الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي و البحث العلمي

جامعة غارداية

كلية : الحقوق و العلوم السياسية

قسم: الحقوق

العنوان:

مكافحة جرائم المعلوماتية

في التشريع الجزائري

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في مسار: الحقوق

تخصص: القانون الجنائي

إعداد الطالب :

ماشوش مراد

إشراف:

الدكتور شول بن شهرة

مساعد المشرف:

أ/ محمد بوكرارشوش

الرقم	إسم الأستاذ و لقبه	الدرجة	الجامعة	الصفة
1	د. الحاج محمد قاسم	محاضر أ	غارداية	رئيساً
2	د. شول بن شهرة	محاضر أ	غارداية	مشرفاً و مقرراً
3	أ. بكرارشوش محمد	محاضر ب	ورقلة	مساعد المشرف
4	أ. لخضاري إيمان	محاضر ب	غارداية	عضواً مناقشاً

السنة الجامعية : 2013 / 2014

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

اَلْحَمْدُ لِلَّهِ رَبِّ ٱلْعَالَمِينَ ٱلرَّحْمَنِ ٱلرَّحِيمِ
مَالِكِ يَوْمِ ٱلدِّينِ إِيَّاكَ نَعْبُدُ وَإِيَّاكَ
نَسْتَعِينُ ٱهْدِنَا ٱلصِّرَاطَ ٱلْمُسْتَقِيمَ
صِرَاطَ ٱلَّذِينَ أَنْعَمْتَ عَلَيْهِمْ غَيْرِ
ٱلْمَغْضُوبِ عَلَيْهِمْ وَلَا ٱلضَّآلِّينَ

يقول عماد الأصفهاني

﴿ إني رأيت أنه لا يكتب إنساناً كتابا في يومه إلا قال في غده ، لو غير هذا لكان أحسن ، ولو زيد هذا لكان أفضل ، ولو قدّم هذا لكان أقوم ، وترك هذا لكان أجمل. وهذا من أعظم العبر ، وهو دليل على استيلاء النقص على جملة البشر..... ﴾

الفهرس

المقدمـــــــة

مقدمـــة:

تعد جرائم نظم المعلومات ظاهرة مستحدثة في مجال الجريمة، و التي تبذل بشأن مكافحتها الجهود الدولية و الإقليمية و حتى الوطنية، وذلك بما لها من تأثير كبير على المصلحة الاجتماعية و الاقتصادية و السياسية في أي دولة، و ذلك يدعي البحث في سبل حماية نظم المعلومات لاسيما أن هذه التكنولوجيا قد ربطت العالم برباط واحد من خلال شبكات المعلومات و هي الأنترنت، و من ثم يكون غير المشروع الذي لا يجرم في دولة مؤثراً بالسلب على الحماية المقررة من قبل الدول الأخرى.

فلقد سارعت كثير من الدول من خلال الجهات القانونية المعنية بالبحث في مواجهة الظواهر المستحدثة من الإجرام، و ذلك بالبحث عن التعريف بها و التعرف على سماتها و حمايتها لكي يمهد الطريق أما المشرع باختيار و انتقاء الحماية الملائمة لمواجهتها.

و الحاصل أن كلما ظهرت وسائل جديدة يستخدمها الانسان حياته، يقترن بها إساءة الاستخدام من قبل الأشخاص الذين يجدون فيها وسيلة ميسرة لارتكاب الجريمة، و كثيراً ما كان يقتصر تأثيرها على أسلوب الجريمة دون أن يؤثر في موضوعها بأي تغيير تخالف به بنيانها التي أسست عليه، فكان التجريم يقتصر على الاعتداء بتلك الوسيلة في مجال الجريمة و تجريم بعض السلوكيات التي ترتبط بها، مثال ذلك ما حدث عند استخدام السيارة كوسيلة لانتقال الأفراد فقد تم تجريم أفعال الإصابة الخطأ أو القتل الخطأ إلى غير ذلك من الأفعال التي ترتبط بتلك الوسيلة.

أما في مجال نظم المعلومات فإن الأمر جد مختلف فنظم المعلومات تدخل في مجالات عديدة في حياة البشر و مرشحة لأن تشمل كافة مجالات الحياة، حيث تعتمد القطاعات المختلفة في الوقت الحاضر في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية نظراً لما تتميز به من عنصري السرعة و الدقة في تجميع المعلومات و تخزينها و معالجتها و من ثم نقلها و تبادلها بين الأفراد و الجهات المختلفة.

غير أن الجانب الايجابي و المشرق لعصر المعلوماتية لا ينفي الانعكاسات السلبية التي افرزتها هذه التقنية العالية و المتمثلة في اساءة استخدام الانظمة المعلوماتية و استغلالها على نحو غير مشروع، حيث أدى هذا التطور الهائل إلى ظهور أنماط مستحدثة من الجرائم اصطلح عليها بالجرائم المعلوماتية كما أن هذه الجرائم الحديثة يختلف مرتكبوها عن المجرمين التقليدين، فهذه الطائفة الجديدة من المجرمين التي تمارس هذه الجرائم متمتعين بقدرات ذهنية غير عادية لا يميل إلى استعمال العنف بل أساليبه تتسم بالهدوء و ذات فعالية كبيرة و مؤثرة.

1- إشكالية الموضوع:

و مع ظهور هذا النوع المستجد من الجرائم، يهدف هذا البحث إلى محاولة الإجابة على الإشكالية التالية:

كيف تعامل المشرع الجزائي الجزائري في مواجهة الجرائم المعلوماتية؟

و سنحاول الإجابة عن ذلك من خلال الإجابة على التساؤلات التالية:

- **ما هو مفهوم الجريمة المعلوماتية من خلال تعريفها و خصائصها و أنواعها؟**
- **من هو المجرم المعلوماتي و ماهي سماته ؟**
- **ماهي الجهود الدولية و الإقليمية التي تركت بصمتها في هذا المجال؟**
-

2- أهمية الموضوع:

إن النشاطات غير المشروعة في مجال المعلوماتية أو الجرائم المعلوماتية تعد من الموضوعات الحديثة التي فرضت نفسها على المستوى الوطني و الإقليمي و الدولي، والتي ينبغي على المشرع الجنائي مواجهتها بتشريعات حاسمة لمكافحتها و عقاب مرتكبيها، و تتبلور أهمية الموضوع على:

أولا: حيث أن الموضوع يتعلق التكنولوجي و الجرائم الناجمة عن هذا التطور و هي جرائم مستحدثة مما يجعلها تختلف في ميكانيزماتها عن الجرائم التقليدية.

