بصفة خاصة في التعاملات البنكية عبر شبكات المعلومات الدولية، حيث أدى التوسع الكبير لإجراء التعاملات البنكية عبر شبكات المعلومات الدولية إلى إعطاء بعد دولي لهذه الجرائم ذلك أن ربط وسائل الاتصالات بالحاسبات الآلية ضاعف من المعاملات المالية الدولية والتي أصبحت تتم بواسطة وسائل الكترونية، وبصفة خاصة من خلال التحويل الالكتروني للأموال والتباعد الالكتروني 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.

[1] نائلة محمد فريد قورة، المرجع السابق، ص 52.

[2] و من الأمثلة عن القضايا التي لفتت النظر إلى البعد الدولي والجرائم المعلوماتية القضية عرفت باسم مرض نقص المناعة المكتسبة (ايدز). وتتلخص وقائها أنه في عام 1989 قام أحد الأشخاص بتوزيع من النسخ الخاصة بأحد البرامج الذي يهدف في ظاهره بعض النصائح الخاصة بمرض نقص المناعة المكتسبة. إلى أن هذا البرنامج بحقيقته كان يحتوي على فيروس يترتب على المجرد تشغيله تعطيل الجهاز.

ولقد أثارت هذه الخاصية الدولية للجريمة المعلوماتية عدة إشكالات قانونية تتعلق أساس بتحديد الدولة صاحبة الاختصاص القضائي. في محاكمة مرتكب الجريمة، فهل هي دولة 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 توفيق 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، وأن يشمل هذا التعاون تبادل المعلومات وتسليم المجرمين وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى، ومع ضرورة هذا التعاون والمناداة به إلا أنه تقف أمام هذا المبدأ عقوبات ومعوقات تحول دون تحققه وتجعله صعب المنال، من أهمها انعدام إعادة نموذج موحد للنشاط الإجرامي المكون للجريمة المعلوماتية وأن كثير من القوانين لم يتم تعديلها بحيث تتلاءم مع هذه الجرائم حتى يتسنى إدراجها ضمن الاتفاقيات الدولة الخاصة بتبادل المساعدة الجنائية في مجال الجرائم المعلوماتية، بالإضافة إلى تنوع واختلاف النظم القانونية و الإجرائية.

ب) صعوبة اكتشاف الجريمة المعلوماتية و إثباتها.

تتسم الجرائم الناشئة عن استخدام الإنترنت بأنها خفية مستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من

جريمته بدقّة، مثلا عند إرسال الفيروس المدمر وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم.[1]

فجرائم الإنترنت في أكثر صورها خفية لا يلاحظها المجني عليه أو يدري حتى بوقوعها والإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الالكترونية التي تسجل البيانات عن طريقها أمر ليس في كثير من الأحوال بحكم توافر المعرفة والخبرة في مجال المحاسبات غالبا لدى مرتكبها.

ج) اعتبارها أقل عنفا في التنفيذ:

لا يتطلب هذا النوع من الجرائم في تنفيذها إلى مجهود كبير أو للعنف فهي أقل جهد ممكن مقارنته بالجرائم التقليدية التي تتطلب نوعا ما من الجهد العضلي الذي قد يكون في صورة ممارسته العنف والإيذاء ولهذا نجد هذا النوع من الجرائم يتميز بطبعه لهدوء بل كل ما يحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني فمن هذا المنطق تعد الجريمة المرتكبة من الجرائم النظيفة فلا آثار فيها لأية عنف وإنما مجرد أرقام وبيانات يتم تغييرها من السجلات في ذاكرة الحسابات الآلية وليس لها أثر خارجي مادي.[2]

المطلب الثالث: موقف المشرع الجزائري من الجريمة المعلوماتية.

لم يجد المشرع الجزائري حلا إلا تعديل قانون العقوبات لسد ما كان من فراغ قانوني في هذا المجال و كان ذلك بموجب القانون رقم:15/04 المؤرخ في: 2004/11/10 المتمّم والمعدّل للأمر 156/66 المتضمن قانون العقوبات،[3] والذي أقر له القسم السابع مكرر تحت عنوان: المساس بأنظمة المعالجة الآلية و لقد جاء في عرض أسباب هذا التعديل أن التقدم

[1] محمد عبيد الكعبي، المرجع السابق، ص32.

[2] سيناء عبد الله محسن، المواجهة التشرعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية.

[3] قانون العقوبات الجزائري.

التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام، مما دفع بالكثير من الدول إلى النص على معاقبتها وأن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات وأن هذه التعديلات من شأنها سد الفراغ القانوني.

وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسوب الآلي فتتحول إلى معلومات بعد معالجتها و تخزينها، فقام بحماية هذه المعطيات من أوجه عده لذلك فقد آثر المشرع الجزائري استخدامه لمصطلح المساس بنظم المعالجة للمعطيات، وينصرف هذا المصطلح وفقا لدلالة الكلمة إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكات المعلومات، ليخرج بذلك من نطاق تجريم تلك الجرائم التي يكون النظام المعلوماتية وسيلة لارتكابها، وحصرها فقط في صور الأفعال التي تشكل اعتداء على النظام المعلوماتية، أي الجرائم التي يكون النظام المعلوماتية محلا لها ثم في مرحلة لاحقة اختار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب القانون رقم04/09،[1] المتضمن الوقاية من هذه الجرائم و مكافحتها.

أ) مفهوم نظام المعالجة الآلية للمعطيات:

تبنى المشرع الجزائري للدلالة على الجريمة المعلوماتية مصطلح المساس بأنظمة الآلية للمعطيات معتبرا أن النظام المعلوماتية في حد ذاته أي المحتوى وما يحتويه من مكونات غير مادية محلا للجريمة المعلوماتية، فالمقصود بنظام المعالجة الآلية للمعطيات هي عملية معالجة المعطيات تحتاج إلى آلية منظمة تتولى عمليات جمع وتوفير المعلومات اللازمة ومعالجتها، وهو الأمر الذي ولد الحاجة إلى إجراءات ووسائل تساعد على القيام بذلك فظهر بالنتيجة

[1] القانون رقم04/09 المتضمن الوقاية من هذه الجرائم ومكافحتها.

مصطلح نظم المعلومات المبنية على الحسابات الآلية أو ما يسمى بنظام المعلومات المحسوبة وهو نظام يعتمد على المكونات والأجهزة البرمجية للحاسوب في معالجة المعطيات واسترجاع المعلومات.

فالمشرع الجزائري عند تعديله لقانون العقوبات وإضافته للقسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات عارضا من خلاله صور هذه الاعتداءات لم يعرض نظام المعالجة الآلية للمعطبات، ذلك أن العناصر التي يتكون منها هذا النظام في حالة تطور تكنولوجي مستمر يخضع للتطورات السريعة والمتلاحقة التي تطرأ على البيئة التقنية التي يمثلها والتي تتسع لإمكانية شمول وسائل تقنية جديدة، لاسيما وأن العالم الافتراضي لا يزال في بدايته و لن يكون من السهولة احتواؤه، ومن جهة أخرى فإن نظام المعالجة الآلية للمعطيات يعد تعبيرا فنيا يصعب على المشتغل بالقانون إدراك طبيعته.

وبالرغم من ذلك فقد ذهب بعض الدول إلى وضع تعريف للنظام المعلوماتية في قوانينها الدخيلة ذات صلة، كالقانون الأمريكي الموحد للمعاملات الالكترونية لسنة 1999، قانون مكافحة جرائم المعلوماتية السعودي الصادر بتاريخ:2007/03/26،[1] قانون سلطنة عمان رقم 2006/69،[2] الخاص بالمعاملات الالكترونية الصادر بتاريخ:2008/05/17.

أما على المستوى الدولي فإن الاتفاقية الدولية لإجرام تقنية المعلومات وقفت عند حد هذا المفهوم عندما عرفت نظام المعالجة الآلية للمعطيات بموجب الفقرة "أ" من المادة الأولى من الفصل الأول بعنوان المصطلحات على أنه كل آلة بمفردها أو غيرها من الآلات المتصلة أو

[1] عرف نظام مكافحة الجرائم المعلوماتية للمملكة العربية السعودية الصادر بتاريخ: 2007/03/26 بأنه مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها وتشمل الحاسبات الآلية.

[2] المادّة الأولى من هذا القانون عرفت النظام المعلوماتية بأنه نظام الكتروني للتعامل مع المعلومات والبيانات.

المرتبطة والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذا لبرنامج معيّن بأداة معالجة آلية للبيانات.

فمن خلال التعريفات نستنتج أن مصطلح نظام المعالجة الآلية يستخدم في الحقل القانوني للدلالة على المعنى المفصود نفسه بهذا المصطلح وفقا لمفهومه العلمي، فهو إذن مصطلح ينطبق على أي نظام مهما كان مسماه يتوفر له عدة عناصر مرتبطة ببعضها بعدد معين من الروابط لتحقيق المعالجة الآلية للمعلومات من تجميعها وتخزينها ومعالجتها و نقلها وتبادلها و ذلك من خلال برنامج معلوماتي.

ب)المقصود بالجرائم المتصلة بتكنولوجيا الإعلام و الاتصال:[1]

إنه وقبل صدور القانون رقم04/09/ المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها كانت الجريمة المعلوماتية في النظام العقابي الجزائري تقتصر فقط على تلك الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وعي وفقا لدلالة الكلمة تنصرف إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكة المعلومات وهذه الأفعال في الحقيقة ما هي إلا جزء من الظاهرة الإجرامية لأجل هذا ففقد تبنى المشرع الجزائري حديثا بموجب القانون 04/09 تعريفا موسعا للجرائم المعلوماتية واعتبر أنها تشتمل بالإضافة إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات من المادة394 مكرر إلى المادة 394 مكرر 07 أي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الالكترونية، وبذلك لم يعد مفهوم الجريمة المعلوماتية في التشريع الجزائري يقتصر على الأفعال التي تكون فيها المنظومة المعلوماتية في التشريع الجزائري يقتصر على الأفعال التي تكون فيها المنظومة المعلوماتية

[1] القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

محلا للاعتداء بل توسع نطاقها لتشتمل إضافة إلى ذلك تلك الأفعال التي تكون المنظومة المعلوماتية وسيلة لارتكابها.

المبحث الثاني: الطبيعة القانونية للجريمة المعلوماتية.

تعتبر أركان الجريمة المعلوماتية جزء لا يتجزّأ عن طبيعتها وتخلف أحدها يؤدي إلى انتفاء الجريمة، حيث يتطلب القانون كأصل عام وجود ركن مادّي وركن معنوي وركن شرعي بموجبه يتمّ التجريم والعقاب وهو الأمر المعمول به في كل الجرائم التقليدية كانت أو مستحدثة، فبالرغم من أنه في الجرائم التقليدية هناك رأي يلغي الركن الشرعي واكتفائه بالركن المادي والمعنوي بحجة أن الركن الشرعي هو الذي يحدد هذه الأركان غير أن في الجريمة المرتكبة عبر الأنترنت يجب أن تتوفر فيها والاعتماد على الأركان الثلاثة لتحديد الجريمة.

المطلب الأول: أطراف الجريمة المعلوماتية.

لقد أضافت المعلوماتية الكثير من الجوانب الإيجابية إلى حياتنا، إلا أنها في المقابل جلبت معها شكلا جديدا من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية، فلم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز هذه الجريمة عن غيرها من الجرائم التقليدية فحسب، بل كان له أثره أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين التقليدين.

أ-خصائص المجرم المعلوماتي:

يتميز المجرم المعلوماتية عن غيره من المجرمين بصفات وسمات معينة جعلت منه محل العديد من الأبحاث والدراسات، واختلف الباحثون في تحديد هذه الخصائص كما اختلفوا

في مدى انطباق وصف جرائم ذوي الباقات البيضاء،[1] على مجرمي المعلوماتية ذلك أن كلا من هؤلاء المجرمين قد يكون من ذوي الكفاءات، و لهم القدرة على التكيف الاجتماعي.

ومع ذلك يمكن أن نستخلص من هذه الأبحاث،[2] مجموعة من السمات التي يتميز بها المجرم المعلوماتية والتي يساعد التعرف عليها في مواجهة هذا النمط الجديد من المجرمين ومن أهم هذه الصفات:

1/الذكاء: يعتبر الذكاء من أهم صفات مرتكب الجرائم المعلوماتية، لأن ذلك يتطلب منه المعرفة التقنية ل: كيفية الدخول إلى أنظمة الحاسب الآلي والقدرة على التعديل والتغيير في البرامج لذلك عادة ما يذكر أن الإجرام ألمعلوماتي هو إجرام الأذكياء وذلك مقارنة بالإجرام التقليدي الذي يميل إلى العنف،[3] فهذا المجرم لا يمكن أن ينتمي إلى طائفة المجرمين الأغبياء، فمن يستعين بجهاز الحاسوب للاستيلاء على أسرار بنك أو شركة مخزنة به لا بد أن يتميز بالمستوى الرفيع من الذكاء حتى يمكنه أن يتغلب على كثير من العقبات التي تواجهه في ارتكاب جريمته.

[1] مصطلح المجرمين ذوي الباقات البيضاء مصطلح حديث نسبيا وأول من أطلقه هو عالم الاجتماع Sutherlanc أين وضح أن هذه الجرائم ترتكب من قبل الطبقة الراقية في المجتمع وذوي المناصب الإدارية الكبيرة وتشمل أنواعا مختلفة من الجرائم كغسل الأموال وغير ذلك من الجرائم التي يقومون بارتكابها وهم جالسون في مكانهم.

[2] يعد الأستاذ Parker واحدا من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة و بالمجرم المعلوماتي بصفة خاصة، ويرى الأستاذ Parker بداءة أن المجرم المعلوماتي وإن كان يتميز ببعض السمات الخاصة به إلا أنه لا يخرج في المهاية عن كونه مرتكبا لفعل إجرامي يستوجب توقيع العقاب عليه، ويرمز الأستاذ باركر لهذه الصفات بكلمة SKRAM وهي تعني المهارة(SKILLS)، المعرفة(Knowledg) الوسيلة(Resours)، السلطة(Autority) وأخيرا الباعث(Motives).

[3] غنام محمد غنام، الحماية الجنائية لبطاقات الائتمان الممغنطة، مؤتمر الجوانب القانونية والأمنية للعمليات الالكترونية، دبي 2003، ص05.

وتتجلى أهمية صفة الذكاء بالنسبة لمرتكب الجريمة المعلوماتية في عدم استخدامه للعنف في ارتكابه للجريمة، فالسلوك الإجرامي ينشأ من تقنيات التدمير الناعمة(Sabotage soft).

فيكفي أن يقوم المجرم المعلوماتي بالتلاعب ببيانات و برامج الحاسب الآلي لكي يمحو أو يدمر هذه البيانات أو يعطل استخدام هذه البرامج.

2/المهارة:

تعد المهارة المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات أو بمجرد التفاعل الاجتماعي مع الآخرين، ومستوى المهارة التي يكون عليها المجرم المعلوماتي هي التي تحدد الأسلوب الذي يرتكب به الجرائم، بحيث إذا كان الشخص مرتكب الجريمة المعلوماتية على قدر ضئيل من مستوى المهارة نجد أن الجرائم التي قد يرتكبها لا تتعدى الإتلاف المعلوماتي أو نسخ البيانات والبرامج،[1] أما إذا كان المجرم المعلوماتي على درجة أعلى في المستوى المهاري فإن أسلوب ارتكابه للجرائم يختلف، إذ يمكنه عن طريق استخدام الشبكات بالدخول إلى أنظمة الحاسب الآلي لسرقة الأموال وارتكاب جرائم تجسس وزرع الفيروسات وغيرها من الجرائم التي تتطلب مهارة عالية في ارتكابها.

كما أن المهارة التي يتميز بها المجرم المعلوماتي تمكنه من تكوين تصور كامل لجريمته، إذ يستطيع أن يطبق جريمته على أنظمة مماثلة كتلك التي يستهدفها و ذلك قبل تنفيذ جريمته، حتى لا يتفاجأ بأمور غير متوقعة من شأنها إفشال مخططاته أو الكشف عنها، فعادة ما يلجأ المجرم المعلوماتي إلى التمهيد لارتكاب جريمته بالتعرف على المحيط الذي تدور فيه،

[1] خالد محمود إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص1354.

وكذا الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، ويساعده في ذلك درجة المهارة التي يتمتع بها.[1]

3/التنظيم والتخطيط:

تتميز الجريمة المعلوماتية عادة بوجود أكثر من فاعل للنشاط الإجرامي الواحد إذ ترتكب أغلب الجرائم المعلوماتية من عدة أشخاص يحدد لكل شخص منهم دور معين، ويتم العمل بينهم وفقا لتخطيط وتنظيم سابق على ارتكاب الجريمة، فقد تحتاج جريمة نسخ برامج الحاسب الآلي مثلا إلى من يقوم بنسخ تلك البرامج وإلى من يقوم بعملية بيعها، كما أنه من الملاحظ أن الأشخاص الذين يقومون بخلق أو تعديل البرامج لأغراض غير مشروعة ليسوا دائما المستفيدين بطريقة مباشرة من النشاط الإجرامي، فجرائم المعلوماتية تتطلب عادة شخصين على الأقل أحدهما متخصص في الحاسبات الآلية يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط ذاته أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل ا لمكاسب،[2] وأحيانا أخرى يمكن تجنيد المجرم المعلوماتي القادر على اختراق نظم المعلومات ضمن عصابات الجريمة المنظمة عن طريق شبكة الأنترنت، ويمكن من خلال هذه الشبكة تبادل أفكار ومعلومات التطرف والإرهاب، كما يمكن الاتفاق معه على ارتكاب إحدى الجرائم الأخلاقية أو التلاعب في الحسابات أو بطاقات الائتمان.....[3]

4/المجرم المعلوماتي يبرر أركان جريمته:

أثبتت بعض الدراسات أنه لا يوجد شعور لدى المجرم المعلوماتي بعدم أخلاقية ما يقوم به أو بمساسه بمصالح أو قيم يحرص المجتمع على حمايتها بل لا يعتبر أن ما يقوم به يدخل

[1] نائلة محمد فورة، المرجع السابق، ص58.

[2] المرجع نفسه، ص61.

[3] عبد الفتاح بيومي حجازي، المرجع السابق، ص105.

في عداد الجرائم، خاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، لذلك فإن كثير من العاملين في مجالا المعلوماتية لا يجدون أي خطأ في استعمال الشيفرات السرية الخاصة بالدخول إلى أنظمة الحاسبات الآلية بطريقة غير مشروعة، أو في نسخ البرامج بدلا من شرائها واستعمالا لحاسبات الآلية للمؤسسات التابعين لها لأغراض شخصية و ما ساعد على نماء هذا الشعور هو عدم وجود احتكاك مباشر بين الجاني والمجني عليه، فالتباعد في العلاقة الثنائية هذه يسهل المرور إلى الفعل غير المشروع و يساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل.

إلا أن الشعور بعدم أخلاقية هذه الأفعال الإجرامية المعلوماتية لدى فئة من المجرمين المعلوماتيين لا ينفي وجود مجرمين يرتكبون الإجرام المعلوماتي وهم على علم ودراية وإدراك بعدم مشروعية و لا أخلاقية هذا الفعل.

أ) أصناف المجرم المعلوماتي

إن التسارع الرهيب في مجال التقنيات الرقمية الحديثة ساهم بدوره في التطور السريع لأنماط جريمة تقنية المعلومات بصفة عامة مما أصبح عائقا أمام دراسات علم الإجرام الحديثة التي تسعى إلى وضع تصنيف ثابت لمجرمي المعلوماتية.

إلا أنه ومن خلال تلك الملامح السابق ذكرها في خصائص المجرم المعلوماتي يمكن تصنيف مرتكبي الجرائم المعلوماتية إلى مجموعة من الطوائف، ولا يعني بطبيعة الحال أن كل مجرم يندرج ضمن طائفة محددة دون غيرها، بل يمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة أو فئة، و سوف نتناولهم بشيء من التفصيل كما يلي:

1. فئة صغار مجرمي المعلوماتية:

أو كما يسميهم البعض صغار نوابغ المعلوماتية (Pranksters) وتضم هذه الطائفة الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح دون أن تكون لديهم نية إحداث أي ضرر بالمجني عليهم، وذلك عن طريق استخدام حاسبات آلية محمولة خاصة بهم أو حاسبات آلية خاصة بمدارسهم، ومن بينهم فئة لم تبلغ بعد سن الأهلية مفتونين كثيرا بالتقنيات الرقمية وهم غالبا ما يكونون في مرحلة المراهقة، وعلى الرغم من صغر سنهم إلا أنهم قادرون على اقتحام كافة أنواع الأنظمة المعلوماتية، وقد أثارت هذه الفئة جدلا واسعا في الوسط الفقهي، ففي حين كثر الحديث عن مخاطر هذه الفئة،[1] التي يمكن أن تتحول إلى فئة القراصنة عندما يصبحون على درجة عالية من الخبرة والمهارة فيتم استئجارهم واستغلالهم في أعمال ذات أهداف إجرامية، ذهب جانب من الفقه أنه من الأحسن عدم تصنيف هؤلاء ضمن دائرة الإجرام لما لديهم من ميل للمغامرة والرغبة في البحث والاستكشاف.

2. فئة القراصنة أو المخترقون: ويمكن تقسيمهم إلى صنفين:

[1]من أشهر الجرائم التي ارتكبت في الو .م .أ جريمة مراهق لم يتجاوز سنه 17 عاما يدعى"دينيسموران" والذي اختار لنفسه اسم"كوليو": حيث قام كوليو بشن سلسلة من الهجمات الالكترونية على مواقع مهمة أنشأتها الحكومة الأمريكية على شبكة الأنترنت، ومنذ نهاية1999 وبداية 2000 استطاع كوليو أن يحول حياة المسؤولين عن هذه المواقع إلى جحيم حيث دأب على مهاجمة موقع (DARE ORG) المسؤول عن مواجهة مخاطر الإدمان ونفذ عمليات تجريبية عليه، و كذلك قضية تلاميذ المدرسة الثانوية في ولاية مانهاتن الذين استخدموا طرفيات غرف الدرس للدخول إلى شبكة الاتصالات ودمروا ملفات زبائن الشركة في هذه العملية، وأيضا نجحت مجموعة من طلبة المدارس العليا بال و.م.أ تتراوح أعمارهم بين 15 و 25 سنة يطلقون على أنفسهم أسرة المجموعة (414) في اختراق أنظمة نحو(60) حاسبا و ذلك عام 1983 ومن بينها حاسبات وبنوك معلومات مختبر في لوس أنجلس وكذلك في مركز Salan Kottering لعلاج الأورام في نيويورك ومعهد ماسا شوسيتي للتقنية و قاعدة ماك كيلان للقوات الجوية.