ثانياً: تثير المعلوماتية باعتبارها علم المعالجة الآلية للبيانات مشكلات قانونية عدة إذ يساء استخدامها لارتكاب الجريمة عن بعد من ناحية، أو أن تكون محلاً للاعتداء عليها من ناحية أخرى، مما يثير مسألة تكييف الاعتداء و ما إذ كان يشكل جريمة أم لا.

ثالثاً: السلوك الإجرامي للمجرم المعلوماتي يختلف عن السلوك الإجرامي للمجرم التقليدي، فالمجرم المعلوماتي استغل هذا التطور في ابتكار اساليب جديدة يجب التصدي لها و معرفة كيفية التعامل معها.

رابعاً: تمثل المعلومة قوة مستحدثة مما يجعلها في مقدمة الأولويات لحمايتها لكي لا تستخدم على نحو غير مشروع.

3- أهداف الدراسة:

يسعى هذا البحث إلى تحقيق هدفه الرئيسي و المتمثل في محاولة تقديم دراسة تبين لنا مفهوم الجريمة المعلوماتية من خلال تعريفها و استظهار سماتها و تتبيان أنواعها، بالإضافة إلى التعرف عن المجرم المعلوماتي و ما يتميز به بالنظر إلى المجرم التقليدي.

كما أحاول تقديم أهم الجهود الدولية و الاقليمية في مواجهة الجرائم المعلوماتية و مدى أنعكاسها على القوانين الجزائية في الجزائر.

4- أسباب اختيار الموضوع:

هناك جملة من الأسباب التي دفعتني إلى اختيار هذا الموضوع، نذكر منها:

- الجرائم المعلوماتية من أخطر الجرائم في العصر، فآثارها لا تقتصر على فرد أو مؤسسة أو على الدولة الواحدة بل تتجاوز الحدود الإقليمية.
- أهمية الوقوف على هذا النمط الجديد من الجرائم الذي بدأ يغزو المجتمعات خاصة مع زيادة استخدام جهاز الكمبيوتر في جميع مناحي الحياة و سهولة الحصول عليه تسبب في كثرة الانتهاكات الواقعة بواسطته و قلة الحماية القانونية
- كون هذه الجريمة تحتاج في مكافحتها تعاون الدول فيما بينها، و أصبحت أساليب هذه الجرائم مستعملة من طرف العصابات المنظمة.

- محاولة الإلمام و معرفة الأساليب الحديثة المتبعة من طرف المجرم المعلوماتي، و محاولة التصدي لها عن طريق ما نص عليه المشرع الجزائي الجزائري من خلال قانون العقوبات و القوانين الأخرى.
- التعرف على الجهود الدولية و الإقليمية لمكافحة هذه الجريمة و مدى انعكاسها على الجهود الوطنية
- و لقد وقع اختياري على دراسة هذا الموضوع إيماناً مني بأهمية الوقوف على هذا النمط الجديد من الجرائم الذي بدأ يغزو مجتمعاتنا مع زيادة استخدام الانظمة المعلوماتية في مناحي الحياة كلها.
-

5- الدراسات السابقة:

بدأت الدراسات العربية في مجال الجرائم المعلوماتية متأخرة بما هو عليه الحال في الدراسات الأجنبية التي رافقت انتشار الكمبيوتر، و ربما يعود ذلك إلى تأخر التقنية الحديثة في معظم الدول العربية و منها الجزائر، و من بين الدراسات المتخصصة في هذا المجال:

- رسالة ماجستير أنجزت من طرف الباحث العزام أحمد حسين بعنوان الحكومة الالكترونية في الأردن مع امكانية التطبيق، الأردن، 2001
- رسالة ماجستير أنجزت من طرف الباحثة أمال قارة بعنوان الجريمة المعلوماتية، بن عكنون الجزائر، 2002
- رسالة ماجستير أنجزت من طرف الباحث حمزة بن عقون بعنوان السلوك الإجرامي للمجرم المعلوماتي، باتنة، الجزائر، 2012
- رسالة ماجستير أنجزت من طرف الباحث يوسف صغير بعنوان الجريمة المرتكبة عبر الأنترنت، تيزي وزو، الجزائر، 2013

6- المناهج المتبعة:

أحاول من خلال هذا البحث بشكل مجمل تقديم صورة عامة لأبرز التحديات المصاحبة لهذه التكنولوجيا، وفق منهجية تطمح إلى تقديم نظرة للظاهرة الإجرامية، لهذا سأعتمد على المنهج الوصفي التحليلي، و ذلك بوصف الجريمة و خصائصها و أنواعها و التحليلي بذكر الجهود الدولية و الإقليمي لمكافحة هذه النوعية من الجرائم و تحليل الأساليب المتبعة من طرف المشرع الجزائري لذلك.

7- الصعوبات المعترضة:

واجهت أثناء إعداد هذا البحث عدة صعوبات أهمها قلة المراجع المتخصصة في المكتبات الجامعية و خصوصاً ما تعلق بالجهود الدولية و الإقليمية، وحتى إن تمكنت الحصول على البعض من المراجع فإنها غالباً لا تتناول الموضوع في التشريع الجزائري.

كما عانيت من ندرة التطبيقات القضائية في هذا المجال، نظراً لحداثته و كذلك لاتصاله بالجانب التقني و الفني بالنظام المعلوماتي بشقيه المادي و المعنوي.

8- خطة الدراسة

و في سبيل إعداد هذا البحث ارتأيت تقسيم هذه الدراسة إلى فصلين:

- تعرض الفصل الأول الإطار المفاهيمي للجريمة المعلوماتية من خلال تناوله لمناهج التعريفات من ضيقة إلى موسعة و من تقنية إلى قانونية بالإضافة إلى تحديد خصائصها من خلال المبحث الأول، أما المبحث الثاني فتطرقت إلى المجرم المعلوماتي و سماته التي يتميز بها بالنظر للمجرم التقليدي و كذلك لأنواع و تقسمات الجريمة المعلوماتية.

- و لأن الإشكالية الأساسية تدور حول مكافحة الجريمة المعلوماتية، فقد تم تخصيص الفصل الثاني إلى الجهود الدولية و الإقليمية في مجال مكافحة الجريمة المعلوماتية بشيء من التفصيل في المبحث الأولو صولاً إلى جهود المشرع الجزائي الجزائري لمواجهة هذه الجريمة في المبحث الثاني.

و أنهيت البحث بخاتمة ضمنتها بالنتائج المتوصل إليها، ثم تراءى لنا بعد الدراسة اقتراح مجموعة من التوصيات.

الفصل الأول

ماهية جرائم المعلوماتية

الفصل الأول : ماهية الجرائم المعلوماتية و أنواعها

نظراً لأن الجريمة المعلوماتية جريمة حديثة نسبياً ، و ذلك لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات ، و نتيجة لحداثة هذه الجريمة فقد كانت هناك اتجاهات مختلفة في تعريفها ، كما أنها اتسمت بمجموعة من الخصائص و السمات التي ميزتها عن غيرها من الجرائم التقليدية و الجرائم الأخرى ، كما انها جلبت معها طائفة جديدة من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية.

و لذلك و في هذا الفصل سوف أتناول تعريف الجريمة المعلوماتية و أهم الخصائص التي ميزتها عن غيرها من الأنماط الأخرى للجرائم (المبحث الأول) ، أما المبحث الثاني فسأستعرض فيه أنواع جرائم المعلوماتية على حسب التصنيف الذي اقترحناه.

المبحث الأول : مفهوم جرائم المعلوماتية

بحث أي فرع من فروع المعرفة لا بد من بيان مفهومه من خلال تعريفه و تبيان سماته الأساسية أي خصائه لكي يتم رسم الصورة العامة لهذا البناء المعرفي[1] و منه ومن خلال موضوع بحثنا حول الجرائم المعلوماتية وحول خصوصية هذا النوع من الجرائم عن غيرها من الجرائم الأخرى و بالرغم من حداثة هذا النوع من الجرائم إلا أنه يصعب إيجاد تعريف موحد لهذا النوع من الجرائم فلقد وجدت العديد من المناهج و المدارس الفكرية التي خاضت في وضع تعاريف علمية دقيقة لجرائم المعلوماتية و على الرغم من اختلاف هذه التعاريف و العقائد الفكرية[2] حولها إلا أنها تصب في قالب واحد، و من جهة أخرى ولاكتمال هذا البناء المعرفي و كما أشرنا حول تعدد هذه المناهج العلمية حول وضع تعريف شامل للجريمة المعلوماتية إلا أنها لا تكاد تتفق حول سماتها و خصائها و هذا ما سنتطرق إليه في هذا المبحث من خلا تبيان تعريف الجريمة المعلوماتية في المطلب الأول و خصائصها في المطلب الثاني.

المطلب الأول : تعريف الجريمة المعلوماتية

بداية لا بد أن نشير إلى أنه لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة المعلوماتية للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات و استخدامها، فالبعض يطلق عليها جريمة الغش المعلوماتي ، و البعض الآخر يطلق عليها الاختلاس المعلوماتي أو الاحتيال المعلوماتي، في حين يذهب آخرون إلى تسميتها إلى جرائم إساءة استخدام تكنولوجيا المعلومات و يسميها آخرون جرائم الكمبيوتر و الأنترنت أو الجرائم الإلكترونية إلى من أطلق عليها الجرائم المستحدثة.

فيذهب الكثير من الفقهاء مع الاتجاه الذي يفضل إطلاق اصطلاح الجريمة المعلوماتية على الجرائم المتعلقة بالحاسوب والإنترنت، فاصطلاح الجرائم المعلوماتية عام ويشمل التقنيات الحالية والمستقبلية كلها المستخدمة في التعامل مع المعلومات بما في ذلك الحاسوب وشبكة الإنترنت.

قبل تطرقنا إلى تعريف الجريمة المعلوماتية يتحتم علينا إعطاء فكرة واضحة مدلولها، فهو مصطلح مركب من شقين **الجريمة** و **المعلوماتية** ، و كما لا يخفى عن الجميع ممن هم من دراسي القانون على مختلف فروعه و عن غير الدراسين للقانون فإن **الجريمة** عموما في نطاق القانون الجنائي العام بأنها سلوك الفرد عملا كان أو امتناعا يواجهها المجتمع بتطبيق

1. د. منذر الشاوي ، فلسفة القانون، مطبوعات المجمع العلمي بالعراق، بغداد 1994 ، ص7
2. د. محمد سامي الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات، دار النهضة العربية،القاهرة،1994، ص173

عقوبة جزائية ،و ذلك بسبب الاضطرابات التي يحدثه في النظام الاجتماعي[1]، و هو التعريف الذي يستند على عناصر الجريمة إلى جانب بيانه لأثرها (السلوك، و السلوك غير المشروع وفق القانون الإرادة الجنائية و أثرها. العقوبة أو التدبير الذي يفرضه القانون) ؛و هي الأوصاف التي تميز بين الجريمة عموما ، و بين الأفعال المستهجنة في نطاق الأخلاق أو الجرائم المدنية أو التأديبية.

أما مصطلح **المعلومة** فهي مترجمة من كلمة (Informations) باللغة الفرنسية ، حيث لا يوجد إلى يومنا هذا نص قانوني يعطي تعريفا جامعا مانعا للمعلومة ؛غير أن القانون الفرنسي الصادر في 29 يوليو 1982 الخاص بالاتصالات السمعية و البصرية أشار إلى تعريف عام للمعلومة حيث ينظر إليها بوصفها "رنين أو صور أو وثائق أو بيانات أو رسائل من أي نوع " **Sons**, **images**, **documents**, **données ou messages de toute nature**" ،و يعرف الأستاذ **Catala** المعلومة بأنها "رسالة ما معبر عنها بشكل يجعلها قابلة للنقل أو الإبلاغ للغير"[2] ،

أما تعريف المعلومات وفقا للمعجم الموسوعي لمصطلحات المكتبات والمعلومات فهي البيانات التي تمت معالجتها لتحقيق هدف معين أو لاستعمال محدد ، لأغراض اتخاذ القرارات ، أي البيانات التي

أصبح لها قيمة بعد تحليلها ، أو تفسيرها ، أو تجميعها في شكل ذي معنى والى يمكن تداولها وتسجيلها ونشرها وتوزيعها في صورة رسمية أو غير رسمية وفى أي شكل[3].

إلا أن المعلوماتية و هو مصطلح مشتق من كلمة المعلومة و هي المعالجة الآلية للمعلومات و ترجمة من اللغة الفرنسية (**Informatique**) * و تعني تكنولوجيا و معالجة و إرسال المعلومات بواسطة كمبيوتر يقصد بها ذلك العلم الذي يهتم بالموضوعات و المعارف المتصلة بتحصيل المعلومات و تجميعها و تنظيمها و إختزانها و استرجاعها و تفسيرها و

1 .د أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، الطبعة الثالثة ، دار هومه، 2006 ، ص 3

2 . Piérre CATALA , la propriété de l'information Cité par f.Toubal le logiciel- analyse juridiqueFUDUL .L.G.D,J1986, p 126

3 د شعبان خليفة ، قاموس البنهاوي الموسوعي في مصطلحات المكتبات والمعلومات، دار المريخ ، 1990 ، ص 512

* ترجمة عربية للمصطلح الفرنسي Informatique الذي أوجده الفرنسي فيليب دريفس Philippe Drefus عام 1962 للميلاد نتيجة قيامه بتجميع المقطع الأول من كلمة معلومات Information مع المقطع الأخير من كلمة اتوماتيك Automatiqueلوصف المعالجة الآلية للمعلومات وقد انتشر هذا الاصطلاح فيما بعد بشكل أوسع عندما تبنته الأكاديمية الفرنسية للمعلومات في 19 أفريل، محمد بن نصير سرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب و الأنترنت، مذكرة ماجستير في العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، 2004، ص29.