الهاكار (les hakers):[1]

وهم المتطفلون الذين يتحدّون أمن النظم المعلوماتية والشبكات من خلال الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض، وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية و إنما ينطلقون من هدف اكتساب الخبرة أو بدافع الفضول أو لمجرد التحدي و إثبات الذات.[2]

الكراكر (les crakers):

هم أشخاص يقومون بالتسلل إلى أنظمة المعالجة الآلية للإطلاع على المعلومات المخزنة بها لإلحاق الضرر أو البعث بها أو سرقتها وذلك بهدف التحدي الإبداعي،[3] وتتميز هذه الفئة بسعة الخبرة والإدراك الواسع للمهارات التقنية، لذلك فقد أثبت الواقع العملي أن الهاكر يستعين بالكراكر إذا ما صادفه أي نوع من أنواع الحماية، وغالبا ما يكون هدف هذه الفئة هو الحصول على المال أو بغرض الشهرة.

فئة المحترفين:

وتعد هذه الفئة هي الأخطر من بين مجرمي التقنية بحيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي سواء لهم أو للجهات التي سخرتهم لارتكاب جرائم تقنية المعلومات، فضلا عن تحقيق أغراض سياسية أو التعبير عن موقف فكري أو فلسفي، ويلاحظ أن الأضرار التي تترتب عن هذه الأفعال تكون بالغة الضرر بعكس الفئات الأخرى، كما أن مواجهتهم تتسم بالصعوبة بما يتمتعون به من كفاءات عالية في مجال المعلوماتية ومواكبتهم للتقنية ذاتها،

---

[1] عرفت اتفاقية الأمم المتحدة لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم(55/63) المؤرخة في 2000/04/12الهاكر (المحترف) بأنه المبرمج المتفوق جدا و لكنه يستخدم جل طاقته في الاتجاه الغير شرعي لمحاولة اختراق أنظمة حاسوبية بهدف إثبات قدرته أو التباهي بها و أحيانا لأهداف إجرامية.

[2] مصطفي محمد موسى، التحقيق في الجرائم الالكترونية، مطابع الشرطة، ط1، ص15.

[3] في سنة 1995 تم إلقاء القبض على أكبر هاكرو يدعى "كيفين منتيك: حيث قام على مدار 20 سنة بارتكاب عدد كبير من الجرائم الالكترونية إذ كان بإمكانه الدخول إلى أي نظام معلوماتي مرتبط بأجهزة الكمبيوتر وتعلم كسر كلمة المرور بسلامة فائقة.

ويعمل المنتمون إلى هذه الطائفة ف أغلب الأحوال بطريقة منظمة بحيث ينطبق على أفعالهم وصف الجريمة المنظمة أو على الأقل يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل.

فئة الحاقدين:

وهم فئة لا يسعون إلى الإشادة بالتفوق العلمي مثل صغار نوابغ المعلوماتية و لا إلى تحقيق مكاسب مادية كفئة المحترفين، وإنما هدفهم هو الانتقام كأثر لتصرف صاحب العمل معهم أو تعبيرا منهم على غضبهم من هيئة معينة.

المطلب الثاني: أساليب و دوافع ارتكاب 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، فإن 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 و الدراية 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 الالكترونية غير المرئية التي تنساب عبر أجزاء نظم المعالجة الآلية وشبكات الاتصال العالمية، وتبعا لذلك فإنه لما 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.

أ) أساليب ارتكاب الجريمة المعلوماتية:

تشابه 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 خداع الحاسب الآلي و التحايل 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 أنه لا يمكن التنبؤ بالوسائل الفنية والتقنية التي قد تستحدث في مجال تكنولوجيا المعلومات،[1] ولعل من أهم هذه التقنيات هي الاختراق واستعمال البرامج الخبيثة (Vérus)[2] وسنحاول شرح ذلك فيما يلي:

أولا: 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 مشروعة.[3]

البرامج الخبيثة"Les virus": تعد الفيروسات بمثابة المرض المعدي الذي يصيب المعطيات فيقضي عليها أو يشوهها فتذهب في كلتا الحالتين بفائدتها ، وفيروس الحاسب الآلي يشبه إلى حد كبير الفيروس الذي يصيب الإنسان لقدرته على الانتقال من حاسب إلى آخر،[4] والفيروس في مجال المعلوماتية هو برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي بصمم بشكل يجعل منه قادرا على التكاثر ونسخ نفسه إلى نسخ كثيرة والانتشار من نظام إلى آخر عبر شبكات الاتصال والقدرة على الاختفاء داخل برنامج سليم بحيث يصعب اكتشافه،كما أنه

---

[1] نهلا المومني، المرجع السابق، ص125.

[2] نهلا المومني، المرجع السابق، ص40.

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

– المستوى الأول: يعرف بهجوم قنبلة صندوق البريد و يؤدي 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 و نسخ الملفات السرية.

[4] محمد خليفة، المرجع السابق، ص50.

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 الأنترنت، وكذلك عند تبادل البريد الالكتروني 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:

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

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

ومن الآثار التي يخلفها الفيروس و التي 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، الفيروسات الثغرات.....

[1] سامي الشوا، المرجع السابق، ص190.

ب) دوافع ارتكاب الجريمة المعلوماتية:

إن الباعث أو الدافع هو العامل المحرك للإرادة التي توجه السلوك الإجرامي، وغالبا ما تتجه التشريعات العقابية إلى عدم اعتبار الدافع (الباعث) عنصرا من عناصر التجريم إلا في الأحوال التي يحددها القانون صراحة، فالجريمة تقوم بتحقيق عناصرها و أركانها أيا كان الباعث من وراء ارتكابها.

والحقيقة أنه مهما كانت درجة الدقة في رسم حدود كل طائفة من الطوائف التي ينتمي إليها مجرمو المعلوماتية فإن الدوافع الرئيسية على ارتكاب الجريمة المعلوماتية تتنوع وتتباين تبعا لطبيعة ودرجة خبرته في مجال المعلوماتية، ولا تخرج بأي حال من الأحوال على ثلاث بواعث تحرك المجرم المعلوماتي، أما الباعث الأول فتشترك فيه الجريمة المعلوماتية مع غيرها من جرائم الاعتداء على الأموال بصورتها التقليدية وهو الرغبة في تحقيق الربح وكسب المال وأما الباعثان الآخران اللذان يميزان الجريمة المعلوماتية عن غيرها من الجرائم فيتمثل الأول في الرغبة في الدخول إلى الأنظمة المعلوماتية للحاسبات الآلية والمعلومات التي تحتويها بدافع المتعة والتسلية، وكذا الرغبة في إثبات الخبرة التقنية التي يتمتع بها الفاعل أو غير ذلك من الأغراض التي لا يكون السعي فيها إلى تحقيق ربح مادي أو الإضرار بهذه الأنظمة، ويتمثل الثاني في الرغبة في الإضرار بهذه الأنظمة، وفي كل الأحوال فقد ذهب الفقه القانوني إلى إرجاع مصدر هذه الدوافع إلى نوعين دوافع شخصية و أخرى خارجية.

- **الدوافع الشخصية:** ويمكن رد الدوافع الشخصية لدى المجرم المعلوماتي إلى دوافع مادية وأخرى ذهنية.

1-الدوافع المادية(تحقيق الربح و كسب المال):

يعد الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة المعلوماتية، وذلك أن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم المعلوماتي إلى تطوير نفسه حتى يواكب كل حديث يطرأ على التقنية المعلوماتية ويقتنص الفرص ويسعى إلى الاحتراف حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك أثرا وراءه،[1] فيعمد الجاني رغبة منه في تحقيق الثراء والكسب المادي إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية إن كان أحد موظفيها، أو اختراق نظم المعالجة الآلية لها من خلال اكتشافه لفجواتها الأمنية، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية لحسابه أو لحساب شركائه أو لحساب من يعمل لحسابهم إن كان من خارج المؤسسة، كما يمكن الحصول على المكاسب المادية من خلال المساومة على البرامج أو المعلومات المتحصل عليها بطريق الاختلاس من جهاز الحاسوب، ولقد أشارت في هذا الإطار مجلة(Sécurité informatique) وهي مجلة متخصصة في الأمن المعلوماتي أن 43% من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال، و23% من أجل سرقة معلومات و19% أفعال إتلاف و15% الاستعمال الغير مشروع للحاسوب لأجل تحقيق منافع شخصية.[2]

وفي حقيقة الأمر أنه في حال نجاح المجرم المعلوماتي في ارتكاب جريمته المعلوماتية فإن ذلك يدري عليه أرباحا كبيرة في زمن قياسي ويمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة اقترافه هذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول جرائم الكمبيوتر، أين أجريت هذه الدراسة

[1] وضاح محمود الحمود و نشأت مفضي المجالي، جرائم الأنترنت، دار المنار للنشر، عمان، 2005، ص30.

[2] نهلا عبد القادر المومني، المرجع السابق، ص90.

بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية وبنوك ومؤسسات مالية ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن جرائم المعلوماتية، فقد تبين أن 85% من المشاركين في الدراسة تعرضوا لاختراقات للأنظمة المعلوماتية و أن 64 % لحقت بهم خسائر مادية جراء هذه الاعتداءات.[1]

1. الدوافع الذهنية(المتعة والتحدي والرغبة في فهم النظام المعلوماتي وإثبات الذات):

قد تكون الدوافع لارتكاب الجريمة المعلوماتية مجرد الشغف بالالكترونيات والرغبة في تحدي وقهر النظام و التفوق على تعقيد وسائل التقنية، فاختراق الأنظمة الالكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبيها والتسلية تغطي أوقات فراغه.

وعلى صعيد آخر قد يكون إقدام المجرم المعلوماتي على ارتكاب جريمته بدافع الرغبة في قهر الأنظمة الالكترونية والتغلب عليها، إذ يميل المجرم هنا إلى إظهار تفوقه على وسائل التكنولوجيا الحديثة وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية وإنما ينطلق من دافع التحدي وإثبات المقدرة.[2]

- الدوافع الخارجية:

قد يتأثر المجرم المعلوماتي ببعض المواقف قد تكون دافعة له على اقتراف الإجرام المعلوماتي ولا يسعى في ذلك حينها لا للمتعة والتسلية ولا لكسب المال، ويمكن إبراز أهم هذه الدوافع فيما يلي:

---

[1] وضاح محمود الحمود، المرجع السابق، ص31.

[2] ومن أشهر القضايا التي وقعت في مثل هذه الحالة قضية كان قد تعامل معها مكتب التحقيقات الفدرالي أطلق عليها اسم مجموعة الجحيم العالمي(Global Hell) تتلخص في تمكن مجموعة من الأشخاص من اختراق مواقع البيت الأبيض والشرطة الفدرالية الأمريكية والجيش الأمريكي ووزارة الداخلية الأمريكية وقد ظهر من التحقيقات أن هذه المجموعة تهدف إلى مجرد الاختراق أكثر من التدمير أو التقاط المعلومات الحساسة.مشار إلى هذه القضية لدى رشيدة بوكر/مرجع سابق، ص95.

1-دافع الانتقام:

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

2-دافع التعاون والتواطؤ:

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

وإذا كانت هذه أبرز الدوافع لارتكاب أنشطة الاعتداء على نظم المعالجة الآلية، ومع ذلك فهي ليست ثابتة ومعتمدة لدى الفقهاء والباحثين لأن السلوك الإجرامي والدوافع لارتكاب الجريمة قد تتغير وتتحول بسرعة من حالة العبث ومحاولة التحدي والتغلب على الأنظمة إلى تدميرها أو على الأقل حيازتها للقيام بعملية الابتزاز والحصول على الأموال لذلك فإن دوافع في ارتكاب جرائم المعلوماتية قد لا يتوقف عند هذا الحد إذ نجد في كل جريمة جديدة دوافع جديدة،

[1] سامي الشوا، المرجع السابق، ص52.

[2] أحمد خليفة اللط، المرجع السابق، ص90.

بل كثيرا ما نجد الجريمة الواحدة لها دوافع متعددة خاصة ما إذا اشترك فيها أكثر من شخص أو أكثر من جهة بحيث يسعى كل منهم لتحقيق مآربه الخاصة.[1]

المطلب الثالث: المجني عليه في الجريمة المعلوماتية.

إن من نتائج ثورة التقنية المعلوماتية انتشار الوسائل المعلوماتية في جميع الأنشطة التي تزاول في المجتمعات الحديثة،[2] إذ أصبحت المعلوماتية من لوازم الحياة المتطورة تعتمد عليها المؤسسات الحكومية أو الخاصة في تسيير أعمالها بشكل أساسي وأصبحت نتيجة لذلك مستودعا لأسرارها، ولما كانت الجرائم المعلوماتية تقوم أساسا نتيجة الاعتداء على المعلومات فإن ذلك أدى إلى تنوع وتعدد فئات المتضررين من الجريمة المعلوماتية من جهة وازدياد حجم الأضرار المالية التي تخلفها[3] من جهة أخرى.

الفرع الأول: الضحية في الجريمة المعلوماتية.

لقد حدد الإعلان العالمي الخاص بالمبادئ الأساسية لتوفير العدالة لضحايا الجريمة وإساءة استعمال السلطة الذي اعتمدته الجمعية العامة للأمم المتحدة بقرارها رقم 401434 الصادر بتاريخ 1985/11/29 مصطلح الضحية والذي جاء شاملا لكل من المجني عليه والمتضرر من الجريمة.

فوفقا لهذا الإعلان المشار إليه يقصد بالضحية الأشخاص الذين أصيبوا بضرر فردي أو جماعي بما في ذلك الضرر البدني أو العقلي أو المعاناة النفسية أو الخسارة الاقتصادية أو

---

[1] رشيدة بوكر، المرجع السابق، ص96.

[2] محمد علي العريان، الجرائم المعلوماتية. دار الجامعة الجديدة للنشر، 2004، ص67.

[3] في مناسبة مناقشة مجلس النواب الأمريكي على القانون الذي يسمح بتطبيق السجن مدى الحياة لمرتكبي جرائم تقنية المعلومات الشريرة أدلى رئيس اللجنة الفرعية المسؤولة عن الجريمة في الكونغرس الأمريكي لامار سميت بتصريح للتدليل على الخسائر الاقتصادية التي تلحق الو. م .أ من جراء الجريمة المعلوماتية :" ما لم نستطع تأمين بنيتنا التحتية الإلكترونية فإن كل ما يحتاجه المجرم الإلكتروني لتعطيل اقتصادنا. هو نقرة بسيطة على الجهاز الحاسوب والاتصال عن طريق الإنترنت".

الحرمان بدرجة كبيرة من التمتع بحقوقهم الأساسية، عن طريق أفعال أو حالات إهمال تشكل انتهاكا للقوانين الجنائية النافذة في الدول بما فيها القوانين التي تحرم الإساءة لاستعمال السلطة، كما يشمل المصطلح أيضا حسب الاقتضاء العائلة المباشرة للضحية الأصلية أو فاعليها المباشرين والأشخاص الذين أصيبوا بضرر من جراء تدخل لمساعدة الضحايا في محنتهم أو لمنع الإيذاء.

يبنى على ذلك أن الضحية في الجريمة بصفة عامة كل شخص طبيعي أو معنوي أصيب بخسارة أو ضرر أو بعدوان نتيجة ارتكاب جريمة سواء بفعل أو بالامتناع عن فعل. أما المقصود بالضحية في الجريمة المعلوماتية هو كل شخص أصابه ضرر مادي أو معنوي نتيجة الاستخدام غير المشروع لتقنية المعلومات، وقد يكون شخصا عاما ممثلا في مؤسسات الدولة وهيئتها وقد يكون خاصا ممثلا في الأشخاص الطبيعية أو المعنوية، و بحسب ذلك فإن الضحايا في الجريمة المعلوماتية يختلفون عن الضحايا في الجرائم التقليدية من مجرد كونهم أشخاصا عادية إلى مؤسسات مالية أو عسكرية أو قطاعات حكومية كان المجرم التقليدي لا يستطيع ارتكاب أي جرائم فيها أو في مواجهتها .

فنظرا لطبيعة استخدام تقنية المعلومات في جميع المعاملات الاقتصادية والمالية الوطنية والدولية والاعتماد عليها في تسيير شؤون الحياة اليومية بالنسبة للأفراد والشؤون العامة بالنسبة للحكومات كان من شأن ذلك أن يضفي أبعادا غير مسبوقة في توسع دائرة المتضررين من الجرائم المعلوماتية وتعدد فئاتهم.

ويلاحظ أنه من الصعوبة بما كان تقدير حجم الجريمة المعلوماتية بتحديد ضحايا هذه الجريمة على وجه الدقة، وربما يرجع ذلك إلى مجموعة من العوامل منها ما يتعلق بالجريمة المعلوماتية ذاتها ومنها ما يتعلق بالضحايا أنفسهم، فأما العوامل المتعلقة بالجريمة المعلوماتية فإن أهمها هو عدم وجود تعريف يحظى بقبول عام للجريمة المعلوماتية وهو ما يقف عائقا أمام

الدراسات الإحصائية التي تهدف إلى بيان حجم الجريمة المعلوماتية، ذلك أن تحديد ما يعد جريمة معلوماتية يختلف من دولة إلى أخرى بالإضافة إلى أن الطبيعة التقنية التي تتميز بها الجريمة المعلوماتية والتي يوفرها لها الحاسب الآلي بما يتمتع به من سرعة فائقة و قدرة عالي على التخزين يجعل من اكتشافها أمرا في غاية الصعوبة فكثيرا من الجرائم المعلوماتية قد تم اكتشافها عن طريق الصدفة. [1]

وأما العوامل المتعلقة بالضحايا فيتمثل أهمها في إحجام المجني عليه عن الإبلاغ على الجريمة المعلوماتية خوفا من الفضيحة، والسبب في ذلك هو أن أكثر الجرائم المعلوماتية تقع داخل المؤسسات المالية وأكثر ما يحرص عليه القائمون على هذه المؤسسات هو السمعة المالية للمؤسسة ولذلك فهم يفضلون تحمل الخسائر التي قد تلحق بهم بسبب هذه الجرائم على ألا يعرف المتعاملون معهم بأن النظم المعلوماتية في المؤسسة قد تم التلاعب بها نتيجة لقصور ما .

وعلى الرغم من عدم دقة الإحصائيات التي تتعلق بتحديد حجم الجريمة المعلوماتية إلا أنها تساعد في إعطاء مؤشر واضح عن مدى اتساع دائرة المتضررين منها وسوف نقوم بعرض أهم فئات المجني عليهم في مجال الجريمة المعلوماتية .

أولا: المؤسسات المالية والجهات الحكومية:

ينجذب مرتكبو الجرائم المعلوماتية إلى القطاعات المالية مثل البنوك والمؤسسات المالية لتنفيذ أفعالهم الإجرامية، فهي من أكثر الأماكن استهدافا نظرا لما لها من أموال، ومن أهم هذه المؤسسات المالية البورصة. وذلك أن أي تعطيل في حركة البورصة يؤثر بدرجة كبيرة على

[1] نائلة محمد فريد قورة، المرجع السابق، ص80.

حجم التعاملات المالية ليس فقط بين الأشخاص العاديين بل قد يصل الأمر إلى التعاملات المالية بين الدول[1].

وقد تعدت حدود الجرائم المعلوماتية القطاعات المدنية إلى المساس بصورة أكبر إلى القطاعات الخاصة بالقوات المسلحة نظرا لطبيعة وأهمية المعلومات التي تحتويها تلك القطاعات وهو ما يبرزه الاهتمام المنصب على الجاسوسية العسكرية وما استتبعه من ظهور حرب من نوع جديدة وهي الحرب المعلوماتية، تعتمد آلياتها على شبكات الحاسب الآلي في نقل المعلومات فتعاظم دور النظم المعلوماتية في هذا المجال نظرا لحتمية وأهمية تخزين البيانات وسرعة معالجتها وعرضها بصورة مناسبة أما القادة لاتخاذ القرار على أساس أهمية تلك المعلومات، مما جعل الدول تبادر إلى القيام بالتجسس على الدول الأخرى للحصول منها على المعلومات التي تجعلها قادرة على مواجهتها.

ثانيا: الأشخاص الطبيعيون:

لا يقتصر تصنيف ضحايا جرائم المعلوماتية على القطاعات المالية والهيئات الحكومية والمؤسسات العسكرية فقط، بل يتعدى كذلك إلى الأشخاص الطبيعيين. فكثيرا ما تعد شبكة الانترنت المجال الخصب لارتكاب تلك الجرائم ضدهم سيما ما يتعلق بالمساس بحق الخصوصية والبيانات الشخصية للأفراد، كما تعتبر جرائم الإتلاف المعلوماتية عن طريق الفيروسات من أكثر الجرائم التي يتعرض لها الأشخاص الطبيعيون عبر بريدهم الالكتروني والذي يعتبر من أهم البوابات التي يقفز منها القراصنة إلى أجهزة الحواسيب الخاصة بالأشخاص. [2]

[1] خالد ممدوح إبراهيم، المرجع السابق، ص150.

[2] استغل بعض الأشخاص الحادث الإرهابي في الولايات المتحدة الأمريكية في 2011/09/11 بإنشاء عدة مواقع على شبكة الانترنت بغرض جمع التبرعات، فأدى ذلك إلى وقوع الكثير من الشعب الأمريكي ضحية نصب.

ثالثا: مقدمي الخدمات الوسيطة في نطاق شبكة الانترنت:

وهم الأشخاص الذين يساعدون على الوصول إلى شبكة الانترنت، فقد يمكن أن يكون الأشخاص الوسطاء ما بين الزبون (العميل)، وما بين شبكة الانترنت ضحايا للجريمة المعلوماتية وهؤلاء الأشخاص هم:

1/ متعهد الوصول: وهو أي شخص طبيعي أو معنوي يقوم بدور فني لتوصيل الجمهور المستخدم إلى شبكة الانترنت وذلك عن طريق عقود اشتراك توصيل الزبون بالمواقع التي يريدها[1] وهو بذلك يقوم بدور فني بحت ولا علاقة له بالمادة المعلوماتية التي تصل إلى الزبون.

2/ متعهد الإيواء l 'hébergeur: وهو أي شخص طبيعي أو معنوي يعرض إيواء صفحات الواب على حساباته الخادمة العملاقة وذلك مقابل أجر، فهو بمثابة مؤجر لمكان على الشبكة للزبون الذي ينشر ما يريد من نصوص أو صور أو تنظيم مؤتمرات أو ينشئ روابط مع المواقع الأخرى.

3/ متعهد الخدمات: وهو ناشر الموقع و المسؤول عن المعلومات التي تعبر على موقعه إلى الشبكة وهو بذلك صاحب السلطة الحقيقية في مراقبة المعلومات التي يتم بثها وهو في القانون السمعي البصري الفرنسي ملزم بإخطار النيابة العامة وملزم بالإيداع القانوني، ويقوم متعهد الخدمات بأدوار عديدة فهو ممول للخدمات ومالك للحاسب الخادم عن دوره في بث المعلومات[2] .

4/ناقل المعلومات: وهو العامل الفني الذي يتولى الربط بين الشبكات بناء على عقد من عقود نقل المعلومات في هيئة حزم من جهاز المستخدم إلى جهاز الحاسب الآلي الرئيسي لمتعهد

[1] مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، 2001، ص100.

[2] جميل عبد الباقي الصغير، الانترنت القانون الجنائي، دار النهضة العربية، القاهرة، 2002، ص164.