بثها و تحويلها واستخدامها عن طريق الرموز و المفاتيح[1] ، أي أنها تشير بصفة واضحة إلى تدخل الآلة في معالجتها هذا ما نستنتجه من خلال هذا التعريف " **هي علم المعالجة العقلية للمعلومات باستخدام آلات تعمل ذاتيا**" و هو التعريف المترجم من اللغة الفرنسية " **La science du traitement relationnel par des machines automatique d'information notamment**"[2].

غير أن العقبة الأولى و الأساسية التي تعترض ظاهرة الجريمة المعلوماتية هي عدم وجود تعريف مجمع عليه لهذه الجريمة ، و ذلك لغياب تعريف لها عند أغلب التشريعات إلا أن الفقه بذل لذلك عدة محاولات لتعريف الجريمة المعلوماتية اتجهت بعضها إلى التضييق من مفهوم هذه الجريمة بتقليل الحالات التي يمكن أن يتصف النشاط الإجرامي بها، و البعض الآخر ذهب إلى التوسع في هذه الجريمة حتى يمكن أن يدخل في عدادها في كثير من الأحيان أفعال لا يمكن أن تعد من قبيل جرائم الحاسب الآلي.

يرى أصحاب المذهب المضيق لتعريف الجريمة المعلوماتية على أنها " كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازماً لارتكابه من ناحية لملاحقته وتحقيقه من ناحية أخرى" [3].

ذهب الفقيه (**Merwe**) إلى أن الجريمة المعلوماتية" هي الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي أو هو الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية"[4].

فيما عرفها الفقيه (**Rose Blat**) بأنها " كل نشاط غير مشروع موجة لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الألى والى تحويل طريقه"[5].

و يرى الأستاذ (**Tiedemann**) الجريمة المعلوماتية تشمل "أي جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات." [6]

1. مسعود خثير ، الحماية الجنائية لبرامج الكمبيوتر أساليب و ثغرات ، دار الهدى ، 2010 ، ص19
2. د أحمد خليفة الملط ،الجرائم المعلوماتية ، الطبعة الثانية، دار الفكر الجامعي، 2006 ص72
3. د نائلة عادل محمد قورة ، جرائم الحاسب الإقتصادية دراسة نظرية و تطبيقية ، ط1 ، دار النهضة العربية ، القاهرة ، 2003 ، ص21
4. Parker Donn , Computer Abus , Stanford Research , 1973, p517
5. Tiedemann , Fraude et autres délits d'affaire commis à l'aide d'ordinateurs , RDPC, 1984 , p 61
6. Tiedemann ، المرجع نفسه ، ص 65

كما يرى الأستاذ (**Masse**) أن المقصود بالجريمة المعلوماتية: " الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح."[1]

ولعل أبرز تعريفات الإتجاه الضيق الذي جاء به الفقيه **SIEBER** :

« Est considère comme crime informatique tout comportement qui concerne un traitement automatique de illégal ou non autorisé données ou de transmission de données.» [2]

لقد انطلق أنصار الاتجاه الضيق في وضع تعريفاتهم من النقطة المتعلقة بضرورة تحديد العلاقة بين المعلوماتية و الأفعال غير المشروعة لتحديد ما إذا كانت تلك الأفعال تدخل في نطاق الجرائم المعلوماتية أم لا أي حتى تشكل هذه الأفعال غير المشروعة جريمة معلوماتية لا بد من توافر القدر الكافي من معرفة تكنولوجيا الحاسبات بدرجة كبيرة من أجل ارتكاب تلك الأفعال من جهة ، و من جهة أخرى و من أجل ملاحقتها و متابعتها و التحقيق فيها لا بد من توافر أيضاً القدر الكبير من معرفة تكنولوجيا الحاسبات عند القائمون على معاينتها و ملاحقة مرتكبيها.[3]

كما اعتمدوا في تحديد الأفعال غير المشروعة على أن هذه الأفعال تكون موجهة ضد الأموال المعلوماتية من خلال الحسابات البنكية و مجمل التعاملات الاقتصادية.

فقد لقي أصحاب هذا الاتجاه المضيق انتقادات لكونه حصر تعريف الجريمة المعلوماتية في الحالات التي تتطلب قدراً كبيراً من المعرفة التقنية لارتكابها ، إذ أنه في كثير من الحالات يرتكب الفعل دون الحاجة إلى هذا القدر من المعرفة و رغم ذلك لا يمكننا انكار ان هذه الأفعال تدخل في عداد جرائم المعلوماتية كإتلاف البيانات المخزنة داخل النظام المعلوماتي.

و على عكس الاتجاه السابق يرى فريق آخر من الفقهاء ضرورة التوسع من مفهوم الجريمة المعلوماتية لتشمل أي فعل متعمد مرتبط بأي وجه بالحاسبات أي كل سلوك إجرامي يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة

1 Masse , Rapport final final du conseil de l'Europe sur la criminalité en relation avec l'ordinateur, 1988, p56

2 Lucas , le droit de l'informatique, vol2, Thiémis, Paris,1998, p 496

3 د نائلة عادل محمد قورة ، المرجع السابق ، ص 29

الكمبيوتر، فلقد عرفها الخبير الأمريكي (Parker) بأنها "كل فعل إجرامي متعمد أياً كانت صلته بالمعلوماتية ترتبت عنه خسارة تلحق بالمجني عليه أو مكسب يحققه الجاني."[1]

أما الفقيه (**Lesli D.Ball**) بأنها "فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسة."[2]

أما الفقيهان (**Totty et Hardcastle**) "بأنها تلك الجرائم التي يكون دور الحاسب فيها إيجابيا أو سلبياً."[3]

وقد ذهبت مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية (**OECD**) في عام 1983 الخاص بالاستبيان حول الغش المعلوماتي الذي أوردته بلجيكا في تقريرها إلى تعريف الجريمة المعلوماتية أنها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها".4

أما مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين فقد تبنى التعريف الآتي للجريمة المعلوماتية إنها: " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية[5]."