الوصول ثم نقلها من الحاسب الأخير إلى الحاسبات المرتبطة لمواقع الإنترنت أو بمستخدمي الشبكة والقانون الفرنسي عرف العامل الفني بموجب المادة الأولى من القانون 659/96 الصادر سنة 1996 المتعلق بالاتصال السمعي البصري على أنه كل شخص طبيعي أو معنوي يستغل شبكة الاتصالات عن بعد والمفتوحة للجمهور ويورد إلى هذه الأجهزة خدمة الاتصالات عن بعد .

الفرع الثاني: مخاطر الجريمة المعلوماتية:

لقد شهد العالم في السنوات الأخيرة تطورا غير مسبوق في مجالات الإعلام والاتصال نظرا إلى توغل وانتشار وسائل التكنولوجيا والابتكارات المستحدثة في الأنشطة المعلوماتية ودخولها في جميع نواحي الحياة وهو ما قد يترتب عليه الخطر الكبير على البنيات المختلفة جراء الاستخدام غير المشروع لهذه التقنيات، والخطر الأكبر هو أن الجرائم المعلوماتية قد تستهدف الأمن القومي بارتكاب جرائم تمس جهات حكومية وأمنية، ليس هذا فحسب بل حتى الأضرار بالاقتصاد كونه أصبح يعتمد بصورة متزايدة على تقنية المعلومات(الاقتصاد الرقمي) مما قد يؤثر (هذا الإجرام التقني) تأثيرا كبيرا على اقتصاد أي دولة يلحق بها خسائر مالية ضخمة.

أولا: بعض التقديرات لحجم الخسائر المالية الناجمة عن الجريمة المعلوماتية:

تبرز المؤشرات والدراسات ازدياد حجم الخسائر والأضرار الناجمة عن الإجرام المعلوماتي خاصة في الدول التي تعتمد بشكل كبير على نظام التقنية المعلوماتية، الأمر الذي يشكل تحديا كبيرا في مواجهة هذه الجرائم ومكافحتها، والخسائر الاقتصادية الناجمة عن ارتكاب الجرائم المعلوماتية تزداد وتتضاعف عندما ترتبط بالجريمة المنظمة، فالمنظمات الإجرامية لديها مهارة كبيرة في اكتشاف فرص القيام بأعمال ومشاريع جديدة غير مشروعة واستغلالها، وأن

المعلوماتية والنمو المتواصل للتجارة الالكترونية وكذا توجه الكير من الدول نحو الحكومة الالكترونية،[1] حمل معه مجالات هائلة لتحقيق أرباح غير مشروعة.[2]

وهناك من الأمثلة العديدة والمختلفة ما من شأنها أن تضع أمام أعيننا حجم الأضرار المالية التي تسببها جرائم تقنية المعلومات، فالتقرير الذي نشرته الجمعية الفرنسية لأمن المعلومات عام 1991 تضمن أن الخسائر وصلت إلى 10.4مليار فرنك فرنسي، 57% منها يرجع إلى أفعال إجرامية، وفي عام 1996 انتهى التقرير الصادر عن نفس الجمعية إلى أن إجمالي الخسائر الناتجة عن المعلوماتية قدّر بحوالي 12.72 مليار فرنك فرنسي.

ومن جهة أخرى توصلت الإدارة العامة للشرطة القضائية باعتبارها إحدى الجهات التي يصل إلى علمها الجرائم المختلفة بما فيها الجرائم المعلوماتية إلا أن أكثر من يتعرض لهذا النمط من الإجرام المشروعات التي تتعلق بالمعلومات بنسبة 25% يليها البنوك بنسبة 21% ثم المشروعات التجارية المختلفة بنسبة18% وأخيرا الجهات الحكومية بنسبة 17%.

أما في الولايات المتحدة الأمريكية فإن إحصائيات مكتب التحقيقات الفدرالي توضح أن متوسط الخسارة في الجريمة المعلوماتية الواحدة حوالي 500 ألف دولار بينما في جريمة سرقة عادية فمتوسط الخسارة 2500 دولار، أي أن متوسط الخسارة في الجريمة المعلوماتية أعلى ب

[1] لما ظهرت شبكة الأنترنت بخدماتها المتعددة عمدت الدول إلى استثمارها في تنفيذ التعاملات الحكومية بشكل الكتروني لما في ذلك من تسيير تقديم الخدمات والارتقاء بمستوى المواطن وتخفيف العبء على المؤسسات الحكومية مما يؤدي إلى زيادة كفاءتها وقد عرفت الأمم المتحدة الحكومة الالكترونية على أنها استخدام الأنترنت والشبكات العالمية العريضة لتقديم معلومات وخدمات الحكومة للمعارضين كما عرّفتها منظمة التعاون الاقتصادي والتنمية عام 2001 على أنها استخدام تكنولوجيا المعلومات والاتصالات وخصوصا الأنترنت للوصل إلى حكومات أفضل ويبنى على ذلك أن فكرة الحكومة الالكترونية تقوم على تجميع الأنشطة والخدمات المعلوماتية في موقع الحكومة الرسمي على شبكة الأنترنت في نشاط أشبه ما يكون بفكرة مجمعات الدوائر الحكومية وتحقيق حالة اتصال دائم بالجمهور مع القدرة على تأمين الاحتياجات الاستعلامية و الخدماتية للمواطن.

[2] نائلة محمد فريد قورة، المرجع السابق: ص70.

150 مرة عنه في الجرائم العادية، كما أصدر المركز القومي للمعلومات الخاصة بجرائم الحاسب الآلي في الولايات المتحدة الأمريكية دراسة معتمدا فيها على المعلومات التي توصل إليها معهد ستانفورد الدولي للأبحاث أسفرت عن مجموعة من النتائج أهمها أن الخسائر الناجمة عن الجريمة المعلوماتية تقدر من 03 إلى 05 مليار دولار وأن المشروعات التجارية هي الأكثر عرضة لهذه الجرائم ثم يأتي بعد ذلك البنوك و المؤسسات الحكومية .[1]

كما بينت دراسة أخرى أجريت من قبل منظمة أن خسائر 163 شركة أمريكية من الجرائم المتعلقة بتقنية المعلومات قد بلغت أكثر من 125 مليون دولار كما أظهر المسح الذي أجري عام 2000 ارتفاع عدد تلك الشركات المتضررة من تلك الجرائم حيث وصل إلى 273 شركة بلغ مجموع خسائرها أكثر من 256 مليون دولار.

كما ورد في التقرير السنوي الثامن لمكتب التحقيقات الفدرالي الأمريكي الصادر عام 2003 بعنوان جرائم الحاسب بأن أكثر خسائر المؤسسات للولايات المتحدة الأمريكية أتي من الاستيلاء على المعلومات والتي كبدتها خلال هذا العام خسائر تتعدى 70 مليون دولار أمريكي ويأتي في المركز الثاني نشاط تعطيل نظم المعلومات محققا خسائر تتجاوز 65.5 مليون دولار.

ثانيا: مخاطر الجريمة المعلوماتية في الجزائر:

أما في الجزائر فإن المحيط الكمي للإجرام المعلوماتي غير واضح لعدم وجود دراسات و بحوث من شأنها كشف اللثام عن أرقام ومؤشرات للخسائر في بلادنا جراء هذا النمط الإجرامي،[2] وإن كانت الجزائر ليست بمنأى عن خطورة الجرائم المعلوماتية طالما أنها تحتل

[1] نائلة محمد فريد قورة، المرجع السابق، ص84.

[2] غياب إحصاءات لهذا النوع من القضايا راجع لعدم وعي المجتمع المحلي بمخاطرها، بالإضافة إلى حداثة الثورة التقنية بالجزائر و قصور البنية التحتية اللازمة لدخول المؤسسات الوطنية بقوة في أعمال التجارة الالكترونية.

جزءا من الفضاء الالكتروني خاصة فيما يتعلق بالحاسبات المالية وبعض الهيئات الحكومية التي يعتبر اختراق مواقعها ضمن حجم الأضرار الناتجة عن الجريمة المعلوماتية.

ونخلص للقول بناء على ما تقدم أن معدل الخسائر المالية نتيجة الجريمة المعلوماتية يفوق في كثير من الأحوال نفس المعدل في الجريمة التقليدي، ويرجع السبب في ذلك إلى الكم الكبير من المعلومات (ذات القيمة المالية العالية) التي يتم برمجتها آليا والتي يمكن التلاعب بها في ثوان معدودات وتحويلها من شخص لآخر.


الفصل الثاني

تمهيد:

إن طبيعة الجرائم المعلوماتية بعناصرها ووسائل ارتكابها قد تدفع المشرع الجزائري إلى أن يعيد النظر في كثير من المسائل الإجرائية، خاصة فيما يتعلق بمسألة الإثبات باعتبارها أهم موضوعات هذا القانون، ذلك أن الدليل الذي قد يقوى على إثبات هذا النوع من الجرائم لا بد 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 إلى الحديث عن مسألة قبول هذا الدليل أما القضاء ومدى تعبيره عن الحقيقة نظرا لما يمكن أن يخضع له من التزييف والتحريف والأخطاء، بل وحتى مع ضمان مصداقية هذا الدليل و كذا مشروعيته فإن الأمر لا يتوقف عند هذا الحد، بل يتجاوزه إلى مسألة أكبر أهمية 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.

المبحث الأول: التحقيق في الجريمة المعلوماتية.

إن التحقيق هو إجراء من أهم الإجراءات التي تتخذ 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،[1] والمرحلة الثانية تدخل في اختصاص قاضي التحقيق،[2] وإننا نؤيد الرأي أو الاتجاه[3] الذي يقسم التحقيق إلى:

- تحقيق أولي والذي 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] حسب المادة 15 من قانون الإجراءات الجزائية:"يتمتع ضابط الشرطة القضائية بـ:

– 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، مفتشوا الأمن لوطني 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.

[2] يبدوا 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.

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

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 المادتين12 و 38 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....."

وعليه فإنه يمكن القول أن إجراءات البحث والتحري عن الجرائم هي من صلاحيات جهات التحقيق سواء كان أوليا أو ابتدائيا، وبهذا المفهوم فإن إجراءات البحث والتحري التي يباشرها رجال الضبط القضائي تصب في إطار التحقيق الأولي، بينما هذه الإجراءات 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 الالكترونية يستوجب بالإضافة إلى كل هذا تطويرا لأساليبه وتكليف جهات مختصة لممارسته من أجل مواكبة حركة الجريمة و تطور أساليب ارتكابها في هذه البيئة.

المطلب الأول: الأجهزة المكلفة بالبحث والتحري عن الجريمة المعلوماتية.

لقد كان للتزايد المستمر للجرائم المعلوماتية 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 الأجهزة تسميات مختلفة منها مثلا شرطة الأنترنت أو فرقة التحري عن جرائم المعلوماتية إلى غير ذلك من التسميات.

ولا يقتصر دور هذه الأجهزة على المستوى الوطني فقط، بل هناك أجهزة متخصصة على المستوى الدولي أيضا، وسوف نستعرض أهم هذه الأجهزة سواء على المستوى الداخلي أو الدولي وذلك كما يلي:

أ) الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الداخلي:

لقد 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.

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

أولا: الأجهزة المختصة في الدول الأجنبية:

كانت الدول المتقدمة 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. **الولايات المتحدة الأمريكية:** قامت الولايات المتحدة الأمريكية بإنشاء عدة أجهزة لمكافحة الجريمة المعلوماتية و منها:

- **شرطة الواب webpolice:** وتعتبر نقطة مراقبة على الأنترنت إضافة إلى أنها تتلقى الشكاوى من مستخدمي الشبكة وملاحقة الجناة والقراصنة، والبحث عن الأدلة ضدهم و تقديمهم إلى المحاكمة.[1]
- **مركز تلقي شكاوى الأنترنت IC3[2]** والذي تم إنشاؤه من طرف مكتب التحقيقات الفدرالي FBI في سنة 2000، ثم في عام 2003 تم دمج مركز شكاوى الاحتيال عبر الأنترنت المعروف ب: IFCC[3] مع هذا المركز، ويعمل مركز ic3 بصورة تشاركية مع مكتب التحقيقات الفدرالي والمركز الوطني لجرائم الياقات البيضاء NWC،[4] ويقوم هذا المركز يتلقي الشكاوى عبر موقعه على الأنترنت أين يقوم الشاكي بماء استمارة الكترونية ثم يقوم المختصون في هذا المركز بتحليل الشكاوى وربطها بالشكاوي الأخرى المستلمة من قبل.
- **قسم جرائم الحاسوب والعدوان على حقوق الملكية الفردية الفكرية:** ويختص هذا القسم بالتعريف بهذه الجرائم والكشف عنها وملاحقة مرتكبيها.
- **نيابة جرائم الحاسوب والاتصالات CTC،[5] وتتألف** 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 الفردية.

---

[1] جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، المرجع السابق، ص77.

[2] وهو اختصار لـ.Internet Crime complaint Center.

[3] وهو اختصار لـ: complaint Center Internet Fraude .

[4] وهو اختصار لـ:National White coller center .

[5] وهو اختصار ل:.QND Télécommunication coordinateur Computer

- **المركز الوطني لحماية البنية التحتية التابع** للمباحث الفدرالية الأمريكية و قد حدد هذا المركز البنى التحتية التي تعتبر هدفا للهجومات والاعتداءات عبر الأنترنت 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 والأنترنت ومن مستشارين قانونيين.[1]

2. **في بريطانيا:**قامت السلطات البريطانية بتخصيص 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.
3. **في فرنسا:** قامت الحكومة الفرنسية بإنشاء عدة أجهزة لمكافحة الجرائم المعلوماتية ونذكر 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 المرتبك بتكنولوجيات المعلومات والاتصالات:** ويعد هذا المكتب سلاح الدولة الفرنسية في مكافحة الجرائم المعلوماتية، وقد تم إنشاؤه في: 2000/05/15.

[1] نبيلة هبة محمد هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات للطبقة الأولى، دار الفكر الجامعي، الإسكندرية، 2007، ص108.

4. في الصين: قامت السلطات في هذا البلد بإنشاء وحدة متخصصة على مستوى جهاز الشرطة تعرف باسم "القوة المضادة للهكرة" وهي تختص برقابة المعلومات التي يسمح لمواطنيها الدخول إليها عبر الأنترنت.[1]

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

1) **الأجهزة المتخصصة في مصر:** قامت وزارة الداخلية في مصر بإنشاء عدة أجهزة أوكلت لها مهمة ضبط ما يقع من جرائم من خلال الشبكة المعلوماتية نعرض لها على النحو التالي:

- **إدارة مكافحة جرائم الحسابات وشبكات المعلومات:أُنشئت هذه الإدارة** بموجب قرار وزاري،[2] 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: 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 الأنترنت على مختلف أنواعها.[3]
- **قسم مكافحة جرائم الحاسبات و شبكات المعلومات:** وقد أنشأ هذا القسم بالإدارة العامة للبحث الجنائي بمديرية أمن القاهرة، ويتبع إدارة المعلومات والحاسب الآلي ويخضع من

---

[1] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 2004، ص812.

[2] قرار وزير الداخلية المصري رقم13507 لسنة 2002 الصادر بتاريخ: 2002/07/07.

[3] نبيلة هبة هروال، المرجع السابق، ص141.

حيث الإشراف الفني لإدارة مكافحة جرائم الحاسبات وشبكات المعلومات ويختص بعمليات تأمين ورقابة نظم وشبكات المعلومات لمنع وقوع أية جريمة عليها باستخدام الأساليب والتقنيات العملية الحديثة، ورصد ومكافحة وضبط الجرائم التي تقع باستخدام الحاسبات على نظم وشبكات المعلومات وقواعد البيانات.

ثانيا: الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الوطني:

أما 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 و كان ذلك إما على مستوى جهاز الشرطة أو الدرك الوطني.

فعلى مستوى جهاز الشرطة فقد أنشأت 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 والإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية، بالإضافة إلى مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومي للدرك الوطني وهو قيد الإنشاء.

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

سبق وأن أسلفنا الذكر بأن الجرائم المعلوماتية تتميز بأنها عابرة للحدود الوطنية يمكن أن يتعدى أثرها عدة دول، لذلك كان لا بد من وجود تعاون دولي من أجل مكافحة هذا النوع من الإجرام، ومن أساليب التعاون الدولي 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:

أولا:على الصعيد الدولي: تعد المنظمة الدولية للشرطة الجنائية(الأنتربول)،[1] من أهم الأجهزة على المستوى الدولي لمكافحة الإجرام بصفة عامة و منها الجرائم المعلوماتية، وتهدف 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:

الأولى: تجمع البيانات والمعلومات المتعلقة بالجريمة والمجرم عن طريق المكاتب المركزية الوطنية الموجودة في أقاليم الدول الأطراف.

الثانية: التعاون في ملاحقة المجرمين الفارين وإلقاء القبض عليهم وتسليمهم للدول التي تطالب بتسليمهم.

وتعمل المنظمة الدولية للشرطة الجنائية في مجال الجرائم المعلوماتية بوضع قائمة اسمية لضباط متخصصين يمكن الاستعانة بهم في مجال البحث والتحري في قضايا الجرائم

[1] بعد انتهاء الحرب العالمية الثانية عقد في بروكسل(بلجيكا) مؤتمر دولي في الفترة من 9-6/9 عام 1946 انتهى إلى إحياء اللجنة الدولية للشرطة الجنائية(ICPO) ونقل مقرها إلى باريس وغير اسمها ليصبح المنظمة الدولية للشرطة الجنائية الأنتربول ووضع ميثاق هذه المنظمة في الفترة من7-1956/06/13 واعتبر نافذا اعتبارا من 1956/06/13.

المعلوماتية بوضع قائمة اسمية لضباط مختصين 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،[1] ولقد 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.

ثانيا: الأجهزة على المستوى الإقليمي:

- **الشرطة الأوروبية أو الأوروبول:** وجهاز على مستوى الإتحاد الأوروبي تم إنشاؤه في لوكسنبورغ عام 1992 ومقره في مدينة لاهاي بهولندا 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 و منها الجريمة المعلوماتية.

وبمبادرة من الشرطة القضائية الفرنسية تم إنشاء جهاز على مستوى الأوروبول أطلق عليه اسم (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 اختصاصه عندما

[1] Myriam QUEMENER Cyebrctinianalité droit pénal appliqué econonica Septembre 2010, p208.

تمس الجريمة دولتين على الأقل من الدول الأعضاء في الاتحاد الأوروبي أو دولة عضو مع دولة أخرى من غير الاتحاد الأوروبي، ويعد الأوروجيست وحدة للتعاون القضائي، مهمتها الأساسية هي التنسيق بين السلطات القضائية المكلفة بالتحقيقات ولها من الصلاحيات ما يؤهلها للفتح تحقيقات ومباشرة متابعات جزائية.

المطلب الثاني: خصائص التحقيق والمحقق في الجريمة المعلوماتية:

تعد مرحلة التحقيق الابتدائي أو ما يطلق عليها مرحلة جمع الاستدلالات، مرحلة هامة في سبيل البحث والتحري عن الجرائم وتبلغ هذه المرحلة أعلى مستوياتها عندما يتعلق الأمر بالجريمة المعلوماتية لأنها تعد حجر الزاوية الذي سيتم على أساسه بناء الدعوى برمتها، فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقب ارتكاب الجريمة مباشرة قد لا يبقى متاحا بعد مرور وقت قصير على ارتكابها والسبب في ذلك يعود إلى الطبيعة التقنية لهذه الجرائم ففي كثير من الجرائم المعلوماتية لم يترك الجاني وراءه سوى ذلك التعبير الذي يعتري وجوه القائمين على تعقبه والممزوج بالإحباط والإعجاب معا.[1]

أ- خصائص التحقيق في الجريمة المعلوماتية:

التحقيق الجنائي عموما هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فله قواعد ثابتة وراسخة بدونها ما كان ليتمتع التحقيق بتلك الصفة.

وهذه القواعد إما قانونية وإما فنية، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزاءها شيئا سوى الخضوع و الامتثال أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته و فطنته و مهارته الكثير.[2]

[1] محمد طارق عبد الرؤوف الجن، المرجع السابق، ص230.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الطبعة الأولى 2009، ص56.

ذلك أن الفكر البشري المتعلق بالمجرم المعلوماتي يجب أن يقابله فكر بشري من قبل المحقق الجنائي، وبالتالي فإن أسلوب التحقيق وفكر المحقق الجنائي يجب أن يتغير ويتطور أيضا، وذلك كنتيجة طبيعية لمواجهة فكر المجرم المعلوماتي.

أولا: منهج أو أسلوب التحقيق الابتدائي في الجريمة المعلوماتية:

التحقيق عموما هو مجموعة الإجراءات التي يقوم بها المحقق وتؤدي إلى اكتشاف الجريمة ومعرفة مرتكبيها تمهيدا لتقديمهم إلى المحاكمة، وقد تكون هذه الإجراءات عملية كالتفتيش أو فنية كمظاهات البصمات أو برمجية كتحديد كيفية الدخول إلى المعطيات المخزنة في النظام المعلوماتي.

والهدف من التحقيق الابتدائي هو التأكد أولا من وقوع جريمة يعاقب عليها القانون، ومن ثمة معرفة نوع هذه الجريمة ومن هو الجاني ومن هو المجني عليه، و كذا معرفة وقوعها وما هي الوسائل التي استعملت في ارتكابها، ويكون ذلك في الجريمة المعلوماتية وفقا لمنهج تحقيقي عن غيره بالنسبة للجرائم الأخرى.

1. **وضع خطة عمل التحقيق:** يبدأ المحقق عمله عند تجميع الاستدلالات المتعلقة بالجريمة المعلوماتية بوضع خطة العمل اللازمة على ضوء المعلومات المتوافرة لديه، وتحديد الفريق الفني اللازم للقيام بمساعدته في أعمال التحقيق وذلك على النحو الآتي:

- وضع الخطة المناسبة والتي لا تبدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات الكفيلة للتصدي للجريمة.
- التخطيط الفني للتحقيق وذلك من أجل الوصول إلى أفضل الطرق والأساليب للتعامل مع هذه الجرائم بالتفصيل والوضوح.

- عمل دراسة وافية وجادة لكافة إجراءات التحقيق ضمن الخطة المسبقة التي تم وضعها وناقشها العاملون في فريق التحقيق.
- تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمتهم وعملهم وتقليل الآثار السلبية والإسراع في إنجاز العمل وهو ما يؤدي إلى ضمان مستوى جيد من الأداء.
- تحديد الإجراءات المسبقة والتي من شأنها التقليل من الأخطاء الفردية التي قد تنتج عن قلة الخيرة أو نقص المعرفة، وبالتالي تساعد على إيجاد درجة جيدة من التقيد بالمستوى المطلوب مع ضمان أن الخطوات التي يقوم بها المحقق خلال جميع مراحل التحقيق تسير ضمن الضوابط التشريعية وتقلل من الأخطاء التي قد تضر بالقضية في مرحلة المحاكمة.[1]

ويجب أن ترتكز خطة العمل على مجموعة من البنود الأساسية يتم الارتكاز عليها أثناء تنفيذ الخطة، وهي أن يتم تعيين الأشخاص الذين سيتم التحقيق معهم وتحديد النقاط التي يجب استيضاحها معهم وتقدير مدى الحاجة للاستعانة ببعض الفنيين اللازم توافرهم لاستكمال التحقيق،[2] بالإضافة إلى مراعاة الظروف والملابسات المحيطة بالواقعة ذلك أن من هذه الظروف ما يشمل عوامل مهمة يجب مراعاتها عند وضع خطة العمل ومنها:

- مدى أهمية الأجهزة والشبكات المتضررة لعمل المنظمة.
- مدى حساسية البيانات التي يحتمل سرقتها أو إتلافها.
- مستوى الاختراق الأمني الذي تسبب فيه الجاني.