و بالرغم من محاولات التوسع في تعريف الجرائم المعلوماتية بالإحاطة قدر الإمكان بجميع الأشكال الإجرامية لم يسلم مريدو هذا الاتجاه من سهام الانتقادات و لعل أبرز الانتقادات الموجهة ، إذ قد ترتكب الجريمة و يستعمل فيها الحاسب الآلي و لا نكون بصدد جريمة معلوماتية كمن يقوم بالاتصال عبر حاسب آلي بشركائه للقيام بعملية سطو على بنك مثلا أو من أجل سرقة أو أي جريمة أخرى.

و نستخلص مما سبق أن اختلاف الفقه سواءاً المضيق أو الموسع في تعريفه للجريمة المعلوماتية مرده الاختلاف في المعيار المعتمد عليه و الزاوية التي ينظر إليها كل منهما. و من أجل مفهوم شامل للجريمة لا بد من تعريفها من الجانب الفني (التقني) و من الجانب القانوني باعتبار أنها جريمة تقليدية ترتكب بأسلوب إلكتروني.

---

1 Parker Donn ، المرجع السابق ، ص 519

2 Tiedemann ، المرجع السابق ، ص 66

3 Totty et Hardcastle, Computer related crime in information technology andthelaw , UK , 1986 , p26

4 د نائلة عادل محمد قورة ، المرجع السابق ، ص 23

5 مؤتمر الأمم المتحدة العار لمنع الجريمة و معاقبة المجرمين ، الذي عقد في فينا بين 10 و 17 أفريل 2000

الفرع الأول : تعريف الجريمة المعلوماتية من الجانب الفني (التقني)

يرى بعض الفقهاء أن لجرائم المعلوماتية تعريفاً فنياً يفصّل العناصر و يحدد أركان كل نشاط إجرامي ، و أورد تعريفه الفني على أنه " كل نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة ، كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[1]، كما ذكر تعريفاً آخر في معرض بحثه في الأدلة الجنائية الرقمية **Digital Evidene** ، حيث عرف الجريمة المعلوماتية بأنها "أية جريمة لها علاقة بالحاسوب و شبكات المعلوماتية ، بما في ذلك من جرائم التي لا تعتمد كثيراً على الحاسوب" و أوضح أن هذا التعريف التقني أو الفني ليشمل الحالات التي لا يدخل الحاسوب بشكل مباشر في الجريمة و لكن يحتوي على أدلة جنائية رقمية لها علاقة بالجريمة و أورد مثالا للتوضيح ، بأن يدفع متهم أنه كان يستخدم الأنترنت وقت وقوع الجريمة أي هنا لا دور للحاسوب في الجريمة و لكنه من الممكن أن تحتوي على أدلة قد تدعم أو تدحض ادعاء المتهم.

وانتهج معظم الفقهاء في تعريفهم للجريمة المعلوماتية و رأوا من منظورهم أن يعرفوها تعريفًا تقنيًا باعتبار أن هذا النوع من الجريمة تعتمد بالأساس على التكنولوجيا و أن موضوعها هو الحاسوب و اعتبر أن الجريمة المعلوماتية " عبارة عن نشاط اجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي[2] "

ولقد تبنى العديد من الفقهاء و الدارسين[3] أن التعريف البلجيكي السالف (OECD) بوصفه لديهم أنه تعريفاً واسعاً و فنياً لأن هذا التعريف يتيح الإحاطة الشاملة قدر الإمكان بهذه الجريمة ، و لأن هذا التعريف المذكور يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها ، و لأنه يتيح امكانية التعامل مع التطورات التقنية المستقبلية.

الفرع الثاني : تعريف الجريمة المعلوماتية من الجانب القانوني

و من ضمن التعريفات التي تعتمد على أكثر من معيار، يعرف الفقه كذلك الجريمة المعلوماتية وفق معايير قانونية صرفة ، ولقد كانت مبرراتهم في هذا الإتجاه (التعريف القانوني) هو مدى التعامل مع الجرائم المعلوماتية كجرائم خاصة[4] و

1 محمد بن نصر السرحاني ، المرجع السابق، ص34

2 د. عبد الفتاح بيومي حجازي ،الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية، مصر ،2002 ، ص01

3 نبيل صقر ، جرائم الكمبيوتر و الأنترنت في التشريع الجزائري ، دار الهلال للخدمات، 2009، ص50

4 نبيل صقر ، المرجع نفسه ، ص52

الإسقاطات الناتجة على ذلك من حيت الشكل أو الموضوع و بقصد بها من الناحية الإجرائية او في نطاق قانون العقوبات و معنى ذلك أننا أمام ظاهرة اجرامية مستجدة من حيث موضوع الجريمة و وسيلة ارتكابها و سمات مرتكبيها و أنماط السلوك الإجرامي المجسد للركن المادي.

من هؤلاء الأستاذ **Thomas J.Smedinghoff** في مؤلفه (المرشد القانوني لتطوير و حماية و تسويق البرمجيات) ، حيث عرفها "أي ضرب من النشاط الموجه ضد أو المنطوي على استخدام نظام الحاسوب"[1] ، و نرى في تعبير "النشاط الموجه ضد" يدخل في إطاره المكونات الأساسية للحاسوب SOFT و هي المكونات المنطقية من حيت نظام التشغيل و البرامج و قاعدة المعطيات ، و كذا HARD و هي المكونات المادية للحاسوب كاللوحة الأم و المكونات المادية الأخرى.

أما الأستاذين **Jack Bologna** و **Robet J. Lindquist** "كل جريمة يستخدم الحاسوب كوسيلة أو أداة لارتكابها أو يمثل اغراء بذلك أو جريمة يكون الحاسوب نفسه ضحية " و بهذا التعريف انضم كلٌ من الأستاذين إلى التعريف السابق الذكر بإعطاء وجه آخر من الجريمة و هو الاعتداء على الحاسوب نفسه وخرجوا بذلك عن المنطق الذي يكرس الحاسوب الوسيلة أو الأداة التي بها يتم النشاط الإجرامي و لخصوا على الجهاز نفسه يكون عرضة لهذا النشاط الإجرامي.

لقد خصص المشرع الجزائري من خلال القانون 09-04[2] المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، الفصل الأول منه للمصطلحات حيث نصت المادة 2:

" الفقرة أ: جرائم المساس بالأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الكترونية.

الفقرة ب: منظومة معلوماتية هي أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذاً لبرنامج معين.

[1] نبيل صقر المرجع نفسه ص 51

[2] قانون 09-04 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، الجريدة الرسمية، 47، الصادر في 16 أوت 2009 .

الفقرة ج : معطيات معلوماتية هي أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها".