ثم بعد ذلك وضع الأسلوب الأمثل لعملية التفتيش وذلك من خلال تحديد نوع الأدلة التي يريد فريق التحقيق البحث عنها.

---

[1] محمد نصير السرحاني، مهارات التحقيق الفني في الحاسوب والأنترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص72.

[2] هشام رستم، الحواسب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، 2000، ص59.

2. **تشكيل فريق التحقيق:** إن التحقيق الابتدائي في الجرائم المعلوماتية يكون غالبا أكبر من أن يتولاه شخص واحد بمفرده، حتى و لو كانت المضبوطات هي مجرد حاسب شخصي واحد، ولذلك فإنه يفض أن يتعاون عدة محققين في إنجاز مهمة التحقي والعثور على الأدلة.

ويجب أن يتشكل فريق التحقيق من فنيين وأخصائيين ذوي خبرة في مجال الحاسوب والأنترنت، يمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي الالكتروني بشكل خاص، ولهؤلاء المحققين أن يستعينوا بخبراء في مجال الحاسوب والأنترنت ليتمكنوا من فك التعقيدات التي تفرضها ظروف وملابسات كل جريمة.[1]

وإن كان أسلوب عمل الفريق يستخدم في التحقيق في كثير من أنواع الجرائم إلا أنه يأخذ أهمية خاصة في الجرائم المعلوماتية لما تتطلبه من مهارات فنية وخبرات متنوعة قد لا تتوافر لدى المحققين، وبذلك يكون تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم أمرا ضروريا ومن الناحية العملية غالبا ما يتكون فريق التحقيق في الجرائم المعلوماتية من:

- المحقق الرئيسي ويكون ممن لهم خبرة في التحقيق الجنائي.
- خبراء الحاسوب وشبكات الأنترنت الذين يعرفون ظروف الحادث وكيفية التعامل مع هذه الجرائم.
- خبراء ضبط وتحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب.
- خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية.
- خبراء التصوير والبصمات والرسم التخطيطي.[2]

[1] عبد الله حسين محمود، إجراءات جمع الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الالكترونية، دبي، 2003، ص612.

[2] عبد الله محمود، المرجع السابق.

وفي هذا الإطار نجد أن المشرع الجزائري قد أشار إلى مسألة إمكانية استعانة الجهات المكلفة بالتحقيق بالخبراء المتخصصين في مجال الحاسوب والنظم المعلوماتية، ومن الذين لهم دراية بعمل المنظومة المعلوماتية أو ممن لهم دراية بالتدابير المتخذة لحماية المعطيات المعلوماتية، وذلك بغرض مساعدة جهات التحقيق في إنجاز مهمتها وتزويدها بالمعلومات الضرورية لذلك.[1]

ثانيا: العناصر الأساسية للتحقيق الابتدائي في مجال الجريمة المعلوماتية:

ونقصد بها تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها، وهناك إجراءات واحتياطات يتعين على الضبطية القضائية مراعاتها قبل البدء في عمليات التحقيق الابتدائي.[2]

1. الإجراءات يجب على الضبطية القضائية مراعاتها قبل البدء في التحقيق: و يمكن أن نسرد الأهم منها كما يأتي:

- تحديد نوع نظام المعالجة الآلية للمعطيات فهل هو كمبيوتر معزول أم متصل بشبكة معلومات.
- وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها و دور كل واحد منهم.
- إذا وقعت الجريمة على شبكة فإنه يجب حصر طرفيات الاتصال بها أو منها لمعرفة الطريقة التي تمت بها عملية الاختراق من عدمه، وهل هناك حواسيب آلية خارج هذه الشبكة ولها إمكانية الاتصال بها أم لا؟

[1] انظر المادة 05 الفقرة الأخيرة من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] جميل عبد الباقي الصغير، المرجع السابق، ص119، د. عبد القتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، دار الكتب القانونية المجلة الكبرى، ط1، ص84، وكذلك د. محمد الأمين الشبري، المرجع السابق، ص50.

- مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة المعلوماتية.
- مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.
- يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الاستدلالات لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار جريمته.
- فصل خطوط الهاتف حتى لا يسيء الجاني استخدامها، و التحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق لأنهم قد يسيئون استخدامها لطمس البيانات.
- التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، ذلك أنه من الخدع التي يستعملها الجاني عند الاختراق أن يتم ذلك بخط هاتفي مسروق عن طريق الدخول إلى شبكة الهاتف والتلاعب فيها وتضليل أجهزة المراقبة و أجهزة التحقيق بعد ذلك.
- إبعاد الموظفين عن أجهزة الحاسب الآلي بعد الحصول منهم على كلمة السر وكذا الشفرات في حالة وجودها.
- تصوير الأجهزة المستهدفة(التي وقعت بها أو عليها الجريمة) من الأمام والخلف وذلك لإثبات أنها كانت تعمل وكذلك للمساعدة في إعادة تركيبه من أجل البدء في إجراءات التحقيق.

2. **الإجراءات التي يجب مراعاتها أثناء التحقيق:** عند البدء في عملية التحقيق الابتدائي سيما عند القيام بعملية تفتيش جهاز الحاسوب فإنه على رجال الضبطية القضائية و برفقتهم الخبراء الذين يستعينون بهم بمراعاة ما يلي:

- عمل نسخة احتياطية من الأقراص الصلبة أو الأسطوانة المرنة قبل استخدامها والتأكد فنيا من دقة النسخ عن طريق الأمر (disque comp).
- نزع غطاء الحاسب الآلي المستهدف والتأكد من عدم وجود أقراص صلبة إضافية.

- أن يكون الهدف من نسخ محتوى الأسطوانة والأقراص تحليل المعلومات الموجودة بغرض التوصل إلى معرفة الملفات الممسوحة، ويمكن استعادتها من سلة المهملات مع ملاحظة أن هناك بعض الملفات التي إن مسحت وضغط على أزرار معينة مثل Shift delete في وقت واحد لا يمكن استعادتها وكذا من أجل معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب.
- العمل على فحص البرامج وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في جريمة اختلاس معلوماتي.
- العمل على فحص العلاقة بين برامج التطبيقات والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها.
- حفظ المعدات والأجهزة التي تضبط بطريقة فنية وسليمة.

ب- خصائص المحقق المعلوماتي:

أمام التطور التقني والتكنولوجي الذي صاحب الجريمة المعلوماتية فإن المختصين بالتحقيق في هذا النوع من الإجرام المستحدث يختلفون عن أولائك المختصين بضبط الجرائم التقليدية من حيث الخصائص وطريقة التكوين، ذلك أن التحقيق في هذه الجرائم لا يعتمد على التدريبات الجسدية التي يتلقاها عادة رجال الضبطية القضائية وإنما يعتمد على البناء العلمي والتكنولوجي وهم يتولون مهمة البحث والتحري عن الجرائم المعلوماتية وكشف النقاب عنها.

وإذا كان قد سبق وأن طرحنا خصائص الجريمة المعلوماتية وكذا خصائص المجرم المعلوماتي فإنه في اعتقادنا يلزم الأمر معرفة الخصائص التي يجب أن يتوفر عليها من يتصدى لمهمة البحث و التحري عم هذا النوع من الجرائم والمجرمين.

أولا: الخصائص الفنية للمحقق في الجريمة المعلوماتية:

تلعب الأجهزة الأمنية دورا أساسيا في صيانة أمن المجتمع وذلك إما بالقيام بدور وقائي يهدف إلى منع ارتكاب الجرائم والحيلولة دون وقوعها وتقليل من فرص اقترافها، وإما القيام بدور قضائي في ضبط الجرائم ومرتكبيها بعد حدوثها.

ولقد أضاف ظهور الجرائم المعلوماتية النابعة من التطور الالكتروني أعباء جديدة على أجهزة التحقيق لما يتطلبه التصدي لهذه الجرائم من قدرات فنية لم يألفها رجال الضبطية القضائية ولم يتعودوا عليها، ما يستلزم ضرورة توفير الإمكانات والمهارات المطلوبة في هذا المجال.

والمشكلة الأساسية التي تواجه المحققين في جرائم نظم المعلومات هي خلفية المحقق نفسه فمتخصص الحاسب الآلي قد تكون لديهم المعرفة التقنية اللازمة ولكنهم ليسوا مدربين على تفهم دواع الجريمة وجمع الأدلة لتقديم المتهم للمحاكمة، وفي كثير من الحالات نجد أن متخصص الحاسب يعتقد أن لديه الدليل الحاسم حول جريمة معلوماتية ما، ولكن من الناحية القانونية يتبين فيما بعد أن هذا الدليل لا يصلح لإقامة الدعوى بينما المحققون ذوي الخلفية القانونية قد تكون لديهم خبرة واسعة في التحقيق ولكنهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم.[1]

وإذا كانت مهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود وغيرها تعتبر من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى المحقق، إلا أنه يلازمه عند

[1] في حادثة طلب أحد المحققين من المشتبه فيه أن يريه الملف الذي قام بتزويره انطلاقا من الحاسب الشخصي له فما كان للمشتبه فيه إلا أن قام عمدا بحذف هذا الملف وبذلك أضاع الدليل الرئيسي في الجريمة وفي حادثة أخرى تم القبض على بعض المهتمين وضبط الحاسوب ثم قامت جهات التحقيق بتفكيك الحاسوب باعتباره دليل على الجريمة وقامت بنقله إلى مركز الشرطة ثم بعدها تبين أن تشغيل الجهاز لفحص مكوناته يحتاج إلى إعادة توصيل الكابلات التي تم نقلها دون أن يتم ترقيمها وكان الأمر يبدو شبه مستحيل وضاع حتى الدليل أيضا.

مباشرته التحقيق في الجريمة المعلوماتية معرفة العديد من الجوانب الفنية ليقوم بعمله على أحسن وجه و نذكر منها:

- معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والأنترنت والتي تتعلق بالجريمة المرتكبة ذلك أن افتقار ضابط الشرطة القضائية للتأهيل الكافي في الميدان التقني قد يفضي إلى إتلاف وتدمير الدليل، على اعتبار أن جهلة بارتكاب أساليب الجريمة المعلوماتية يجعله يقع في كثير من الأحيان في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها مثل إتلاف محتويات الأقراص الممغنطة وأوعية المعلومات التي تخزن بها البيانات،[1] وبالتالي فإن الكشف عن هذه الجرائم يقتضي أن تكون الأجهزة المعنية على دراية كافية بأساسيات التعامل مع هذه الجرائم وكيفية تقصيها وضبطها وصولا إلى مرتكبيها.
- إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الالكترونية التي تدل على وقع الجريمة، وتخزينها في الأقراص المعدة لذلك و منع حذفها والحرص على عدم تعريض وسائط التخزين كالأقراص المرنة أو المدمجة لأية مؤثرات خارجية كالقوى الكهرومغناطيسية أو موجات الميكروويف حتى لا تتلف محتوياتها.
- كما يتوجب على المحقق معرفة آلية عمل تشكيلات الحاسوب والأنترنت وتبرز أهمية فهم المحقق لهذه المبادئ في كونها ضرورية لتصور كيفية ارتكاب الفعل الإجرامي في العالم الافتراضي من اختراق للشبكات واعتراض حزم البيانات أثناء انتقالها عبر الشبكة والتجسس عليها وتحويلها عن مسارها، كما أنها تعطي للمحقق تصورا جيدا عن مدى إمكانية متابعة مصدر الاعتداء على الشبكة والمعوقات التي تحول دون ذلك.[2]

[1] جميل عبد الباقي، الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية القاهرة، 2002، ص115.

[2] حسين الغافري، المرجع السابق، ص02.

- يتوجب على المحقق أن يستطيع التمييز بين الأنظمة المختلفة لتشغيل الحاسوب وأن يلم بجميع الأنظمة التشغيلية لأجهزة الحاسوب وما تتسم به من خصائص ومميزات كل نظام على حدى لأنه ملزم بالتعامل معها، وكذلك أنظمة الملفات التي يعتمدها كل نظام حتى يتمكن من إجراء التحقيق في الجرائم المعلوماتية وفي كشف المجرمين ومعاينة مسرح الجريمة وإذا كان التعامل المباشر مع هذه الأنظمة والقيام بفحصها ورفع الأدلة الجنائية الرقمية الموجودة فيها يعتبر مهمة الخبير"إلا أن معرفة المحقق الجنائي الأولية بهذه الأنظمة ضرورية لكي يشارك في متابعة فحص وتفتيش مسرح الجريمة المعلوماتية.
- كما يتعين على المحقق كذلك التعرف على معطيات الحاسوب المختلفة ليصبح قادرا على معرفة صيغ الملفات وما يمكن أن تحتويه من معطيات، ومعرفته لأهم التطبيقات التي يمكنه من خلالها قراءة أو مشاهدة محتوى هذه الملفات،[1] والتي تعد أمرا في غاية الأهمية،لأنها تعتبر الوعاء الحقيقي لأدلة الإدانة في كثير من القضايا ذات الصلة بالحاسوب والأنترنت بما تحتويه من معلومات.
- ومن الأمور الفنية التي يتوجب على المحقق معرفتها أيضا أن يكون ملما بالأساليب المستخدمة في ارتكاب الجرائم المعلوماتية وتقنيات الأمن المعلوماتي، ذلك أن معرفة رجال التحقيق لهذه الأساليب يعد من الأمور المهمة التي تساعدهم في معرفة الجناة ومواقع ارتكاب الجريمة ومن أي طرفية الكترونية صدر السلوك الإجرامي وكذلك في مناقشة الشهود وسماع المشتبه فيهم ومحاصرتهم بالأسئلة التي تتعلق بكيفية ارتكاب الجريمة وطرق تنفيذها.

[1] يتم حفظ البيانات الرقمية داخل الحاسوب على شكل مجموعات أو كتل من البيانات تمثل وحدة واحدة تسمى الملفات ويتميز كل ملف ببنية وصيغة خاصة تميزه عن غيره، وغالبا ما ترتبط صيغة بنوع محدد من المحتوى كأن يحتوي الملف على بيانات تمثل صورا أو أصواتا أو مستندا خطيا منسق أو غير منسق.

كما أن الإلمام بتقنيات الأمن المعلوماتية والحاسوبية من الأمور المهمة والتي لا بد للمحقق المعلوماتي من معرفتها واستيعابها، لأنها تساعده في معرفة مجريات التحقيق، فالمحقق عندما يباشر التحقيق في جريمة اختراق شبكة الحاسوب التابعة لمؤسسة ما يسأل القائمين على الشبكة عن نوع برامج الحماية المستخدمة وكيفية إعدادها والكيفية التي تفاعلن بها مع الحدث محل التحقيق، وهناك الكثير من التقنيات التي تستخدم في أمن الحاسوب والشبكات والتي تكون وثيقة الصلة بالتحقيق، ويكون فهم المحقق لوظائفها وأسلوب عملها وطرق استخدامها عاملا مساعدا له عند قراءته للتقارير الجنائية التي يعدها خبير الحاسوب والتي تعد من أهم الوثائق التي يرجع إليها المحقق و يعتمد عليها في تحقيقه وترفق بعد ذلك بمحاضر التحقيق و يرتكز عليها توجيه الاتهام عند اللزوم.

ثانيا: تأهيل وتدريب المحقق المعلوماتي:

في مكافحة الجرائم المعلوماتية بصفة عامة لا بد من وضع سياسة جنائية رشيدة تستند على تدريب أجهزة العدالة الجنائية لمكافحة هذه الجريمة، ويمتد هذا التأهيل والتدريب إلى العاملين بأجهزة الضبطية القضائية.

وقد تنبهت الدول إلى هذا الأمر وظهر هذا الاهتمام في توصيات العديد من المؤتمرات الدولية الخاصة بمنع الجريمة ومعاملة المجرمين، ومنها ما جاء في القاعدة1/22 من قواعد بيكين التي أكدت على الحاجة إلى التخصص المهني والتدريب.

ولهذا فإنه من الضروري إعداد المحققين في الجرائم المعلوماتية باعتبارهم يواجهون أنشطة إجرامية معقدة وتنفذ بطرق دقيق وذكية، ويتأتى ذلك من خلال الإسراع في أن يطور رجال البحث الجنائي وسائلهم البحثية وقدراتهم العلمية وليس بالضرورة أن يكون المحقق في الجريمة المعلوماتية خبيرا في الحاسوب والنظم المعلوماتية ولكن لا بد من الإلمام ببعض

المسائل الأولية التي تمكنه من التفاهم مع خبراء الحاسب الآلي وحسن استغلالهم في كشف الجرائم وجمع الأدلة كما أنه من الضروري أن يكون المحقق ملما بالإجراءات الاحتياطية التي ينبغي اتخاذها على مسرح الجريمة والتدابير اللازمة لتأمين الأدلة ومعلوماتها الممغنطة بصورة عملية وسليمة.[1]

وإذا كانت الشركات الخاصة تستعين بمحققين هم خبراء في الحواسيب، فالجهات الحكومية أولى بإعداد كوادرها للضبط والتحقيق فيا لجرائم المعلوماتية، فالتقدم المتواصل في تكنولوجيا الحاسب الآلي والأنترنت يفرض على جهات تطبيق القانون أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات وهذا الأمر يتطلب الأمر يتطلب الإلمام بالتقنيات الجديدة حتى يمكن مواجهة مجرمي المعلوماتية.

ويرى الفقه الجنائي أنه حال التدريب على التحقيق في الجريمة المعلوماتية يتعين مراعاة عناصر أساسية تتمثل في شخص المتدرب ومنهج الدورة التدريبية وصفة وأسلوب التدريب.[2]

ويجب أن يشمل منهج التدريب خصوصا تدريس الأساليب الفنية المستخدمة في ارتكاب الجريمة والأساليب التي تتعلق بالكشف عنها وكيفية إثباتها ومعاينتها والتحفظ عليها وكيفية فحصها فنيا.

وقد كان هناك من يرى أن صعوبة التحقيق الجنائي في الجرائم المعلوماتية تتطلب أن يعهد بهذا التحقيق إلى بيوت خبرة متخصصة في هذا المجال، لكن هذا الأمر له خطورته إذ من شأنه أن يضحي بمصلحة الفرد والمجتمع ويضعها تحت رحمة هذه الشركات التي يكون همها تحقيق الربح المادي على حساب إظهار الحقيقة، فضلا عن الإخلال بمبدأ سرية التحقيق

[1] محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت بكلية الشريعة والقانون، جامعة الإمارات العربية المتحدة الفترة من01 إلى03 ماي 2000.

[2] هشام محمد فريد رستم، الجرائم المعلوماتية بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت، ص115.

سيما لو تعلق التحقيق بجرائم عرض الأشخاص وأسرارهم الشخصية أو تعلق الأمر بأمن الدولة.[1]

المطلب الثالث: الحماية الفنية للمنظومة المعلوماتية

إن المنع الجنائي وتحديد عقوبات لجرائم المعلوماتية بصفة مسبقة بما يتماشى مع مبدأ الشرعية وإن كان يوفر حماية أساسية للنظام وللمعلومات ضد المخاطر والأضرار الناجمة عن هذه الجرائم من إتلاف وتدمير باهظ التكلفة في حالة الوصول إلى معلومات سرية، إلا أنه غير كاف لوحده، فحتى تكون هناك الفعالية في الحركة والأداء لابد أن تعززها حماية فنية تعمل على الحيلولة دون وقوع هذه الجرائم أو التخفيف من آثارها إذا وقعت.[2]

ويقصد بالحماية الفنية أو أمن المعلومات[3] دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها، أو استغلال نظمها في ارتكاب الجريمة باعتبارها إجراءات وقائية لتجنب اختراق النظام المعلوماتي.

ويشترط لضمان توفر الحماية الفنية الكافية للمعلومات الإلكترونية السرية أو الموثوقية التكاملية، سلامة المحتوى، استمرارية توفر المعلومات وأخيرا عدم الإنكار. فما هي الوسائل الفنية اللازمة لتأمين حماية هذه المعلومات غير العقاب الجنائي.

تتعدد وسائل الأمن التقنية المتعين استخدامها في بيئة المعالجة الآلية للمحافظة على المعلومات بشكل آمن كما تتعدد أغراضها ونطاقات استخدامها.

---

[1] محمد الأمين البشري، المرجع السابق، ص25.

[2] وهذا ما أكدت عليه المذكرة التفسيرية لاتفاقية بودابست حينما ذهبت إلى القول من أن الوسيلة الأكثر فعالية لمنع الولوج غير المصرح به تتمثل بطبيعة الحال في التهديد بقانون العقوبات، ومع ذلك فإن هذا العرض لا يكون مكتملا دون تبني ووضع إجراءات أمنية فعالة، أنظر في ذلك، د. هلالي عبد الله أحمد، الجوانب الإجرائية والموضوعية لجرائم المعلوماتية على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة 2003ص7.

[3] خالد ممدوح إبراهيم، أمن المعلومات، المرجع السابق، ص38.

الفرع الأول: الحماية الفنية عن طريق البرامج:

ويمكن تصنيف هذه الوسائل في ضوء غرض الحماية إلى الوسائل التالية:

1. الوسائل المتعلقة بالتعريف بشخص المستخدم وموثوقية الاستخدام ومشروعيته:

وهي الوسائل التي تهدف إلى ضمان استخدام النظام أو الشبكة من قبل الشخص المخول هذا الاستخدام وتضم هذه الطائفة كلمات السر بأنواعها، البطاقات الذكية المستعملة للتعريف، وسائل التعريف لبيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي كما تظم أيضا ما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفاذ.

2. **الوسائل المتعلقة بالتحكم في الدخول والنفاذ إلى الشبكة:**

وهي الوسائل التي تساعد على التأكد من أن الشبكة قد استخدمت بطريقة مشروعة ومن أهم الوسائل الفنية المعتمد عليها ما يعرف بالجدران النارية والتي هي عبارة عن برامج تثبت داخل النظام بغرض مراقبة المنافذ التي يتم من خلالها نقل البيانات من وإلى الجهاز أثناء التعامل مع شبكة الإنترنات، فيتم إجبار جميع عمليات الدخول إلى الشبكة أو الخروج منها بأن تمر من خلال هذا الجدار الناري والذي يمنع أي مخترق أو متطفل من الوصول إلى الشبكة. وذلك عن طريق مراقبة الحزم الذي يتم إرسالها واستقبالها من الحاسب الآلي الخاص بالمستخدم. وعند مراقبة الجدار الناري لهذه الحزم والمنافذ التي ترسل وتستقبل من خلالها فإن عليه السماح أو الاعتراض على دخول هذه البيانات أو خروجها. وتنبه المستخدم لذلك.