إن طبيعة و أبعاد ظاهرة الجرائم المعلوماتية ، سيما في ظل تطور انماطها يوما بعد يوم مع تطور استخدام الشبكات و ما أتاحته الأنترنت من فرص جديدة لارتكابها مما يضطر المشرع من وضع تعريفات و نصوص جديدة قادرة على الاحاطة بمفردات و متطلبات و خصوصية هذا النوع من الجرائم و أنه يجب مراعاة عدة اعتبارات مهمة عند وضع تعريف للجريمة المعلوماتية منها :

- أن يكون هذا التعريف مقبول ومفهوم على المستوى العالمي.
- أن يراعى هذا التعريف التطور السريع والمتلاحق في تكنولوجيا المعلومات.
- أن يحدد التعريف الدور الذي يقوم به جهاز الكمبيوتر في إتمام النشاط الإجرامي.
- أن يفرق هذا التعريف بين الجريمة العادية والجريمة المعلوماتية وذلك عن طريق إيضاح الخصائص المميزة للجريمة المعلوماتية.

المطلب الثاني : خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بخصائص و سمات تميزها عن غيرها من الجرائم الأخرى، فأول ما يلفت النظر في هذا النوع من الجرائم هو نعومتها و بعدها عن العنف فلا تتطلب لإرتكابها الشدة و لا استعمال الأدوات الخطرة كالأسلحة ولا تحتاج إلى مداهمات و كسراً للأبواب أو تسلق الجدران، فنقل بيانات ممنوعة أو التلاعب بالأرصدة البنكية مثلاً لا تحتاج إلا إلى لمسات أزرار. ثم إن الجريمة المعلوماتية تمتاز أيضاً بإمكانية تنفيذها بسرعة فائقة أي ترتكب في وقت قياسي كما تتميز أيضاً بإمكانية إرتكابها عن بعد فلا تتطلب لوجود الفاعل في مكان الجريمة بل يمكنه تنفيذها في مكان بعيد عن مسرح الجريمة، فالشخص القائم على الحاسوب في أحد المصارف في طوكيو مثلاً يستطيع تحويل مبلغاً من المال إلى أحد فروع المصارف في برلين في ألمانيا ، و إن نسبة معتبرة من الجرائم المعلوماتية ترتكب عبر شبكات الأنترنت Internet حيث يكون الجاني في دولة و المجني عليه في دولة أخرى مما جعل التعاون الدولي[1] أمراً حتمياً لمكافحة هذ الظاهرة الإجرامية الجديدة ، كما أن الجريمة المعلوماتية صعبة الإثبات لعدم وجود تلك الآثار المادية عند الجرائم التقليدية (بقع الدم ، تكسير، خلع ....).

دون أن نغفل في سرد الخصائص و السمات التي تتميز بها الجريمة المعلوماتية عن غيرها من الجرائم عن الفاعل أو مرتكب هذه الجريمة الذي أصبح يعرف **بالمجرم المعلوماتي** [2] لتميزه أيضاً عن المجرم التقليدي في أسلوبه المنفرد في تنفيذه للجريمة و سرعته و مهارته.

و سنحاول فيما يلي التطرق إلى بعض السمات الخاصة بالجريمة المعلوماتية من خلال الفرع الأول ، أما الفرع الثاني سنخصصه بدراسة أهم سمات التي تميز المجرم المعلوماتي.

1 تجدر الإشارة إلى مؤتمر الامم المتحدة الثامن لمنع الجريمة و معاقبة المجرمين ، هافانا 1990 ، و في القرار المتعلق بالجرائم ذات الصلة بالحاسوب ناشد الدول الأعضاء أن تكثف من جهودها كي تكافح بمزيد من الفعالية عمليات إساءة إستخدام الحاسوب من خلال التعاون الدولي عير آليات قانونية ، محمد أحمد عبابنة، جرائم الحاسوب و أبعادها الدولية ، دار الثقافة ، عمان ، 2005 ص 361

2 د نائلة عادل محمد قورة ، المرجع السابق ، ص 49

الفرع الأول : السمات الخاصة بالجريمة المعلوماتية

تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية في عدة نواح ،سواء كان هذا التمييز في السمات العامة لها أو في الباعث على تنفيذها أو في طريقة هذا التنفيذ ذاته، كما تتميز بطابعها الدولي في أغلب الأحيان حيث تتخطى آثار هذه الجريمة حدود الدولة الواحدة.

أولاً : خصوصية الجريمة المعلوماتية : تتسم الجريمة المعلوماتية بصعوبة اكتشافها و إثباتها ؛و يرجع ذلك إلى عدة أسباب من بينها :

- وسيلة تنفيذها التي تتميز في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد، بالإضافة إلى الإحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجني عليهم من فقد ثقة عملائهم؛ فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة1. فعلى سبيل المثال أحصت وزارة الداخلية في فرنسا عام 1986 حوالي 1200 جريمة معلوماتية في حين كان هناك حوالي **53600** جريمة ضد الأشخاص و **900** 18 جريمة تندرج تحت وصف جرائم الآداب و **3 مليون جريمة ضد الأموال**، و في أحدث تقارير مركز شكاوى احتيال الانترنت (**IFFC**) الأمريكي أظهر التحليل الشامل للشكاوى التي قدمت للمركز خلال سنة 2004 قد بلغت **6 384** شكوى من ضمنها **5 273** حالة تتعلق باختراق الكمبيوتر عبر الانترنت و 814 تتعلق بوسائل الدخول و الاقتحام الأخرى كالدخول عبر الهاتف أو الدخول المباشر إلى النظام بشكل مادي؛ مع الإشارة إلى أن هذه الحالات هي فقط التي تم الإبلاغ عنها و لا تمثل الأرقام الحقيقية لعدد حالات الاحتيال الفعلي2.
- وفي مقابل انخفاض نسبة جرائم المعلوماتية في مواجهة الجرائم التقليدية ؛ترتفع الخسارة الناجمة عن الجرائم المعلوماتية بصورة كبيرة بالمقارنة بغيرها من الجرائم، فعلى سبيل المثال و في بحث منشور عبر شبكات الأنترنت للمركز الوطني للبيانات (**NCCCD**)3 للباحث **Berrnard Standlar** كانت الخسارة الناجمة عن **8 000** حالة سرقة في فرنسا عام 1986 حوالي **561** مليونا من الفرنكات الفرنسية ؛في حين يتضاعف هذا الرقم في حالة الجرائم المعلوماتية على الرغم من انخفاضها نسبة **8 مرات**؛ و في الولايات المتحدة الأمريكية توصل مكتب التحقيقات الفيدرالية .F.B.I إلى أن متوسط الخسائر التي تحققها الجريمة

1 د نائلة عادل محمد قورة ، المرجع السابق ، ص50

2 د هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن،-الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 1992 ، ص53

3 Berrnard Standlar، computer crime law، 2014/04/20، www.google.com

المعلوماتية يبلغ حوالي 500.000 دولار في حين لا تزيد الخسائر التي تخلفها جرائم السرقة العادية عن 3500 دولار[1].