3. الوسائل التي تهدف إلى منع إفشاء المعلومات لغير المخولين أو المصرح لهم بذلك:

وتهدف هذه الوسائل إلى ضمان سرية المعلومات وتشمل تقنيات تشفير المعطيات والملفات، إجراءات حماية نسخ الحفظ الاحتياطية، برامج الفلترات (Filtration) والموجهات.

4. **الوسائل التي تهدف إلى حماية التكاملية وسلامة المحتوى:** وهي الوسائل المناط بها ضمان عدم تعديل محتوى المعطيات من قبل جهة غير مخولة لها ذلك، ومن أهمها برامج تحري الفيروسات ومضادات الفيروسات(Antivirus).
5. **الوسائل المتعلقة بمنع الإنكار:** وتهدف هذه الوسائل إلى ضمان عدم قدرة الشخص المستخدم على إنكار أنه هو الذي قام بالتصرف، وترتكز هذه الوسائل بصفة أساسية على تقنيات التوقيع الإلكتروني وشهادات التوثيق الصادرة من طرف ثالث.
6. **وسائل مراقبة الاستخدام وتتبع سجلات النفاذ والأداء:** وهي التقنيات التي تستخدم لمراقبة مستخدمي النظام وتحديد الشخص الذي قام بالعمل المعين في الوقت المعين وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التي تحدد الاستخدام.

وهذه الوسيلة قد أشار إليها المشرع الجزائري في القانون 04/09 (التزامات مزودي الخدمة) في المادة 10 منه، حينما ألزم مقدمي الخدمات العمل على حفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة المتعلقة بتاريخ ووقت ومدة كل اتصال بالإضافة إلى حفظ المعطيات التي تسمح بالتعرف على المرسل إليه الاتصال وعنوان الموقع المطلع عليه.

وتجدر الإشارة أن كل مؤسسة أو هيأة لها طريقتها الخاصة في توفير الأمن الفني في حدود متطلبات حماية المعلومات، فلا تكون إجراءات الأمن الفني، رخوة ضعيفة لا تكفل الحماية وبالمقابل لا تكون مبالغاً فيها إلى حد يؤثر على عنصر الأداء في النظام محل الحماية، فتعقيد الحماية على المعلومات لدرجة يصعب فيها حتى على المخولين الوصول إليها

قد يدفع لاحقا إلى إهمال كل الإجراءات الأمنية، مما يجعل المعلومات عرضة للخرق وهذا ما يسمى لدى الخبراء التقنيين في مجال أمن المعلومات "التأثير على صحة الأداء وفعاليته".

وفي الحقيقة فإن جميع هذه الوسائل الغرض منها هو تحقيق أمن معلوماتي أفضل ضمن فضاء افتراضي يتم فيه تبادل المعلومات الرقمية وتجري عبره كافة أنواع المعاملات والخدمات الالكترونية بواسطة تقنيات وبرمجيات وبروتوكالات تتجدد وتتطور بشكل متسارع، لذلك فإن الأمر يقتضي إجراء عمليات تقييم للآثار الناجمة عن هذه الوسائل من أجل الوقوف على مدى نجاعتها في تحقيق النتائج المرجوة منها.

الفرع الثاني: الحماية الفنية عن طريق نظام الرقابة الوقائية عبر الوسائل الالكترونية

من القواعد الفنية الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة على النظام والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها نظام المراقبة الإلكترونية، إذ يعد هذا النظام من بين أهم آليات الوقاية من جرائم المعلوماتية.

ويقصد بمراقبة الاتصالات الإلكترونية، العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبطا بالزمن لتحقيق غرض أمني.[1]

ولم يتطرق المشرع الجزائري شأنه شأن التشريعات المقارنة إلى تحديد المقصود بمراقبة الاتصالات الإلكترونية، مكتف فقط بتحديد مفهوم الاتصالات الإلكترونية[2] رغم أخذه بهذا النظام بموجب المادة 03 من القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة

[1] رشيدة بوكر، المرجع السابق، ص 370.

[2] المادة 02 من القانون 04/09 عرفت الاتصالات الالكترونية بأنها "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية"

بتكنولوجيات الإعلام والاتصال، والتي تنص على إمكانية وضع الترتيبات التقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، إذا تطلبت ذلك حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية. وذلك مع مراعاة الأحكام القانونية التي تتضمن سرية المراسلات والاتصالات[1].

وفي هذا الإطار نجد أن المشرع الجزائري قد ميز بين نوعين من المعطيات المعلوماتية محل المراقبة الإلكترونية، وهما المعطيات المتعلقة بحركة السير (معطيات المرور) والمعطيات المتعلقة بمحتوى الاتصال، فبالنسبة للنوع الأول فقد عرفها المشرع بموجب المادة 02 من القانون 04/09 بأنها " أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات توضح مصدر الاتصال، والوجهة المرسلة إليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة،[2] أما النوع الثاني والمتعلقة بالمحتوى فلم يأت على تعريفها، وإن كانت تتعلق بمضمون الاتصال أو الرسالة أو المعلومات المنقولة عن طريق الاتصال فيما عدا المعطيات المتعلقة بالمرور، واعتبر المشرع أن هذا النوع الأخير من المعطيات هو ما يكون محلا للمراقبة الإلكترونية عندما أدرجها في

[1] نصت المادة 21 من الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية بودابست تحت عنوان اعتراض معطيات المحتوى على أنه: "يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من أجل تحويل السلطات المختصة فيما يتعلق بالجرائم الخطيرة التي يحددها القانون الداخلي المكنات التالية:

– جمع أو تسجيل عن طريق تطبيق الوسائل الفنية المتواجدة على أرضه.

– إلزام مقدم الخدمة في نطاق قدراته الفنية المتوافرة على أن يمنح السلطات المختصة عون ومساعدته من أجل تجميع أو تسجيل في الوقت الفعلي المعطيات المتعلقة بمحتوى اتصالات معينة.

[2] نصت المادة الأولى من اتفاقية بوادابست على تعريف لمعطيات المرور كما يلي: "أنها كل البيانات التي تعالج الاتصالات التي تمر عن طريق نظام معلوماتي والتي تتم إنتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصرا في سلسلة الاتصال مع تعيين المعلومات التالية: أصل الاتصال مقصد الاتصال الجهة المقصودة بالاتصال، خط السير، ساعة وتاريخ الاتصال، حجم وفترة الاتصال، أو نوع الخدمة".

المادة 04 تحت مسمى مراقبة الاتصالات الإلكترونية، أما النوع الأول فقد خصها بإجراء آخر تحت مسمى حفظ المعطيات المتعلقة بحركة السير في المادة11.

وقد أكدت اتفاقية بوداسبت هذا التمييز، حيث أدرجت كل إجراء على حدى تحت عنوان خاص، فخصت حركة المعطيات بعنوان التجميع في الوقت الفعلي لمعطيات المرور (المادة 20) أما محتوى المعطيات فجاء تحت عنوان اعتراض معطيات المحتوى.

والملاحظ أنه وإن كان من المقبول أن كلا من النوعين من المعطيات يمكن أن تمس مصالح ذات طبيعة خاصة، إلا أنه وبالنسبة لمعطيات المحتوى فإن المصالح الفردية تكون أعلى نظرا لطبيعة محتوى المعطيات، ومن هذا المنظور يمكن فرض قيود على محتوى المعطيات بشكل أشد من تلك الخاصة بمعطيات المرور.

ومما لاشك فيه أن هذه المراقبة الإلكترونية لمحتوى الاتصالات الإلكترونية من شأنها المساس بالحق في الخصوصية، لذلك فإنه ينبغي إحاطتها بجملة من الضمانات بغرض تحقيق التوازن بين حق الإنسان في الخصوصية وحماية سرية اتصالات هو حق المجتمع في مقاومة الجريمة. ولعل أهمها أن يتم تنفيذ هذا الإجراء بإذن من القضاء. وأن تكون ثمة ضرورة تدعو إليه وفي نطاق ضيق من أجل الوقاية من الجرائم التي تمس حقوقا ذات أهمية لاعتبارات يقدرها المشرع. وهو ما سنأتي على بيانه في حينه.

المبحث الثاني: وسائل الإثبات للجريمة المعلوماتية.

يختلف الوسط الذي ترتكب فيه الجريمة المعلوماتية من وسط مادي إلى وسط معنوي إما يعرف بالوسط الافتراضي، وعلى ضوء ذلك فإن أدلة الإثبات في إطار مدى اتفاقها مع الطبيعة التقنية لهذه الجرائم ووسائل ارتكابها أصبح غير ذي معنى إذا لم يكن مدعما بتوفيق من قبل التقنية ذاتها، مما أدى إلى ظهور طائفة خاصة من الأدلة الإجرامية يمكن الاعتماد عليها في إثبات هذه الجرائم ومن ثمة نسبها إلى فاعلها بحيث يكون من ذات الطبيعة التقنية الناجمة عن النظم المعلوماتية التي تنتج عنها في حالة الاعتداء عليها مع طبيعة الوسط الذي ارتكبت فيه الجريمة وهي الأدلة الرقمية أو الأدلة الالكترونية حسب ما عبرت عنها الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية.

فالدليل أثر يولد أو حقيقة تنبعث من الجريمة المرتكبة، ولذلك فإن طبيعة الدليل يتشكل من طبيعة الجريمة التي يولد منها، فدليل التزوير يأتي من إثبات تغير الحقيقة في المحرر الذي يقع عليه، ودليل جريمة القتل قد يولد من فحص الأداة التي استخدمت في القتل وطلقات الذخيرة التي استعملت فيها، وتطبيق ذلك على الجريمة المعلوماتية فإنه يمكن أن تثبت بأدلة تقنية ناتجة عن الوسائل التقنية التي ارتكبت بواسطتها.

المطلب الأول: الدليل الرقمي.

إن الدليل الرقمي مأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجمعها أو تحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء، وهناك من يعرفه بأنه معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة النظم المعلوماتية وملحقاتها وشبكات الاتصال، ويمكن استخدامها

في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جاني أو مجنى عليه، وأنه الدليل الذي يوجد له أساسا في العالم الافتراضي.

كما عرف الدليل الرقمي أيضا أنه مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها و تحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية.

فالدليل الرقمي هو أي معلومات سواء كانت من صنع الإنسان أو تم استخلاصها من الحاسوب يتقبلها العقل والمنطق.

كما ذهبت بعض التعريفات إلى أن الأدلة الجنائية الرقمية ما هي إلا مرحلة متقدمة من الأدلة المادية الملموسة التي يمكن إدراكها بإحدى الحواس الطبيعية فلإنسان إلى الاستعانة بجميع ما يبتكره العلم من وسائل تقنية عالية ومنها الحاسوب، ولكن الحقيقة أن الأدلة الرقمية هي نوع متميز من وسائل الإثبات ولها من الخصائص العلمية والمواصفات القانونية.

الفرع الأول: خصائص الدليل الرقمي: تقوم خصائص الدليل الرقمي على مدى ارتباطه بالبيئة الافتراضية والذي يتميز بعدة خصائص تميزه عن الدليل الجنائي التقليدي.

1. **الدليل الرقمي هو دليل علمي:**أي أنه يحتاج إلى بيئته التقنية التي يتكون فيها لكونه من طبيعة تقنية المعلومات ذات المبنى العلمي ومن ثمة فإن ما ينطبق على الدليل العلمي ينطبق على الدليل الرقمي.
2. **الدليل الرقمي من طبيعة تقنية:** الدليل الرقمي يجب أن يكون مستنبطا من البيئة الرقمية أو التقنية وهي في إطار جرائم المعلوماتية ممثلة في العالم الرقمي أو العالم الافتراضي.
3. **الدليل الرقمي دليل متنوع و متطور:** يشتمل الدليل الرقمي كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقميا بحيث يكون بينها وبين الجريمة رابطة من نوع خاص وتتصل

بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني وتعني هذه الخاصية أنه على الرغم من أن الدليل الرقمي في أساسه متحد التكوين بلغة الحوسبة والرّقمية، إلا أنه مع ذلك يتخذ أشكالا مختلفة يمكن أن يظهر عليها، كأن يكون بيانات غير مقروءة من خلال ضبط مصدر الدليل كما هو الشأن حال المراقبة عبر الشبكات،و قد يكون بيانات مفهومة كما لو كان وثيقة معدة بنظام المعالجة الآلية كما من الممكن أن يكون صورة ثابتة أو متحركة (أفلام رقمية) أما عن كون الدليل الرقمي دليلا متطورا فهي خاصية تكاد تكون تلقائية، نظرا لارتباطه بالطبيعة التي تتمتع بها حركة الاتصال عبر الأنترنت و العالم الافتراضي.

4. **الدليل الرقمي صعب التخلص منه:** إن القاعدة التي تسري على كافة ما يتعلق بهيكلة تكنولوجيا المعلومات، هي أنه كلما حدث اتصال بتكنولوجيا المعلومات في معنى إدخال بيانات إلى ذلك العالم فإنه يصعب التخلص منها، ويمكن اعتبار هذه الخاصية ميزة يتمتع بها الدليل الرقمي عن غيره من الأدلة التقليدية.
5. **الدليل الرقمي ذو طبيعة رقمية ثنائية(1-0):** إن الآثار التي يتركها مستخدم النظام المعلوماتي والتي تشمل الرسائل المرسلة منه أو التي استقبلها و كافة الاتصالات التي تمت من خلال الحاسب الآلي وشبكة الاتصال تكون على شكل الرقمي، فالبيانات الموجودة داخل الحاسب الآلي سواء كانت في شكل نصوص أو حروف أو أرقام أو فيديو تحول إلى صيغة رقمية حيث ترتكز تكنولوجيا المعلوماتية الحديثة على تقنية الترقيم التي تعني ترجمة أو تحويل أي مستند إلى نظام ثنائي في تمثيل الأعداد يفهمه الحاسب الآلي قوامه الرقمان(0) و (1) فأي شيء في العالم الرقمي يتكون من الصفر والواحد.

كما يأخذ الدليل الرقمي في تحديد أنواعه إلى نوعين رئيسين هما:

أ. السجلات التي تم إنشاؤها بواسطة الجهاز التلقائي وتعتبر هذه السجلات من مخرجات الجهاز ولم يساهم الإنسان في إنشائها.

ب. السجلات التي جزء منها تم حفظه بإدخال وجزء تم إنشاؤه بواسطة الجهاز ومن أمثلة ذلك البيانات التي تم إدخالها إلى الأدلة وتتم معالجتها من خلال برامج خاصة وأما النوع الثاني أي الأدلة الرقمية التي تعد لتكون وسيلة إثبات فهي تلك الأدلة التي تنشأ دون إرادة الشخص بمعنى أي أثبر يتركه دون أن يكون راغبا في وجوده ويسمى هذا النوع من الأدلة بالبصمة الرقمية أو الآثار المعلوماتية للرقمية، وهي تتجسد في الآثار التي يتركها مستخدم النظام المعلوماتي بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال النظام المعلوماتي و شبكة الاتصالات.

الفرع الثاني: مصادر الحصول على الدليل الرقمي:

إن مصادر الحصول على الدليل الرقمي تكمن في البيئة الرقمية التي ارتكبت فيها الجريمة المعلوماتية، وتتمثل في أجهزة الحواسيب الخاصة بالجاني أو المجنى عليه وكذا أجهزة مقدم الخدمة.

وهذه المصادر قد تكون على سبيل المثال لا الحصر إذ أن التطور العلمي والتقني قد يسفر على أنواع جديدة من المصادر التقنية، إذ المقصود هنا من أين يمكن لجهات التحقيق والتحري عن الجريمة المعلوماتية استخلاص الدليل الرقمي.

الفرع الثالث: فحص جهاز الحاسوب الخاص بالجاني والمجنى عليه:

إن فحص جهاز الحاسوب الخاص بالجاني يمكن من التحقيق وبيان الطريقة التي قام بها هذا الأخير في ارتكاب جرائمه، ومما لا شك فيه أن المجنى عليه هو المصدر الكاشف

والنتيجة التي يترتب عليها ما قام به الجاني من جرائم، وبالتالي فإن فحص جهاز الحاسوب الخص به يمكن المحقق من معرفة الدخول و تتبع مصدره.

ويمكن الوصول إلى الدليل الرقمي المتعلق بالجرائم المعلوماتية من خلال أجهزة الحاسوب سواء الخاصة بالجاني أو المجنى عليه عن طريق البحث في المصدرين التاليين:

أولا: أنظمة الحاسوب وملحقاتها:

تعد الحواسيب مصدرا غنيا بالأدلة الرقمية خاصة تلك الحواسيب الشخصية التي تعد بمثابة أرشفة سلوكية للأفراد، فهذه الحواسيب تحتوي على الكثير من المعلومات المتعلقة بنشاطات الأفراد ورغباتهم وعملية حجز الحاسوب بقصد تفحصه تعد نقطة البداية في الكشف عن خفايا الجريمة المعلوماتية باعتبار أن هذا الجهاز هو وسيلة تنفيذها، والحاسب الآلي في ذاته يقوم في تركيبته على أمرين هما: القطع الصلبة (hardware) والقطع المرنة أو البرمجيات (soft ware) وهناك عنصر ثالث يتوزّع بين البرمجيات والقطع الصلبة وهو عنصر المعلوماتية.[1] لذلك فإن الأمر يستلزم أن يكون الفحص ماديا ومعنويا للارتباط القائم بشكل طبيعي بين مكونات الحاسوب ككل.

وقد تعتمد عملية الفحص على الحاسوب ذاته أي ما يسمى بالفحص الذاتي من خلال قيام الحاسوب ذاته بفحص مكوناته وتقديم تقرير كامل بذلك إلى طالب الفحص، ومثل هذه العملية تتطلب من القائم بها مهارة عالية أو قد يتم الفحص عن طريق الاستعانة بجهاز آخر أو أجهزة تقنية للبحث في جزئيات عبر جهاز الحاسوب، ويجب أن تشمل عملية الفحص على ما يلي:

[1] حسين بن سعيد بن سيف الفاغري، المرجع السابق، ص425.

1. **فحص القرص الصلب:** يحتوي القرص الصلب بداخله على مجموع البيانات الرقمية ذات الطابع الثنائي والتي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي(1-0). وتتم عملية فحص القرص الصلب إما كليا أو جزئيا فالفحص الجزئي يؤدي إلى التعرف على محتوى البيانات والتي يؤدي التعامل معها إلى الكشف عن القيمة الاسترادادية للبيانات المخزونة فيه سواء كانت محتويات مكتوبة،صور أو أصوات.... إلخ.

بالإضافة إلى إمكانية معرفة ما تم حذفه من بيانات و برامج الاستعانة ببرمجيات خاصة للقيام بذلك.[1] والمثال المستخدم هنا هو حالة البحث في ملفات النسخ وهذه الأخيرة عبارة عن ملفات تأخذ نسخة احتياطية في كل صفحة يتم الولوج إليها عبر الأنترنت كما توجد ملفات خاصة بالتنزيل(Dowlond file) مهمّتها استقبال الملفات التي يتم تحيلها على جهاز الحاسب الآلي من خارجه وعبر الأنترنت فهذه الملفات مركزها القرص الصلب.

وللتعرف على محتويات القرص الصلب فإن ذلك يتوقف على مسائل عديدة منها الكيفية التي يتم بها ضبط الحاسوب ومهارة الشخص القائم باستخلاص البيانات دون العبث بمحتوياتها لذلك فإنه عند ضبط جهاز الحاسب الآلي، على المحقق أن ينتزع القرص من الجهاز الخاص به ويحافظ عليه من الارتجاج أو الاصطدام بأي شيء، وعدم محاولة تفريغ أي بيانات متواجدة عليه وذلك تفاديا لفقد أي بيانات، وتسليمه إلى الفني الخبير المختص الذي يقوم بتحليل النسخ التي تصدر من القرص وبعرض ما ترسل إليه على المحقق.

وهنا لا بد من مراعاة شرط سلامة جهاز الحاسب الآلي، الذي يعني صحة حركة القطع الصلبة فيه وذلك لتجنب الوقوع في مأزق رفض المحكمة الاعتداد بالدليل المنبثق عنه، فشرط سلامة الحاسوب مطعن رئيسي على كل دليل ثم الحصول عليه بحيث يجب الكشف

[1] عمر أبو بكر بن يونس، المرجع السابق، ص10-11.

على حركة الحاسوب بداية والإقرار بسلامته.[1] وإن من الأشياء التي تظهر بعد عملية فحص أو قرص صلب لأي جهاز تلك البيانات التي كان يستخدمها الجاني، وكذا الصور المخزنة فيه ومخابئ صفحات الأنترنت، ومن خلالها يمكن التوصل لصفحات وعناوين مواقعه الأنترنت وكذا رسائل البريد الالكتروني بالإضافة إلى رؤوس الصفحات المرسلة والمتلقاة ومجموعة البرامج الجاهزة والمتخصصة التي استخدمها(المشتبه فيه) ومنها يمكن تحديد أصدقاء(المشتبه فيه) وكذا تحديد ما يتحاورون فيه.

2. فحص البرمجيات:

يتطلب الأمر في مثل هذه الحالة أن نميز بين الفحص الداخلي للبرمجيات والفحص الخارجي لها، فالفحص الداخلي يتم من خلال البحث في البناء المنطقي للبرمجة بما يوحي أن هناك مجهودا تجديديا في إعداده للعمل حين إنزاله على جهاز الحاسب الآلي (installation) خلال تتبع خطوات منطقية تعبر عن هذا الجهد، وأكثر ما يتم البحث عنه في إطار الفحص الداخلي هو البحث عن مصدر الملفات الموجودة في هذا الإطار، ذلك أن النسخ عبر الأنترنت لا يشبه النسخ باستخدام برمجيات المعالجة فالأول نسخ عبر العالم الافتراضي والثاني يتم باستخدام مصنف متداول في العالم المادي، وتفيد وسيلة النسخ في ترتيب كيفية حدوث الجريمة.

أما في حالة الفحص الخارجي والذي يتم اللجوء فيه إلى النسخة الأصلية للمقارنة بينهما وبين النسخة محل الاشتباه و ذلك للدلالة على ثبوت ارتكاب الجريمة بدرجة مقنعة.

[1] خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص215.

وفي كلتا الحالتين ينبغي التنبيه إلى خطورة البرمجيات المعيبة التي يمكن أن تؤثر في الحاسوب و تجعله محل شك تهتز معه قيمة الدليل، يكون لهذا القصور أثره في عملية تقييم الدليل المستمد من البرمجيات ذاتها.[1]

3. فحص النظام المعلوماتي:

إن المهمة الأساسية لكل نظام معلوماتي هو تحقيق فرضية تنفيذ الأوامر التي يمكن أن يقوم بها مستخدم الحاسوب، وتعني عملية فحص النظام المعلوماتي ضبط كافة ما يحتويه جهاز الحاسب الآلي من معلومات [2] يمكن استرجاعها عبره تكون مخزنة في ملفات على أي شكل يمكن أن تكون عليها الحركة الاسترادادية مادام موضوعها يشكل جريمة.

والحقيقة أنه على حسب كثرة التعامل بالحاسب الآلي يتكاثر محتوى النظام المعلوماتي مما يزيد من صعوبة فحصه بالنظر إلى الحجم الضخم والكم الهائل من المعلومات المخزنة فيه.

بالإضافة إلى أن عملية تخزين البيانات لا تتخذ شكلا محددا وإنما تتنوع أساليبها، والتي يصل مداها إلى حد إمكانية تخزين البيانات بشكل آمن في الحاسوب بنظام التشغيل أو بنظام إخفاء البيانات المعلوماتية بحيث لا يظهر الملف حتى في حالة البحث الآلي للحاسب عنه والذي قد يحتوي على مواد إجرامية، وتفوت الفرصة بسبب هذه التقنية على المحققين من الوصول إليه [3].

---

[1] خالد ممدوح إبراهيم، المرجع السابق، ص219.

[2] إن النظام المعلوماتي للحاسب الآلي لا يحتوي على معلومات مكتوبة كما هو المعتقد السائد، وإنما المحتوى المعلوماتي عادة ما يتكون من بيانات ثنائية الهيئة الرقمية يتم إيداعها في الحاسب الآلي في شكل تخزين ويقوم الحاسوب بمعالجة هذه البيانات ويبرزها على هيئة معلومة محددة حيت يتم استدعاؤها من قبل المستخدم الحاسوب وما دام لم يتم استدعاء معلومات محددة فإن بياناتها تضل في حالة تخزين في الحاسوب فلا يقوم الحاسوب باستدعاء كافة المعلومات مرة واحدة.

[3] خالد ممدوح إبراهيم، المرجع السابق، ص222.

ثانيا: فحص أنظمة الاتصال بالأنترنت:

يقصد بنظام الاتصال بالأنترنت بالمفهوم الإجرائي هو تلك الإجراءات أو المراحل المتبعة حال استخدام الاتصال بالأنترنت، ومن أهم المسائل المثارة في صدد فحص أنظمة الاتصال بالأنترنت سعيا وراء البحث عن الدليل هي مسألة تحديد مكان الجريمة أو جهاز الحاسب الآلي الذي انطلق منه النشاط الإجرامي، وذلك من خلال تتبع الحركة العكسية لمسار الأنترنت أي تتبع الحركة التراسلية للنشاط الممارس من خلال الأنترنت، فالحاسوب بمجرد أن يتعرف على المسار يقوم تلقائيا باختيار البروتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات.[1]

ويستخدم في عملية تتبع حركة مسار الأنترنت نظام فحص الكتروني يطلق عليه علم البصمات المعاصر،[2] وما يتم التوصل إليه بعد ذلك هو عنوان رقمي يسمى Protocol internet adress IP وهو عبارة عن بروتوكول لعنونة البيانات والمواقع في شبكة الأنترنت، وبمقتضى هذا البروتوكول (IP) يتم التعرف على الكمبيوتر الموصول بشبكة الأنترنت من خلال عناوين عديدة، حيث لكل كمبيوتر عنوانه الوحيد والخاص به تماما،[3] يسمىAdresse IP وكل عنوانIP مكون من جزأين:

الأول يشمل أرقام الشبكة والثاني يشمل أرقام مقدم الخدمة، ويعمل بروتوكول IP بشكل متزامن مع هذا بروتوكول آخر وهو بروتوكول التحكم بالنقل (PROTOCOL Tram mission control) TCP وهذان البروتوكولان(TCP/IP) هما من عائلة بروتوكولات الاتصال بين عدة

[1] عمر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، المرجع السابق، ص998.

[2] وقد تم استخدام هذا المنهج في الكشف عن العديد من الجرائم مثل تتبع مبتكر فيروس ميليسا وكذا التوصل إلى الشخص الذي ابتكر مواقع خدمات بولمي روج لأخبار المال الاحتياطي لكي يرفع الأسهم بطريق الخداع.

[3] عبد الحميد عبد المطلب استخدم بروتوكول TCP/IP TD FPE فيبحث وتحقيق الجرائم مع الكمبيوتر، المرجع السابق، ص05.

أجهزة من الحواسيب طورت أساسا لنقل البيانات بين أنظمة(UNIX)،[1] ثم أصبحت المقياس المستخدم لنقل البيانات الرقمية عبر شبكة الأنترنت، ويرتكز البروتوكولان معا (TCP/IP) على تقنية التبديل المعلوماتي بواسطة الحزم المعلوماتية(Packet) بين مختلف الوصلات السلكية واللاسلكية المتخصصة التي تربط الشبكات المختلفة الموصولة فيما بينها.

وحزمة المعلومات جزء أو قسم من ملف معلوماتي ذات حجم مصغر ثابت تحمل كل منها رقما خاصا ومعلومات تعريفية بكل من المرسل والمرسل إليه، وعند كل وصلة تتم قراءة جهة المقصد أو المرسل إليه ثم تتم إعادة إرسال الحزم المارة عبرهما نحو الوصلات التالية الأقرب إلى جهة المقصد النهائية.

ويعتبر نظام (TCP/IP) من أكثر البروتوكولات المستخدمة في شبكة الانترنت فهو جزء أساسي منه، لذلك تبرز أهمية الاستعانة بالمعلومات والمصادر والعناوين التي يمكن أن يحتويها هذا البروتوكول في تحقيق الجرائم المعلوماتية، حيث تدل بصفة جازمة عن مصدر الجهاز المستخدم في الجريمة وتحديد الأجهزة التي أصابها الضرر من الفعل الإجرامي وتحديد نوعية النشاط الإجرامي من خلال الفترة الزمنية لاقتراف الجريمة.[2]

ويتنازع إمكانية تحديد مسار الأنترنيت من عدمه رأيان، إذ يذهب رأي إلى أنه لا يمكن تحديد مسار ارتكاب الجريمة وتكمن واجهة هذا الرأي في أن شبكة الأنترنات ذات طبيعة مرنة بحيث أنه حتى وإن أمكن مستقبلا تحديد مسار الانترنات، فإن ما يتم الحصول عليه في هذا الإطار إنما هو دليل رقمي يحتاج إلى تكملته بأدلة إثبات أخرى فيما لو اقتصر الأمر على هذا

---

[1] UNIX هو نظام تشغيل متعدد المهام و متعدد المستخدمين مصمم لاستخدامه في الكمبيوتر المنزلي أو المكتبي لاعتبار أن هذا النظام مكتوب بلغة c لذلك فهو أكثر قابلية للنقل المعلوماتي من الأنظمة الأخرى، واللغة C لغة برمجة عالية المستوى صمت أصلا لتعمل تحت النظام UNIX ومستخدمة في كتابة كافة التطبيقات بعد أن يرى وضع مقاييسها من قبل المعهد القومي الأمريكي للمقاييس.

[2] ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص01.

الدليل فإن الأمر يظل في حومة الشك،[1] ذلك أن ما يتم التوصل إليه في الحقيقة من خلال الدليل الرقمي إنما هو عنوان رقمي فقط adresse TP وهذا لا يكفي في نسبة العمل الإجرامي إلى صاحب الحاسوب أو العنوان المذكور، إذ من الممكن ألا يكون هو مرتكب الجريمة كم لو كان جهاز الحاسوب مسروقا أو يكون أحد يستخدمه احتيالا أو يتم استخدام جهاز الحاسوب في مقهى الأنترنات، فمثل هذه الأمور تجعل من الصعوبة بمكان الاعتماد على مسار حركة الأنترنات للتوصل إلى تحديد شخص الجاني وإنما قد يحتاج الأمر إلى دليل مادي مكمل للدليل الرقمي، ويمكن التأكيد على أنه حتى في الحالات التي تمت فيها إدانة الأشخاص أمام القضاء المقارن كان هناك دائما دليل مادي يتم الاستناد إليه إلى جوار الدليل الرقمي، في حين يذهب الرأي إلى القول بإمكانية تتبع مسار الأنترنت ويمكن من خلال هذا التتبع التوصل إلى تحديد مسار العمل الإجرامي.

وتجدر الإشارة إلى أنه في إطار فحص نظام الاتصال بالأنترنت كمصدر يمكن من خلاله البحث عن الدليل الرقمي، يتضمن أيضا لزوم فحص الخادم أو الملقم Serveur وهو حاسوب ضخم مهمته تحقيق حركة الاتصال بالمواقع والصفحات التي تتم استضافتها على هيئة رقمية فيه، لذلك فإنه يطلق على الخادم Lieu de stockage numérisées des données.

- **تعاون مزودي الخدمة من جهات التحقيق:** لما كان الدليل الرقمي قابع في البيئة التقنية ويتسم بخصائصها، وهي خصائص تبنى على أساس الطبيعة المرنة التي يبنى عليها العالم

[1] خالد ممدوح إبراهيم، المرجع السابق، ص 207 208.

الافتراضي، فإن للفاعل إمكانية إزالة الدليل من على بعد باستخدام التقنية ذاتها، من أجل ذلك استلزم الأمر وضع إطار قانوني وهو نظام إلزام مزودي الخدمة[1] بحفظ المعطيات.

وهذا ما تضمنه قرار الجمعية العامة للأمم المتحدة رقم(63/55) المؤرخ في 2001/01/22 والمتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية في الفقرة "و" من المادة الأولى منه والتي ألزمت الدول أ تسمح بحفظ المعطيات الالكترونية المتعلقة بالتحقيقات الجنائية الخاصة وسرعة الوصول إليها وهو ما أكده المشرع بموجب المادة 10 من الفصل الرابع في القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها تحت عنوان" التزامات مقدمي الخدمات".

أولا: المقصود بمزودي الخدمات:

حسب المادة الأولى فقرة ج من اتفاقية بودابست فإن مزود الخدمة هو كل من يقوم بخدمات الإيصال أو خدمات معالجة البيانات أو خدمات تخزين البيانات وقد يكون جهة عامة أو جهة خاصة وقد يقدم خدماته للجمهور أو لمجموعة من المستخدمين الذي يشكلون مجموعة مغلقة.

ويعرف قانون الحماية الخاصة في مجال الاتصالات الالكترونية في الولايات المتحدة الأمريكية نوعين من مزودي الخدمة:

- **النوع الأول:** مزود خدمة الاتصالات الالكترونية و يقصد به كل من يقدم خدمة إلى مستخدمي الشبكة والتي تتمثل في تسهيل إرسال الاتصالات الالكترونية.

[1] أورد المشرع الجزائري في المادة 10 أنه في إطار تطبيق أحكام هذا القانون (04/09) يتعين على مزودي الخدمة تقديم المساعدات للسلطات المكلفة بالتحريات القضائية ... بوضع المعطيات التي يتعين عليهم حفظها وفقا لأحكام المادة 11 أدناه تحت تصرف هذه السلطات.

- **النوع الثاني:** وهو مزود خدمة الحوسبة عن بعد و يقصد به كل من يقدم للجمهور خدمة معالج البيانات عن بعد بوسيلة من وسائل الاتصالات الالكترونية.

وقد عرف المشرع الجزائري مزود الخدمة (مقدم الخدمة) بموجب الفقرة06 من المادة الثانية من القانون 04/09 بأنه:

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

وعلى هدي ذلك فإن المراسلة بالبريد الالكتروني والتي يتم استقبالها بواسطة مزود الخدمة الخاص بالمرسل إليه والتي لم يطلع عليها بعد، فإنها تستقر في حالة تخزين الكتروني وتكون في هذه المرحلة نسخة من الاتصال المخزنة تتواجد فقط كإجراء أو وسيط مؤقت في انتظار استقبال المرسل إليه لها من مزود الخدمة وبمجرد استلام المرسل إليه المراسلة بالبريد الالكتروني فإن الاتصال يكون قد وصل إلى وجهته الأخيرة، وهنا يكون موقف مزود الخدمة يتراوح بين أمرين: إما أن يقوم بمسح تلك الرسالة أو يقوم بالاحتفاظ بها.[1]

[1] تجدر الإشارة إلى أنه من الأهمية بمكان التفرقة بين مصطلحي التحفظ على المعطيات والاحتفاظ أو أرشفة المعطيات فرغم أن للكلمتين معنيين متجاورين في اللغو الشائعة لكن لهما معنى مختلفا في اللغة المعلوماتية إذ أن عبارة يتحفظ على المعطيات تعني حفظ معطيات سبق وجودها في شكل مخزن وحمايتها من كل شيء يمكن أن يؤدي إلى إتلافها أو تجريدها من صفتها أو حالتها الراهنة في حين أن عبارة الاحتفاظ حفظ المعطيات لدى حائزها بالنسبة لمستقبلي المعطيات في طور الإنتاج والتوالد ومعنى ذلك أن أرشفة المعطيات عبارة عن عملية تخزين للمعطيات على عكس التحفظ عليها الذي يعني النشاط الذي يضمن للمعطيات سلامتها وسريتها.

ثانيا: التزامات مقدمي الخدمة: ألزم المشرع الجزائري مقدمي الخدمات بحفظ المعطيات،[1] وذلك بتجميع المعطيات المعلوماتية وحفظها وحيازتها في أرشيف ووضعها في ترتيب معين في انتظار اتخاذ إجراءات قانونية محتملة أخرى كالتفتيش وغيره.

وما تجدر الإشارة إليه في هذا الإطار أنه ليست أي معطيات معلوماتي محل اعتبار من المشرع، بل حصل المشرع الجزائري المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمة في المعطيات المتعلقة بحركة السير(معطيات المرور)، وهي كلمة عرفها في المادة الثانية من القانون 04/09 تلك المعطيات المتعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة.

باعتبارها جزءا من حلقة الاتصالات، توضح مصدر الاتصال، الوجهة المرسل إليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الاتصال، ونوع الخدمة، وقد حصر المشرع معطيات المرور التي ألزم في المادة 11 مزوّدي الخدمة بحفظها في:

1. المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
2. المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
3. الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.
4. المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.
5. المعطيات التي تسمح بالتعرف على المرسل إليه و كذا عناوين المواقع المطلع عليها.

وقد عرفت اتفاقية بودابست في مادتها الأولى فقر "د" هذا النوع من المعطيات بأنها صنف من بيانات الحاسوب التي تشكل محلا لنظام قانوني محدد، حيث يتم توالد هذه المعطيات من

[1] آثر المشرع الجزائري استعمال عبارة حفظ المعطيات في المادة 11 بدل التحفظ على المعطيات وذلك عكس ما فعلت اتفاقية بودابست في المادة 16 منها وهو بذلك إما أنه لا يفرق بين المصطلحين أو أنه لا يقيم أهمية لمسألة ضمان أمن المعطيات من خطر التغير أو التجريد من صفتها أو حالتها الراهنة.

الحواسيب عبر تسلسل حركة الاتصالات لتحديد سلك الاتصالات من مصدرها إلى الجهة المقصودة، وهي بذلك تشمل طائفة من المعطيات تتمثل في مصدر الاتصال ووجهته المقصودة خط السير، وقت أو زمن الاتصال، حجم الاتصال ومدته ونوع الخدمة المؤداة.

وبما أن حفظ المعطيات إجراء وقتي واحترام للحق في الخصوصية فإن المشرع الجزائري وضع التزاما على مزودي الخدمات بإزالة المعطيات التي يقومون بتخزينها بعد سنة من تاريخ التسجيل،[1] وعلى غرار المشرع الجزائري نجد المشرع الفرنسي حرص بدوره في نطاق التخزين التلقائي للمعطيات المتعلقة بالاتصالات الالكترونية.

وذلك بموجب المادة 32 من قانون البريد والاتصالات المضافة بموجب المادة 29 من القانون رقم 1062/2001 والمعدلة بالمادة 20 من القانون239/2003 المؤرخ في: 2003/03/18 المتعلق بالأمن الداخلي على ضرورة مسح المعطيات المخزنة بعد الاحتفاظ بها لمدة أقصاها سنة إذا دعت مقتضيات البحث والتحقيق والمتابعة القضائية ذلك.

وقد رتب المشرع الجزائري مسؤولية إدارية وأخرى جزائية على تقاعس مزودي الخدمة عن حفظ المعطيات المذكورة،[2] لإمكانية أن يشكل هذا التقصير عرقلة للسير العادي للتحريات القضائية.

واسترشادا بما ذكر فإن المزودين لخدمة الأنترنت يعتبرون مصدرا لجهات البحث والتحقيق للحصول على الدليل الرقمي من خلال المعطيات التي يكونون ملزمين بحفظها وملزمين في نفس الوقت بوضعها تحت تصرف هذه الجهات التي إذا ما تم طلبها.

---

[1] المادة 11 من القانون(04/09) ".... تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل".

[2] المادة 11 الفقرة الأخيرة"..... يعاقب الشخص الطبيعي بالحبس من 06 أشهر إلى 05 سنوات وبغرامة مالية من 50.000 دج ويعاقب الشخص المعنوي وفقا للقواعد المقررة في قانون العقوبات".

المطلب الثاني: مشروعية الدليل الرقمي.

تعرف المشروعية بأنها التوافق والتقيد بأحكام القانون في إطاره ومضمونه العام، فهي تهدف إلى تقرير ضمانة أساسية وجديرة للأفراد لحماية حريتهم وحقوقهم الشخصية ضد تعسف السلطة، ومن تطاول عليها في غير الحالات التي رخص فيها القانون بذلك، من أجل حماية النظام الاجتماعي وبنفس القدر تحقيق حماية مماثلة للفرد ذاته، لذلك فإن لصحة الإجراءات التي تقوم بها جهة التحقيق أن يكون مبدأ المشروعية من أجل أن تثمر على دليل صحيح وسليم يعوّل عليه القضاء في أحكامه، فلا شك أن مبدأ شرعية الجرائم والعقوبات التي يستقيم عليها بنيان القانون الجنائي الموضوعي ينعكس على قواعد الإثبات الجنائي ويفرض خضوعها هي الأخرى لمبدأ المشروعية، والتي تستلزم عدم قبول أي دليل يكون البحث عنه أو الحصول عليه قد تم بطريقة غير مشروعة، وتهدّ مسألة قبول الدليل الجنائي بصفة عامة الخطوة الأولى التي يتخذها القاضي الجزائي اتجاهه وذلك بعد التنقيب عنه وقبل إخضاعه لتقديره، وقبول الدليل على هذا النحو يتسع ويضيق تبعا للمبادئ التي تقوم عليها أنظمة الإثبات السائدة والحقيقة أن مشروعية الدليل الرقمي هي مشروعية وجود ومشروعية حصول.

الفرع الأول: مشروعية وجود الدليل الرقمي:

ويقصد بمشروعية وجود الدليل الرقمي أن يعترف المشرع بهذا الدليل من خلال تصنيفه في قائمة الأدلة القانونية التي يجيز القانون فيها للقاضي الاستناد إليه في تكوين عقيدته، ولعل المعيار الذي يتحدد على أساسه موقف القوانين فيما يتعلق بسلطة القاضي الجزائي في قبول الدليل الرقمي يتمثّل في طبيعة نظام الإثبات السائد في الدولة إذ تختلف النظم القانونية في موقفها من حيث الأدلة التي يمكن قبولها في الإثبات.

الفرع الثاني: موقف المشرع الجزائري من الدّليل الرقمي:

لقد عرفت التشريعات الإجرائية الجزائية نظامين رئيسيين للإثبات هما:

- نظام الإثبات المقيد وفيه يقوم المشرع بتحديد أدلة الإثبات وكذا قوة الإثباتية لكل دليل من الأدلة بناء على قناعة المشرع بها وهو ما يعرف بنظام الأدلة القانونية.
- نظام الإثبات الحر والذي يقوم على أساس حرية الإثبات فلا يقوم المشرع بتحديد الأدلة بل يكون للقاضي دور إيجابي في البحث عن الأدلة و تقدير قوتها الثبوتية حسب قناعته بها، فلا يلزمه القانون بأدلة للاستناد إليها في تكوين قناعته فله أن يبني هذه القاعدة على أي دليل.

وفي هذا الصدد فإن المشرع الجزائري وكغيره من التشريعات المنتمية إلى النظام الحر لا نجده قد أفرد نصوص خاصّة تحظر على القاضي مقدما قبول أو عدم قبول أي دليل بما في ذلك الدليل الرقمي وهو أمر منطقي طالما أن المشرع الجزائري يستند لمبدأ حرية الإثبات، حيث يتضمن القانون04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ومنها أن الأصل في الأدلة مشروعية وجودها ومن ثم فإن الدليل الرقمي سيكون مشروعا من حيث الوجود ومن جهة أخرى فإنه وطبقا لمبدأ الشرعية الإجرائية فلا يكون الدليل مقبولا في عملية الإثبات إلا إذا كان مشروعا لأن القاضي لا يقدر إلا الدليل المقبول و لا يكون كذلك إلا إذا كان مشروعا.

الفرع الثالث: مشروعية الحصول على الدليل الرقمي:

لأنه من الضروري أن يتم رسم ضوابط وأطر معينة يتعين أن تمارس في نطاقها عملية البحث عن الأدلة وتحصيلها والتحقق فيها بحيث لا تنحرف عن الغرض الذي يبتغيه المشرع

من ورائها وهو الحصول على إلى لحقيقة الفعلية في الدعوى فهي الهدف الاسمي لقانون الإجراءات الجزائية.

فإنه من المقرر أن الإدانة في أي جريمة لا بد أن تكون مبنية على أدلة مشروعة تم الحصول عليها وفق قواعد الأخلاق واحترام القانون من طرف الجهة المختصة بجمع الدليل الجزائي بما يتضمنه من أدلة مستخرجة من وسائل الكترونية، ولا يكون مشروعا إلا إذا أجرى التنقيب عنه أو الحصول عليه أو كانت عملية تقديمه إلى القضاء أو إقامته أمامه بالطرق التي رسمها القانون، فمتى ما تم الحصول على الدليل خارج هذه القواعد القانونية فلا يعتدّ بقيمته مهما كانت دلالته الحقيقية وذلك لعدم مشروعية وعلى هذا الأساس فإن إجراءات جمع الأدلة الرقمية المتحصلة من الوسائل الالكترونية إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون باطلة و بالتالي بطلان الدّليل المستمد منها ولا تصلح لأن تكون أدلة تبنى عليها الإدانة في المواد الجنائية.

وفي إطار مشروعية الأدلة الرقمية نجد أن قانون الإجراءات الجنائية الفرنسي رغم أنه يتضمن نصوص تتعلق بمبدأ الأمانة والنزاهة في البحث عن الحقيقة إلا أن الفقه والقضاء كانا بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليدية أم في مجال التنقيب في الجرائم المعلوماتية، ويشير الرأي الفقهي الفرنسي إلى أن القضاء قبل استخدام الوسائل العلمية الحديثة في عملية البحث والتحري عن الجرائم تحت تحفّظ أو ن يتمّ الحصول على الأدلة الجنائية ومن بينها الأدلة الرقمية بطريقة شرعية و نزيهة،[1] وقد قضي في هولندا أنه إذا كانت بيانات الحاسوب المسجلة في ملفات الشرطة غير قانونية فذلك يؤدي إلى نتيجة مؤداها ضرورة محو هذه البيانات وعدم إمكانية استخدامها كدليل جنائي بسبب مبدأ استبعاد الأدلة القانونية.