- عدم اتسام الجريمة المعلوماتية بالعنف الذي تتميز به عن غيره من الجرائم التقليدية الأخرى، حتى أنه لا يوجد شعور حقيقي بعد الأمان في مواجهة الجريمة المعلوماتية كالذي يوجد بصورة دائمة في مواجهة غيرها من الجرائم ، حيث تكاد تختفي الصورة التقليدية للمجرم مصدر الخطر.
- غياب الشعور العام بعدم أخلاقية الفعل أو المساس بمصالح و قيم يحرص المجتمع على حمايتها بل غن الكثير من العاملين في مجال المعلوماتية لا يجدون حرجاً في استعمال الشفرات و الدخول إلى أنظمة الحاسبات الآلية بطريقة غير مشروعة أو نسخ البرامج بدلاً من شرائها، و هذا لا ينفي وصف الجريمة على هاته الأفعال من حيث اعتدائها على مصالح لها أهميتها في المجتمع و من تم تستحق الحماية القانونية و معاقبة من يمس بها.[2]

ثانيًا: الطبيعة لدولية للجريمة المعلوماتية

يمكن القول أن من أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، و من اكتسابها طبيعة دولية ،أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعددة الحدود، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل و تبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال ؛قد أدت إلى نتيجة مؤداها أن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد ، كما أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة المعلوماتية و حجم المعلومات و الأموال المستهدفة و المسافة التي قد تفصل الجاني عن هذه المعلومات و الأموال، قد ميزت الجريمة المعلوماتية عن الجريمة التقليدية بصورة كبيرة.

و من القضايا التي لفتت النظر إلى البعد الدولي للجريمة المعلوماتية ، قضية عرفت باسم مرض نقص المناعة (الأيدز) ، و تتلخص وقائعها عام 1989 عند قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج التي يهدف في ظاهره إلى اعطاء بعض النصائح الخاصة بهذا المرض، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة)[3] ، و كان يترتب تعطيل الجهاز بمجرد تشغيله ، ثم تظهر عبارة على الشاشة يقوم فيها الفاعل بطلب مبلغ

1 Rose Philipe, La criminalité informatique à l'horizon analyse prospective, 2005,p49

2 سفيان سوير ، جرائم المعلوماتية ، مذكرة ماجستير ، جامعة أبو بكر بلقايد تلمسان ،الجزائر ، 2010 ص 19

3 برنامج له القدرة على التمويه ببرنامج بديل ، و عند تشغيل البرنامج يبدأ نشاطه التدميري و يؤدي إلى تعديل و محو بعض أو كل البيانات

مالي يرسل على عنوان حتى يتمكن المجني عليه من الحصول على مضاد لهذا الفيروس، و في الثالث من فبراير 1990 تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة ، و تقدمت المملكة المتحدة بطلب تسليمه لمحاكمته لديها باعتبار أن النشاط الإجرامي المتمثل في إرسال البرنامج تم في أراضيها، و أياً ما كان الأمر فإن لهذه القضية الأثر البالغ من ناحيتين ، الأولى: أنها المرة الأولى التي تتم فيها تسليم متهم في جريمة معلوماتية و الثانية : أن يتقدم شخص للمحاكمة بتهمة إعداد برنامج مخرب.

ولقد أثارت الطبيعة الدولية للجرائم المعلوماتية تساؤلا مهما يتعلق بتحديد الدولة التي يختص قضاؤها بملاحقة الجريمة، فهل هي الدولة التي وقع بها النشاط الإجرامي ؛أم تلك التي توجد بها المعلومات محل الجريمة؛ أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب[1] ،كما أثارت هذه الطبيعة أيضا الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة المعلوماتية و بصفة خاصة فيما يتعلق بجمع و قبول الأدلة[2] ؛و لذلك فلقد بات من الضروري إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة جرائم المعلوماتية و العمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم ،فيجب أن يشمل هذا التعاون تبادل المعلومات ، تسليم المجرمين ،و ضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى ،كما أن هذا التعاون يجب أن يمتد إلى مكافحة الجريمة المعلوماتية ،و هو ما يقتضي أيضا تبادل المعلومات بين الدول المختلفة، و تعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو "إبرام الاتفاقيات الدولية".

و تعد الاتفاقيات الخاصة بتسليم أو تبادل المجرمين من أهم الوسائل الكفيلة بضمان محاكمة مجرمي المعلوماتية و تجنب خلق ما يسمى "بجنة جرائم المعلوماتية" **Computer Crime Havens** ، إلا أن الوصول إلى إبرام هذه الاتفاقيات يقتضي بطبيعة الحال التنسيق بين قوانين الدول المختلفة لضمان تحقق "مبدأ ازدواجية التجريم" فيما يتعلق بجرائم المعلوماتية.

و نجد أن هذا المبدأ يقف عقبة رئيسية طالما أن كثيرا من القوانين لم يتم تعديلها بحيث تتلاءم مع هذه الجرائم. و إن كان مشرعنا قد خطى خطوة إلى الأمام في هذا المجال بصدور القانون 15/04 المعدل و المتمم للأمر 156/66 المتضمن قانون العقوبات، و الذي استحدث نصوصًا خاصة بالجرائم الماسة بالأنظمة المعلوماتية في المواد من المادة 394 مكرر إلى غاية المادة 394 مكرر 7 من القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات بالإضافة إلى قانون

1 إن المشرع الجزائري قد عقد الاختصاص للمحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال المرتكبة خارج الوطن عندما يكون مرتكبها أجنبي و تستهدف الدولة أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني ، المادة 15 من قانون 04/09

2 د. نائلة عادل محمد فريد قورة –المرجع السابق– ص54.

04/09 المؤرخ في 05 08 2009 المتضمن القواعد الخاصة للوقاية من الإجرام المتصل بتكنولوجيات الإعلام و الاتصال و مكافحته و سنّ أحكام خاصة بالتعاون و المساعدة القضائية الدولية[1]. ونخلص مما سبق إلى أنه في سبيل مكافحة الجريمة المعلوماتية يجب أن تتحرك الدول المختلفة في محورين :

- **الأول** : داخلي بحيث تتلاءم تشريعاتها الداخلية مع هذا النمط الجديد من الجرائم.
- **الثاني** : دولي عن طريق عقد الاتفاقيات الدولية، حيث لا يستفيد مجرمو المعلوماتية عن عجز التشريعات الداخلية من ناحية ،و غياب الاتفاقيات الدولية التي تعالج سبل مواجهة هذه الجرائم من ناحية أخرى.