[1] علي محمد حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والأنترنت، عالم الكتب الحديثة، الأردن، ص186.

ولقد وضعت الدساتير والقوانين الإجرائية نصوص تضمن لضوابط لشرعية الإجراءات الماسة بالحرية، ومن ثم مخالفة هذه النصوص في استخلاص الدّليل يصبح دليلا بالمشروعية والقول وبذلك يهدر قيمته، فمشروعية الدليل تتطلب صفة في مضمونه و أن يكون هذا المضمون قد تم الحصول عليه بطرق مشروع تدل على الأمانة والنّزاهة من حيث طرق الحصول عليه، والحقيقة أن مشروعية الدليل تعد قيدا وخطا فاصلا بين حق الدولة في توقيع العقاب لضمان أمن واستقرار المجتمع من جهة وبين ضمان حقوق الأفراد وحرياتهم من جهة أخرى.

المطلب الثالث: موقف المشرع الجزائري من الدليل الرقمي في مجال الإثبات الجزائي.

إن الإثبات في المواد الجنائية هو النتيجة التي تتحقق باستعمال وسائله وطرقه المختلفة للوصول إلى الدليل الذي يستعين به القاضي لاستخلاص حقيقة الوقائع المعروضة عليه وإعمال حكم القانون عليها، ويعني ذلك أن موضوع الإثبات هو الوقائع وليس القانون.[1]

وبالتالي فإن الإثبات الجزائي هو كل ما يؤدي إلى كشف غموض الجريمة وإقامة الدليل على وقوعها والتأكد من أن المتهم هو مرتكب الجريمة بالفعل ووجود الدليل على ذلك، ويعتبر الدليل الوسيلة القانونية التي يستعين بها القاضي للوصول إلى الحقيقة وكشف غموض الجريمة ونسبتها إلى المتهم، ولقد ذهب الفقه الإجرائي إلى وضع نظامين إجرائيين في مجال الإثبات الجزائي يختلفان فيما بينهما من حيث الأسس التي يقوم عليها كل واحد منهما وهذه الأنظمة هي:

[1] أشرف عبد القادر قنديل، النظرية العامة للبحث الجنائي وأثرها في عقيدة القاضي، المرجع السابق، ص212.

نظام الإثبات القانوني أو المقيد وفيه يحدد القانون الأدلّة التي يجوز الأخذ بها والاستناد عليها والثاني هو نظام الإثبات الحر وفيه لا يقيد القانون القاضي بأدلة معينة في إثبات الواقعة وله أن يقتنع بأي دليل يعرض عليه.

فأي من هذين النظامين أخذ به المشرع الجزائري وما أثر ذلك على مسألة الإثبات بالدليل الرّقمي في الجريمة المعلوماتيّة.

الفرع الأول: أنظمة الإثبات الجنائي: يوجد في مجال الإثبات الجزائي نظامان:

1. نظام الإثبات المقيد أو نظام الأدلة القانونية: Système de la preuve légale مفاد هذا النظام هو أن يتقيد القاضي في حكمه سواء بالإدانة أو البراءة بأنواع معينة من الأدلة طبقا لما يرسمه التشريع، فالفكرة الأساسية لهذا النظام تقوم على أن المشرع هو الذي يكون له الدور الأساسي في الإثبات، وذلك من خلال التحديد المسبق للأدلة المقدمة في الدعوى والتي يستند إليها القاضي الجزائي في حكمه ولا سبيل له إلى الاستناد إلى أي دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات.

وفي هذا النظام لا يكون للقاضي الجزائي دور في القيمة الإقناعية للدليل فيتقيد القاضي وفق هذا النظام بالأدلة التي رسمها المشرع سلفا دون أن يعمل فيها ميوله أو اقتناعه الشخصي بشأنها، إذ يقوم اقتناع المشرع مقام اقتناع القاضي وعليه فإن اليقين القانوني يقوم أساسا على افتراض صحة الدليل بغض النظر عن حقيقة الواقع و اختلاف ظروف الدعوى، ويتجلى دور القاضي في هذا النظام كمطبق فحسب من حيث مراعاة توفر الدليل وشروطه، بحيث إذا لم تتوافر هذه الشروط وتلك الآليات التي يتطلبها القانون في الدليل فإن القاضي لا يستطيع أن يحكم بالإدانة حتى ولو كان اقتناعه يقينا بارتكاب المتهم للجريمة المسندة إليه.

ويقوم هذا النظام على مجموعة من الخصائص أهمها أن دور القاضي الجزائي سلبي، ذلك أن الإثبات الجنائي في هذا النظام يخضع لقواعد شكليه تتضح في سلطة القاضي المقيدة في تقدير عناصر الإثبات التي يستمد منها إقناعه وتقدير قيمة الأدلة المعروضة عليه، كما يتميز أيضا هذا النظام بالدور الإيجابي للمشروع في عملية الإثبات من حيث أنه هو الذي ينظم قبول الأدلة سواء عن طريق تعيين الأدلة المقبولة للحكم بالإدانة، أو باستبعاد أدلة أخرى أو بإخضاع كل دليل لشروط معينة، وأنه هو الذي يحدد القيمة الإقناعية لكل دليل بأن يعطي لبعض الأدلة الحجية الأقوى دون الأدلة الأخرى.

وقد أعاب الفقه الجنائي على هذا النظام أنه أخرج القاضي من وظيفته الطبيعية التي تتمثل في فحصه للدليل وتقديره، ومن ثم تكوين اقتناعه الشخصي وأقحم المشرع في وظيفة القاضي وإملاء أدلة الإدانة عليه على سبيل الحصر.

ومن العيوب التي واجهها هذا النظام أيضا أنه قام بتقنين اليقين في نصوص قانونية محدّدة سلفا رغم أنّ اليقين مسألة يطرحها الواقع و يقدّرها القاضي.

2. نظام الإثبات الحر أو نظام الاقتناع الشخصي للقاضي الجزائي:

وفقا لهذا النظام لا يرسم القانون طرقا محددة للإثبات، إذ يتمتع القاضي الجزائي في هذا النظام بحرية مطلقة في تكوين اعتقاده من أي دليل يطرح أمامه،[1] ومن ثمة فإن هذا النظام يقوم على خاصيتين أساسيتين:

- الخاصية الأولى تتمثل في إطلاق حرية الإثبات للقاضي الجزائي انطلاقا من موضوع الإثبات في المسائل الجزائية الذي يتعلق بوقائع مادية ونفسية لا يصلح لإثباتها تحديد

[1] محمد عبد الغريب، حرية القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام، المرجع السابق، ص08.

مجموعة من القواعد الإثباتية مسبقا، بل إن الإثبات في هذه المسائل يكون بكافة طرق الإثبات.

- أما الخاصية الثانية فتتمثل في حرية القاضي الجزائي في الاقتناع بالدليل المطروح عليه في جلسة المحاكمة دون أن يكون عليه أي رقيب سوى ضميره ودون أن يكون مطالبا ببيان سبب اقتناعه بدليل آخر.

وعلى هذا الأساس يكون للقاضي الجزائي دور فعال حيال الدليل الذي يوضع أمامه، وله في مقابل ذلك كافة الصلاحيات التي تمكنه من اتخاذ الإجراء الذي يراه مناسبا ويخدم لإظهار الحقيقة.

وعقيدة القاضي هي نتاج وزن الأدلة المطروحة بالدعوى الجزائية أمامه، والذي يقوم بقبول الأدلة التي قدمها أطراف الدعوى فلا يوجد حظر على الأدلة إلا إذا كانت غير مشروعة، وقد ذهب البعض،[1] إلى القول أن الاقتناع الشخصي للقاضي الجزائي هو الضمانة الحقيقية لضبط ميزان العدالة.

الفرع الثاني: موقف المشرع الجزائي الجزائري من أنظمة الإثبات وأثر ذلك في إثبات الجريمة المعلوماتية.

نصت المادة 212 من قانون الإجراءات الجزائية على أنه يجوز إثبات الجرائم بأي طريق من طرق الإثبات وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص...." كما نصت المادّة 307 من قانون الإجراءات الجزائية أيضا أن القانون لا يطلب من القضاة أن يقدّموا حسابا عن الوسائل التي قد وصلوا بها إلى تكوين اقتناعهم وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة للمتهم....".

[1] أشرف عبد القادر قنديل، المرجع السابق، ص213.

ومن خلال هذين النصين القانونيين يتضح جليا أن المشرع الجزائري قد تبنى كقاعدة عامة نظام الاقتناع الشخصي للقاضي الجزائي، إلا واستثناء نجده أخذ أيضا بنظام الأدلة القانونية في إثبات بعض الجرائم أين يشترط لإثباتها أدلة قانونية محددة مسبقا وعلى سبيل الحصر.[1]

وبتحليل المادة 212 من قانون الإجراءات الجزائية نجدها تكرس قاعدتين تكمل إحداهما الأخرى، قاعدة الاقتناع الحر للقاضي الجزائي من جهة وقاعدة حرية اختيار وسائل الإثبات الجزائي من جهة أخرى.

وإذا كان الدليل الرقمي ذو الأصالة العالمية هو الأوفر والأنسب في إثبات الجريمة المعلوماتية فما مدى إمكانية إعمال القاضي الجزائي لمبدأ الاقتناع الشخصي حيال هذا الدليل.

1. **تعريف مبدأ الاقتناع الشخصي:** يعرف فقهاء القانون الجزائي الاقتناع بأنه حالة ذهنية ذاتية تستنتج من الوقائع المعروضة على بساط البحث، أو بمعنى آخر هو حالة ذهنية ذو خاصية ذاتية نتيجة تفاعل ضمير القاضي وأدلة الإثبات المطروحة والتي يثيرها الخصوم إما لإثبات أو إنكار اتهام،[2] ومن خلال هذا التعريف فغن الاقتناع الشخصي للقاضي الجزائي يتميز بخاصيتين هما:

- **الخاصية الأولى** تتمثل في أنه حالة ذهنية مبنية على الاحتمال وأن العبرة ليست بكثرة الأدلة وإنما بما تتركه من أقر في نفسية القاضي، لأن هذا التأثير سيلعب دورا في تحديد مصير الدعوى الجزائية بالإدانة أو البراءة.

[1] انظر المادتين 341-339 من قانون العقوبات الجزائري.

[2] نصر الدين ماروك، النظرية العامة فلإثبات الجنائي، الجزء الأول، ص620.

ولكنها ترجع إلى ا؟لإثبات في المسائل الجزائي والوصول إلى الدليل مسألة جد صعبة وذلك لاختلاف أساليب ارتكاب الجريمة وأن المجرم عادة ما يسعى إلى إخفاء جريمته، لذلك فالبحث عن الحقيقة من خلال الأدلة الجزائية لا يكون إلا عن طريق منح القاضي الجزائي هامشا عن الحرية لمناقشة الدليل الذي يراه مناسبا في إثبات الجريمة.

2. وسائل تكوين الاقتناع الشخصي للقاضي الجزائي:

إن الجهد الاستنباطي الذي يبذله القاضي من خلال نشاطه العقلي المكون لناعته و الذي ينصرف إلى فرز الحقيقة من الدليل مجل تقديره يرتكز فيه القاضي على:

- قبوله جميع الأدلة المطروح أمامه في الجلسة ولا حضر على القاضي أو يفرض عليه دلي محدد ولا يتقيد إلا قيد مشروعية الدليل و أنه قد تم طرحه للمناقشة بالجلسة.
- أن يقوم القاضي بوزن كل دليل على حدى عن باقي الأدلة المطروحة أمامه وله أن يهدر أي دليل مهما كانت قيمته طالما أنه لم يطمئن إليه.
- سلطة القاضي في تنسيق الأدلة المطروحة أمامه ومساندة الأدلة لبعضها أو ما يعرف بتساند الأدلة.

الفرع الثالث: سلطة القاضي الجزائي في تقدير الدليل الرقمي:

إن الأصالة العلمية للدليل الرقمي جعلت من سلطة القاضي في تقدير هذا الدليل محل خلاف فقهي، إذا أن هناك من يرى أن الدليل العلمي ومنه الدليل الرقمي له قوته الثبوتية حتى للقاضي، مستندين في رأيهم إلى أن هذا الدليل يتسم بالدقة العلمية التي يبلغ معها إلى درجة اليقين، وهناك من يرى أم مبدأ حرية القاضي في الاقتناع يجب أن يبسط سلطاته على كل الأدلة دون استثناء حتى على الدليل الرقمي معتبرين أن الدليل الرقمي قوة ثبوتية لا يستطيع القاضي مناقشتها أو تقديرها يعد بمثابة رجوع إلى مذهب الإثبات القانوني(المقيد).

والمشرع الجزائري كما سبق بيانه أجاز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الجرائم التي قد يتطلب إثباتها دليلا معينا، ومنح القاضي الجزائي سلطة تقدير الدليل والحرية في تكوين اقتناعه من أي دليل يطمئن إليه، فهل تنصرف هذه السلطة التقديرية التي يتمتع بها القاضي الجزائي إلى الدليل الرقمي المستخرج من الوسائل الالكترونية؟

لقد سبق الذكر أن الجريمة المعلوماتية في القانون الجزائري تشمل الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وكذا كل جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الالكترونية، وهذه الأخيرة قد تنصرف إلى جرائم تقليدية منصوص عليها في قانون العقوبات يمكن حسب طبيعتها أن ترتكب بواسطة معلوماتية.

وهذا يعني أن الإجرام المعلوماتي قد يأخذ وصف الجناية أو الجنحة أو المخالفة حسب وصف الجرم المرتكب بواسطة المنظومة المعلوماتية، وإن كان مبدأ الاقتناع القضائي عام النطاق لدى كافة أنواع المحاكم الجزائية سواء كانت محاكم الجنايات أو الجنح أو المخالفات.[1] فإن قواعد بيان العناصر تقدير الدليل تختلف حسب اختلاف وصف الفعل للمجرم، فإذا كان الفعل من طبية جنائية فإن محكمة الجنايات تتمتع بسلطة تقديرية مطلقة في مواجهة الأدلة المعروضة أمامها وتصدر أحكامها دون أن يكون قضاتها مطالبين بتسبيب أحكامهم ولا رقابة لجهات الطعن عليهم، أما إذا أخذ الفعل للمجرم وصف الجنحة فإن قاضي الجنح مطالب بعرض وبيان تقديره للدليل المعروض عليه من خلال تسبيب حكمه، والذي يكون محل رقابة من جهة الطعن،[2] لهذا فهو مطالب باحترام القواعد العامة المنظمة للقوة الثبوتية لكل وسيلة من وسائل الإثبات والتي قد تأخذ شكل محاضر معدو بمناسبة تفتيش أي اعتراض مراسلات أو

[1] وإن كان المشرع الجزائري لم يحدد ذلك صراحة في المواد المقررة لهذا المبدأ راجع المواد212.307 من قانون الإجراءات الجزائية بخلاف المشرع الفرنسي فقد صرح ذلك صراحة حيث خصص المادة(1-353) من ق.إ.ج لتطبيق المبدأ أمام محكمة الجنايات كما نصت المادة (427) من ذات القانون على تطبيق هذا المبدأ بالنسبة لمحاكم الجنح.

[2] انظر المادة 379 من ق إ ج ج والتي تقابلها المادتين 485-593 من ق إ ج فرنسي.

شكل تقرير خبرة محررة بمناسبة معاينة وفحص الأدلة المضبوطة من جهاز الإعلام الآلي أو دعامات الكترونية.

فأما ما يتعلق بالمحاضر فإن الشرع اعتبر أنها قاعدة عامة مجرد استدلالات ما لم ينص القانون على خلاف ذلك، ولا يكون للمحضر أي قوة إثبات إلا إذا كان صحيحا من حيث الشكل، وأنه قد تم إعداده من طرف واضعة أثناء مباشرة أعمال وظيفته، ويكون مضمونه ما يدخل في اختصاصه،[1] إلا أن المحاضر التي يخول القانون لضباط الشرطة القضائية إعدادها بنص خاص لإثبات جنح معينة فإن هذه المحاضر تكون لها حجتها ما لم يدحضها دليل عكسي.[2]

أما بالنسبة لتقارير الخبرة فإن المحكمة العليا ذهبت للقول أن الخبرة شأنها شأن باقي أدلة الإثبات تخضع للسلطة التقديرية لقاضي الموضوع،[3] وهذا المعنى تؤكده المادة 215 من: ق إ ج التي تنص على أنه:" لا تعتبر التقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات....".

لكن الطبيعة العلمية والتقنية للجريمة المعلوماتية غالبا ما تفرض على القاضي الاستناد في تكوين اقتناعه على الخيرة الفنية والتقيد بالنتيجة المتوصل إليها الخبير في تقرير خبرته ولا يمكنه طرحها واستبعادها إذا قدر أن ما تحمله من أدلة لا يتوافق مع ظروف وملابسات الواقعة أو تتناقض مع الحقيقة العلمية، فحسب الاجتهاد القضائي أنه أحيانا ما تكون الخبرة وحدها كافية بالنسبة للقاضي عندما يكون مطالبا للفصل في وقائع ذات طابع تقني دون أن يحتاج إلى مناقشتها.[4]

---

[1] انظر المادة 214 من ق إ ج.

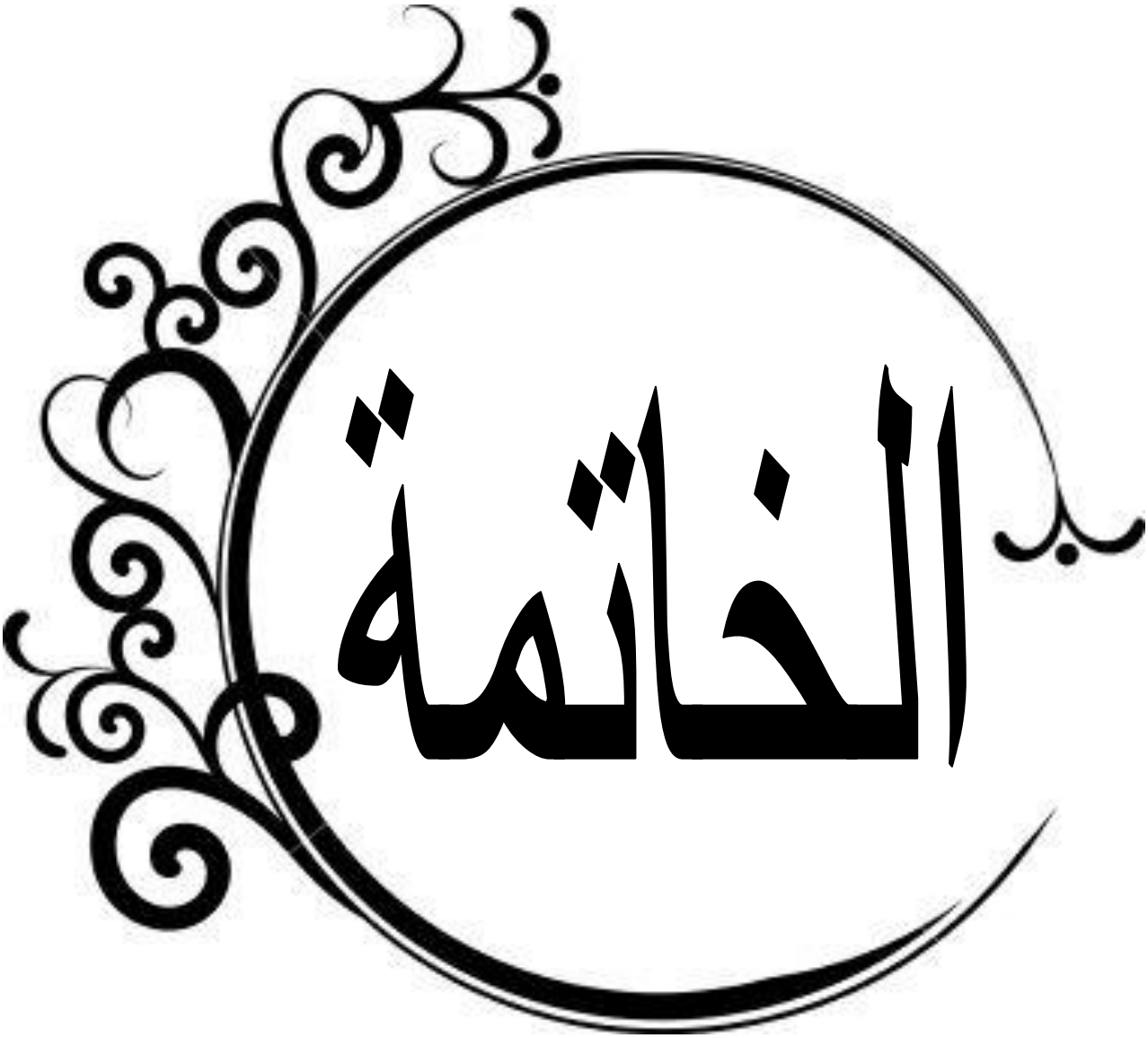
[2] انظر المادة 216 من ق إ ج.

[3] ورد في مضمون قرار المحكمة العليا المؤرخ في 1995/07/11 المنشور في نشرة القضاء رقم 58 لسنة 2006، ص170.

[4] قرار المحكمة العليا الغرفة الجنائية المؤرخ في 2002/06/04، نشرة القضاء رقم 58 لسنة 2006، ص255.

وفي الأخير يمكن القول أن إساءة استخدام التقنية المعلوماتية تعد منم الموضوعات التي فرضت نفسها على المستوى الوطني والدولي على حد سواء وأجبرت التشريع الجزائي على التدخل من أجل مواجهتها بتشريعات حاسمة لمكافحتها ومعاقبة مرتكبها إلا أن ذلك يبدو غير كاف لتحقيق هذه الهدف، فعلى المستوى الإجرائي تثير الجريمة المعلوماتية مشكلات عدة بدءا من مرحلة الاستدلال حتى صدور الحكم الجزائي لاسيما فيما يتعلق بإثبات الجريمة المعلوماتية ومدى صلاحية الدليل لرقمي للإثبات ومدى شرعية الأدلة المحصل عليها عبر التقنية المعلوماتية وحجيتها أمام القاضي الجزائي، لذلك خصص هذا الفصل لتناول هذه المسائل من خلال تحديد الأجهزة المكلفة بالبحث والتحري عن الجريمة المعلوماتية، ثم التعريف الخصائص التي يتميز بها التحقيق والمحققون فيها.

ثم بعد ذلك تم البحث في الدليل المناسب لإثبات هذا النوع من الجرائم وهو ما يعرف بالدليل الرقمي أين تم توضيح مفهومه وتحديد أشكاله ومصادر الحصول عليه، كما تم معالجة القواعد الإجرائية المستعملة في التحقيق من أجل استخلاصه وما هي الصعوبات والمعوقات التي تواجه القائمين على ذلك، كما تم التناول في هذا الفصل مسألة ضمانات المشتبه فيه أثناء ممارسة إجراءات الحصول على الدليل الرقمي وأثرها على الحق في الخصوصية، وأخيرا تم بحث القيمة القانونية للدليل الرقمي في مجال الإثبات الجزائي وما هو موقف المشرع الجزائري من هذا الدليل.


الخاتمة

إن مفهوم الجرائم المعلوماتية ينصرف إلى الأفعال التي تشكل اعتداء على نظم المعالجة الآلية للمعطيات، والتي تستهدف بشكل خاص للمعلومات المختلفة في البيئة الرقمية، بالإضافة إلى كل جريمة ترتكب أن يسهل ارتكابها بواسطة منظومة معلوماتية، وهذه الأخيرة في الغالب ما تكون جرائم تقليدية.

ومن أهم مميزات جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، أنها تنصب على محل من نوع خاص يختلف تماما على محل الجرائم التقليدية، فهذه الجرائم تستهدف المساس بالمعلومات الالكترونية المتواجدة في البيئة الرقمية على هيئة إشارات ونبضات غير مرئية تنساب عبر أجزاء النظام المعلوماتي وشبكات الاتصال العالمية.

وقد تبين لي أنه ونظرا لكون النصوص الجزائية العقابية إنما وضعت للتعامل مع جرائم تنصب على محل مادي ملموس، فإن الأمر قد تبعه قصور أو عجز هذه النصوص القانونية عن توفير الحماية الجزائية لمثل محل الجرائم المعلوماتية فكان ذلك من دواعي تدخل المشرع إلى إصدار نصوص جزائية تجرم بحق الأفعال التي تشكل اعتداء على نظم المعالجة الآلية للمعطيات وهو ما يقتضيه مبدأ الشرعية الموضوعية القائم على التفسير الضيق للنصوص القانونية العقابية وعدم جواز القياس.

وقد توصلت أيضا إلى أن هذا القصور لم يعتر النصوص الموضوعية فقط ولم يقف عند الشق الموضوعي للقانون الجزائي، بل امتد تأثير التقنية المعلوماتية إلى الشق الإجرائي للقانون الجزائي، فقد أثارت هذه التقنية الحديثة العديد من الإشكالات في نطاقها، ذلك أن نصوص قانون الإجراءات الجزائية إنما وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها مع خضوعها لمبدأ حرية القاضي الجزائي في الاقتناع.

لذلك فإن من الطبيعة الخاصة للجريمة المعلوماتية دعت المشرع إلى إعادة تقييم بعض القواعد الإجرائية المتاحة في استخلاص الدليل كالتفتيش والضبط وجعلها صائغة الاستعمال في مجال البيئة الرقمية ظن وهو ما كان فعلا بموجب القانون04/06 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فضلا عن استحداث نوع من قواعد إجرائية أخرى تتلاءم مع الطبيعة الرقمية التي يكون الدليل المناسب في إثبات هذا النوع من الجرائم كاعتراض المراسلات ومراقبة الالكترونية

وقد تبين معنا كذلك أن الدليل المناسب والأوفر في إثبات الجريمة المعلوماتية هو الدليل الرقمي والذي هو عبارة عن معلومات مخزنة في النظم المعلوماتية في شكل نبضات مغناطيسية أو كهربائية من الممكن من الناحية التقنية استخلاصه من البيئة الرقمية التي تواجد بها، وتجميعه لاستخدام برامج وتطبيقات تقنية، ليظهر بعد ذلك في شكل مخرجات الكترونية أو حتى ورقية بعد طبعه

كما أظهر البحث أيضا أن عملية استخلاص الدليل الرقمي سواء بطرق الإجرائية التقليدية أو المستحدثة ليس من السهولة بما كان، إذ تعوقها في غالب الأحيان صعوبات تتعلق إما بالطبيعة التكوينية للدليل الرقمي أو بالعامل البشري

إن الدليل الرقمي على ضوء ما أسفرت عليه التطورات التقنية في مجال المعلوماتية لا يغني عنه أن يكون مشروعا، وذلك بأن يتم الحصول عليه بالطرق القانونية وأن يقدم للمحكمة على نفس الهيئة التي تم جمعه عليها، لأن لا يطرأ عليه أي تغيير أو تحريف خلال فترة حفظه.

إن الأدلة الرقمية وإن كانت تتمتع بقيمة علمية قاطعة في الدلالة على الحقائق التي تتضمنها، إلا أن الكشف عن الهوية الحقيقية للفاعل ليس بالمر السهل، فقد يمكن التعرف على هوية الحاسوب المستعمل في ارتكاب الجريمة والمرتبط بشبكة الأنترنت من خلال عنوان .....

ip لأنه من الصعب تحديد هوية الفاعل ما لم يتم تدعيم هذا الدليل الرقمي بالأدلة التقليدية الأخرى فيما بعد.

وقد لاحظت من خلال البحث حول مسألة تقدير القيمة القانونية للدليل الرقمي أنه يجب التمييز بين أمرين: الأول القيمة العلمية القاطعة للدليل الرقمي والثاني الظروف والملابسات التي تحيط بهذا الدليل، فالقاضي ليس له أن ينازع فيما أسفرت عليه التكنولوجيا والمعلوماتية والعلوم التقنية من الناحية العلمية وإنما له أن يقدر الظروف والملابسات التي أحاطت بهذا الدليل، وله في ذلك أن يرفض هذا الدليل إذا لم يقتنع بظروف القضية وملابساتها.

وهذا ما قدرني إلى الوصول إلى نتيجة أخرى مؤداها تمتع القاضي الجزائي بدور إيجابي من حيث تقدير القيمة القانونية للدليل الرقمي وخضوعه للسلطة التقديرية.

كما تبين أن الاتصالات الالكترونية والنظم المعلوماتية تعتبر أحد أوجه الحياة الخاصة للإنسان ومظهرا من مظاهر خصوصيته، وبالتالي فإن إجراءات استخلاص الدليل في البيئة الرقمية قد تؤدي إلى المساس بهذه الخصوصية وإمكانية اطلاع المحققين على أسرار خاصة بأشخاص قد لا يكون لهم أصلا يد في الجريمة، مما جعل المشرع يحرص كل الحرص على هذه المسألة بأن اشترط اللجوء إلى هذه الإجراءات إذا دعت إلى ذلك ضرورة التحري والتحقيق والتي يجب أن تقدر بقدرها.

وفي الأخير فإنه وعلى ما توصلت إليه في هذا البحث فإنه قد بدا لي أن أقدم جملة من المقترحات آملة أن أكون موفقة في طرحها:

- إن الجزائر وهي تخطوا الخطوات الأولى في تطبيق مشروع الحكومة الالكترونية والذي من خلاله يتم السعي إلى استخدام تقنية المعلومات والاتصالات الالكترونية في توفير وتقديم معلومات وخدمات الحكومة للمواطنين وجعلها متاحة للجمهور، فهذا المشروع لا بد أن تتبعه خطوة تشريعية هامة يكون الهدف منها توفير الحماية القانونية الشاملة لهذا

المفهوم بصورة منسجمة ومتزامنة مع هذا التحول من أجل تخطي الثغرات القانونية التي قد يستفيد منها العابثون بأمن المعلومات، لاسيما وأن الأمر يتعلق بأنظمة معلوماتية تخص إدارة الدولة.

- وحسب مفهوم المادة 44 من ق إ ج الفقرة الثانية المدرجة بموجب القانون06/22 المؤرخ في 2006/12/20 فإنه لا يجوز لضباط الشرطة القضائية في إطار التحري والتحقيق عن الجرائم الماسة بأنظمة المعالجة للمعطيات الانتقال إلى مساكن أشخاص الذين يظهرون أنهم ساهموا في ارتكاب هذه الجريمة لإجراء التفتيش هناك إلا بإذن مكتوب من الجهة المختصة، مع وجود استظهار هذا الإذن قبل الدخول إلى المسكن والشروع في عملية التفتيش، وعليه فالإذن في هذه المادة يتعلق حصرا بتفتيش المساكن، لكن المشرع في القانون04/09 أجاز في إطار التحري والتحقيق في الجريمة المعلوماتية تفتيش محل آخر غير السكن وهو المنظومة المعلوماتية دون أن يشترط للدخول إليها ضرورة الحصول على إذن من الجهة القضائية المختصة، فحصول ضابط الشرطة القضائية على إذن يسمح له بالدخول إلى الأماكن التي تتواجد بها الحواسيب لا ينصرف في رأيي إلى الإذن بدخول المنظومة المعلوماتية لهذه الحواسيب وتفتيشها لاختلاف محل التفتيش أصلا.
- سبق أن مر بنا أم من بين الصعوبات في تحديد هوية المجرم المعلوماتي هو استعمال هذا الأخير لحواسيب غير شخصية في تنفيذ جريمته وغالبا ما يكون في مقاهي الأنترنت، هذه الأخيرة التي يرتادها عدد كبير من الزبائن لا يمكن معرفة هوياتها، لذلك أقترح على المشرع إعادة النظر في تسيير هذه المقاهي وعدم اعتبارها مجرد نشاط تجاري كغيره من الأنشطة التجارية الأخرى، بل لا بد من فرض أعباء والتزامات على مقدمي هذه الخدمة ومسيري مقاهي الأنترنت، كأن يطلب من أي زبون قبل شروعه في استخدام الأنترنت ملء استمارة تحدد فيها كامل هويته والتوقيت الذي استعمل فيه شبكة الأنترنت ورقم جهاز الحاسوب الذي استعمله، كما يلتزم مسير المقهى بالاحتفاظ بعناوين

المواقع التي تم زيارتها في ذاكرة كل حاسوب لمدة معينة، ونفش الشيء بالنسبة لاستعمال شبكات الأنترنت الموجودة في المؤسسات العامة كالجامعات و غيرها.

- وأخيرا أرجوا أن أكون قد وفقت في معالجة هذا الموضوع، وإن لم أوفق فعذري أنني اجتهدت و لكل مجتهد نصيب.


قائمة
المصادر والمراجع

القرآن الكريم.

الكتب:

1. أشرف عبد القادر قنديل، النظرية العامة للبحث الجنائي وأثرها في عقيدة القاضي، المرجع السابق، ص212.
2. جميل عبد الباقي الصغير، الانترنت القانون الجنائي، دار النهضة العربية، القاهرة، 2002، ص164.
3. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت.
4. جميل عبد الباقي الصغير، المرجع السابق، ص119، د. عبد القتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، دار الكتب القانونية المجلة الكبرى، ط1، ص84، وكذلك د. محمد الأمين الشبري.
5. جميل عبد الباقي، الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية القاهرة، 2002، .
6. خالد عباد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة، 200.
7. خالد ممدوح إبراهيم، الجرائم المعلوماتية، الدار الفكر الجامعي، الطبعة الأولى، ص88.
8. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الطبعة الأولى 2009،
9. زهير كاظم عبود، بحث مقدم للأكاديمية العربية المفتوحة في الدنمارك، كلية القانون والسياسة قسم القانون للدراسات العليا 2007 بدون ترقيم.
10. سيناء عبد الله محسن، المواجهة التشرعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية.

11. عبد الحميد عبد المطلب استخدم بروتوكول TCP/IP TD FPE فيبحث وتحقيق الجرائم مع الكمبيوتر.
12. عبد الله حسين محمود، إجراءات جمع الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الالكترونية، دبي، 2003.
13. علي محمد حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والأنترنت، عالم الكتب الحديثة، الأردن.
14. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 2004.
15. غنام محمد غنام، الحماية الجنائية لبطاقات الائتمان الممغنطة، مؤتمر الجوانب القانونية والأمنية للعمليات الالكترونية، دبي 2003.
16. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت بكلية الشريعة والقانون، جامعة الإمارات العربية المتحدة الفترة من01 إلى03 ماي 2000.
17. محمد أمين الشوابكة، جرائم الحاسوب والانترنت(الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع الطبعة الأولى، 2009.
18. محمد أمين الشوابكة، جرائم الحاسوب والانترنيت (الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2009.
19. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994،. ص06.
20. محمد عبد الغريب، حرية القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام.
21. محمد علي العريان، الجرائم المعلوماتية. دار الجامعة الجديدة للنشر، 2004.
22. محمد نصير السرحاني، مهارات التحقيق الفني في الحاسوب والأنترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

23. مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، 2001.

24. مصطفي محمد موسى، التحقيق في الجرائم الالكترونية، مطابع الشرطة، ط1.

25. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، الطبعة الأولى، 2005.

26. نبيلة هبة محمد هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات للطبقة الأولى، دار الفكر الجامعي، الإسكندرية، 2007.

27. نصر الدين ماروك، النظرية العامة فلإثبات الجنائي، الجزء الأول.

28. نهلا عبد القادر المومني، الجريمة المعلوماتية، الطبعة الثانية، 2010، دار الثقافة للنشر والتوزيع.

29. هشام رستم، الحواسب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، 2000.

30. هشام محمد فريد رستم، الجرائم المعلوماتية بحث مقدم إلى مؤتمر القانون والكمبيوتر والأنترنت،.

31. هلال عبد الإله أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية(دراسة مقارنة) الطبعة الأولى، دار النهضة العربية، 2000.

32. ورد في مضمون قرار المحكمة العليا المؤرخ في 1995/07/11 المنشور في نشرة القضاء رقم 58 لسنة 2006.

33. وضاح محمود الحمود و نشأت مفضي المجالي، جرائم الأنترنت، دار المنار للنشر، عمان، 2005.

القوانين والقرارات:

1. المادة 216 من ق إ ج.

2. المادة 05 الفقرة الأخيرة من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
3. المادة 214 من ق إ ج.
4. المادة 379 من ق إ ج ج والتي تقابلها المادتين 485-593 من ق إ ج فرنسي.
5. المادتين 341-339 من قانون العقوبات الجزائري.
6. المادة 15 من قانون الإجراءات الجزائية
7. المادة 02 من القانون 04/09 عرفت الاتصالات الالكترونية بأنها "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية"
8. المادة 11 الفقرة الأخيرة"..... يعاقب الشخص الطبيعي بالحبس من 06 أشهر إلى 05 سنوات وبغرامة مالية من 50.000 دج ويعاقب الشخص المعنوي وفقا للقواعد المقررة في قانون العقوبات".
9. المادة 11 من القانون(04/09) ".... تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل".
10. المادّة الأولى من هذا القانون عرفت النظام المعلوماتية بأنه نظام الكتروني للتعامل مع المعلومات والبيانات.
11. قرار المحكمة العليا الغرفة الجنائية المؤرخ في 2002/06/04، نشرة القضاء رقم 58 لسنة 2006، ص255.
12. قرار وزير الداخلية المصري رقم13507 لسنة 2002 الصادر بتاريخ: 2002/07/07.
13. القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

المراجع بالفرنسية:

1. Myriam QUEMENER Cyebrctinianalité droit pénal appliqué econonica Septembre 2010.

فهرس الموضوعات

الفهرس

إهداء	
شكر وتقدير	
قائمة المختصرات	
مقدمة	أ
الفصل الأول: الجوانب القانونية للجريمة المعلوماتية	
تمهيد	01
المبحث الأول: ماهية الجريمة المعلوماتية	02
المطلب الأول: تعريف الجريمة المعلوماتية:	03
الفرع الأول: الاتجاه الذي يضيق مفهوم الجريمة المعلوماتية	05
الفرع الثاني: الاتجاه الموسع لمفهوم الجريمة المعلوماتية	07
المطلب الثاني: خصائص الجريمة المرتكبة على الانترنت	09
المطلب الثالث: موقف المشرع الجزائري من الجريمة المعلوماتية	13
المبحث الثاني: الطبيعة القانونية للجريمة المعلوماتية	17
المطلب الأول:أطراف الجريمة المعلوماتية	17
المطلب الثاني: أساليب ودوافع ارتكاب الجريمة المعلوماتية	24
المطلب الثالث: المجني عليه في الجريمة المعلوماتية	31
الفرع الأول: الضحية في الجريمة المعلوماتية	32
الفرع الثاني: مخاطر الجريمة المعلوماتية	36
الفصل الثاني: الجوانب القانونية للتحقيق في الجريمة المعلوماتية	
تمهيد	41
المبحث الأول: التحقيق في الجريمة المعلوماتية	42
المطلب الأول: الأجهزة المكلفة بالبحث والتحري عن الجريمة المعلوماتية	44
المطلب الثاني: خصائص التحقيق والمحقق في الجريمة المعلوماتية	51
المطلب الثالث: الحماية الفنية للمنظومة المعلوماتية	64
الفرع الأول: الحماية الفنية عن طريق البرامج	64

الفهرس

الفرع الثاني: الحماية الفنية عن طريق نظام الرقابة الوقائية عبر الوسائل الالكترونية	67
المبحث الثاني: وسائل الإثبات للجريمة المعلوماتية	70
المطلب الأول: الدليل الرقمي	70
الفرع الأول: خصائص الدليل الرقمي	71
الفرع الثاني: مصادر الحصول على الدليل الرقمي	73
الفرع الثالث: فحص جهاز الحاسوب الخاص بالجاني والمجنى عليه	73
المطلب الثاني: مشروعية الدليل الرقمي	85
الفرع الأول: مشروعية وجود الدليل الرقمي	85
الفرع الثاني: موقف المشرع الجزائري من الدّليل الرقمي	86
الفرع الثالث: مشروعية الحصول على الدليل الرقمي	87
المطلب الثالث: موقف المشرع الجزائري من الدليل الرقمي في مجال الإثبات الجزائي	88
الفرع الأول: أنظمة الإثبات الجنائي	89
الفرع الثاني: موقف المشرع الجزائي الجزائري من أنظمة الإثبات وأثر ذلك في إثبات الجريمة المعلوماتية	91
الفرع الثالث: سلطة القاضي الجزائي في تقدير الدليل الرقمي	93
خاتمة	99
قائمة المصادر والمراجع	114
الفهرس	
الملخص	

ملخص

يتلاءم موضوع هذه الدراسة مع التطورات الحديثة الحاصلة في مجال المعلوماتية التي أصبحت تشكل أداة لارتكاب الجريمة أو مجالا لها وذلك بإساءة استخدامها واستغلالها على نحوز غير مشروع. وقد سعيت من خلالها(هذه الدراسة) إلى توضيح القواعد الإجرائية التي على مداها يمارس العاملون في مجالات البحث والتحري عن الجريمة المعلوماتية عملهم من أجل الحصول على الدليل المناسب لإثبات هذه الجرائم، وقد تناولت في الفصل الأول الجانب النظري للجريمة المعلوماتية من خلال مناقشة الجوانب القانونية لهذه الجريمة وضمن هذا العنوان تم البحث في ماهية الجريمة المعلوماتية من خلال تحديد مفهوم الجريمة المعلوماتية كشرط مفترض لقيامها وتوضيح خصائصها وكذا موقف المشرع الجزائري في الجريمة المعلوماتية ثم تناولنا الطبيعة القانونية الخاصة الذي تميزه هذه الجريمة عن غيرها من الجرائم التقليدية وكذا أطراف المجرم المعلوماتية والتي تنولنا فيها خصائص المجرم المعلوماتي وأصنافه وماهية الأساليب ودوافع المحركة للمجرم المعلوماتي لهذه الجريمة وكذا تعريف المجني عليه كما وضحنا الضحية في الجريمة المعلوماتية ومخاطرها .

وفي الفصل الثاني تم معالجة موضوع إجراءات تحصيل الدليل الرقمي لإثبات الجريمة المعلوماتية وأهم الجوانب القانونية لعملية التحقيق في هذه الجريمة، وهنا تناولت الأجهزة المؤهلة للبحث و التحري عن الجريمة المعلوماتية سواء في النظام القانوني الجزائري أو الأنظمة القانونية المقارنة، كما تم بعد ذلك البحث في الخصائص التي يتميز بها التحقيق والمحقق في الجريمة المعلوماتية، ثم تم تحديد مفهوم الدليل الرقمي من خلال توضيح خصائصه وأنواعه ومصادر الحصول عليه، وبعد ذلك تم التركيز بنوع من الشرح على القواعد الإجرائية المناسبة في عملية استخلاص الدليل الرقمي في بيئته الإلكترونية وتبيان أهم الصعوبات والمعوقات التي تواجهها هذه العملية.

كما تناولت في هذا الفصل أيضا ضمانات المشتبه فيه و أثر إجراءات الحصول على الدليل الرقمي على الحق في الخصوصية وأخيرا تناولت مسألة القيمة القانونية للدليل الرقمي في مجال

الإثبات سواء من حيث مشروعيته أم من حيث حجيته أمام القاضي الجزائي.

وفي الخاتمة تم تبيان أهم النتائج التي تم التوصل إليها ووضع بعض التوصيات والاقتراحات التي من شأنها تفعيل وتنظيم الإجراءات المناسبة للتحقيق في الجرائم المعلوماتية.

والله ولي التوفيق

الكلمات المفتاحية:

الجريمة المعلوماتية- حماية الجزائية للأنظمة المعولماتية- الجرائم المتصلة بالتكنولوجيا- المجرم المعلوماتي- فيروس الحاسب الآلي- الضحية في الجريمة المعولماتية.

Abstract of master's thesis

Summary:

The subject of this study is compatible with recent developments in the field of informatics that have become a tool for committing crime or a field for it by misusing and exploiting it in an illegal way. And I sought through it (this study) to clarify the procedural rules within the scope of which workers in the fields of research and investigation on information crime exercise their work in order to obtain the appropriate evidence to prove these crimes, and I have discussed in the first chapter the theoretical side of information crime by discussing aspects The legal of this crime, and within this title, the essence of the information crime was discussed by defining the concept of the information crime as a presumed condition for its establishment and clarifying its characteristics and the position of the Algerian legislator in the information crime. Then we examined the special legal nature that this crime distinguishes from other traditional crimes and such parties The information criminal, in which we deal with the characteristics and types of the information criminal, and what are the methods and motives for the information criminal of this crime, as well as the definition of the victim, as we explained the victim in the information crime and its risks.

And in the second chapter, the issue of procedures for obtaining the digital guide to prove information crime and the most important legal aspects of the

process of investigating this crime was addressed, and here the qualified agencies to search and investigate information crime both in the Algerian legal system or comparative legal systems were dealt with, as was then the search In the characteristics of the investigation and the investigator in the information crime, then the concept of the digital guide was defined by clarifying its characteristics, types and sources of obtaining it, and after that, a kind of explanation was focused on the appropriate procedural rules in the process of extracting the digital evidence in its electronic environment and Explain the most important difficulties and obstacles facing this process.

The chapter also examined the guarantees of the suspect and the effect of the procedures for obtaining the digital evidence on the right to privacy. Finally, it addressed the issue of the legal value of the digital evidence in the field of evidence, whether in terms of its legitimacy or in terms of its authenticity before the criminal judge.

In the conclusion, the most important results reached were outlined and some recommendations and suggestions were made that would activate and organize appropriate procedures to investigate information crimes.

Keys words:
Information crime - criminal protection of information systems - technology-related crimes - information criminal - computer virus - victim of information crime.