الفرع الثاني : السمات الخاصة بالمجرم المعلوماتي

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب ،و إنما كان له أثره أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين .و لقد اختلف الباحثون في تحديد هذه السمات[2]، و يعد الأستاذ **Parker** واحدا من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة ؛و بالمجرم المعلوماتي بصفة خاصة. إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه. فكل ما في الأمر أنه ينتمي إلى طائفة خاصة من المجرمين تقترب في سماتها من جرائم ذوي الياقات البيضاء. و إن كانت – في رأيه- لا تتطابق معها.

فالمجرم المعلوماتي من ناحية ينتمي في أكثر الحالات إلى وسط اجتماعي متميز كما أنه على درجة من العلم و المعرفة (و إن لم يكن من الضروري أن ينتمي إلى مهنة يرتكب من خلالها الفعل الإجرامي كما هو الحال في جرائم ذوي الياقات البيضاء[3] . كما يتفق مجرمو المعلوماتية مع ذوي الياقات البيضاء في أن الفاعل في الحالتين يبرر جريمته ، بل إنه لا ينظر إلى سلوكه باعتباره جريمة أو فعل يتنافى مع الأخلاق.

1 و قد علق المشرع الجزائري التعاون القضائي الدولي في مجال مكافحة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال على شرط احترام الاتفاقيات الدولية و الاتفاقيات الثنائية والمعاملة بالمثل ، أنظر سفيان سوير، المرجع السابق ، ص22

2 د. نائلة عادل محمد فريد قورة ، المرجع السابق ، ص54

3 Suthreland (Eduin H) ,White collar criminality , Gers (Gilbert) in white collar criminal The offender in business the professions, , 1968, p125

ويتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين و يرمز إليها الأستاذ Parker بكلمة S.K.R.A.M و هي تعني :

- **المهارة Skills**،
- **المعرفة Knowledge**،
- **الوسيلة Resources**،
- **السلطة Anthority**،
- **و أخيرا الباعث Motives**[1].

وتعد المهارة : المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي، و التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال ،أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات ،أو بمجرد التفاعل الاجتماعي مع الآخرين. إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال. بل إن الواقع العملي قد أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال.

أما المعرفة : فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها و مكانيات نجاحها و احتمالات فشلها، إذ أن المجرم المعلوماتي باستطاعته أن يكون تصورا كاملا لجريمته، كون المسرح الذي تمارس فيه الجريمة المعلوماتية هو النظام المعلوماتي ، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها و ذلك قبل تنفيذ جريمته.

أما الوسيلة: فيراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته ففيما يتعلق بالمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية هي في أغلب الحالات تتميز نسبيا بالبساطة و بسهولة الحصول عليها، كما يستطيع نظراً لمهارته ابتكارها ، إذ و أنه كلما كان النظام المعلوماتي غير مألوف و يتميز بالخصوصية كانت تشكل تحدياً للمجرم المعلوماتي و كانت الوسائل المتطلبة أكثر صعوبة[2]

1 Parker (Donn B) ، المرجع السابق ، ص114

2 د. نائلة عادل محمد فريد قورة ، المرجع السابق ، ص55

أما السلطة: فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي و التي تمكنه من ارتكاب جريمته ؛ قد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات و التي تعطي الفاعل مزايا متعددة كفتح الملفات و محو أو تعديل المعلومات التي تحتويها أو مجرد قراءتها أو كتابتها. و قد تتمثل هذه السلطة في الحق في استعمال الحاسب الآلي أو إجراء بعض التعاملات.

و أخيرا يأتي الباعث وراء ارتكاب الجريمة، الذي قد لا تختلف في كثير من الأحيان عن الباعث لارتكاب غيرها من الجرائم الأخرى ، فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمة المعلوماتية[1] ، ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب و تخطي حواجز الحماية المضروبة حوله، و أخيرا الانتقام من رب العمل أو أحد الزملاء، حيث يفرق مرتكبي هذه الجرائم بين الأضرار بالأشخاص الأمر الذي يعدونه غاية اللاأخلاقية ،و بين الاضرار بمؤسسة أو جهة في استطاعتها اقتصاديًا تحمل نتائج تلاعبهم، و هو ما يطلق عليه أعراض روبن هود The Roben **Hood Syndrome**[2]. و بناءا على ما تقدم يمكن أن نقسم مجرمي المعلوماتية **Cyber criminals** إلى مجموعة من الطوائف المختلفة، حيث أسفرت الدراسات المختلفة في هذا المجال عن وجود سبعة أنماط من مجرمي المعلوماتية و يمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة و تتمثل هده الطوائف فيما يأتي[3] :

- **تضم الطائفة الأولى Pranksters** : الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية و المزاح مع الآخرين، بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم ، و يندرج تحت هذه الطائفة بصفة خاصة صغار مجرمي المعلوماتية (الأحداث).

- **أما الطائفة الثانية Hackers** : فهي تضم الأشخاص الذين يهدفون إلى الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها و كسر الحواجز الأمنية الموضوعة لهذا الغرض ،و ذلك بهدف اكتساب الخبرة، أو بدوافع الفضول أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.

- **وتتضمن الطائفة الثالثة "Malicious Hackers** : هدفهم إلحاق خسائر بالمجني عليهم دون أن يكون الحصول على مكاسب مالية من ضمن هذه الأهداف ،و يندرج تحت هذه الطائفة الكثيرون من مخترقي فيروسات الحاسبات الآلية و موزعيها.

---

1 و يرى البعض أن أغلب مجرمي المعلوماتية ليس لديهم أطماع مادية بقدر ما يحاولون حل مشكلات مادية تواجههم لا يستطيعون حلها باللجوء إلى الجرائم الأخرى أنظر ،Parker (DonnB)ouvrage ، المرجع السابق ، ص142

2 د هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1995، ص38

3 د نائلة عادل محمد فريد قورة ، المرجع السابق ، ص 58

- **أما الطائفة الرابعة Personnel Problem Solvers** : فهم الطائفة الأكثر شيوعا بين مجرمي المعلوماتية ،فهم يقومون بارتكاب جرائم المعلوماتية التي تلحق بالمجني عليهم خسائر و لا يستطيع حلها بالوسائل الأخرى بما فيها اللجوء إلى الجريمة التقليدية.

- **وتتضمن الطائفة الخامسة Career Criminals** مجرمي المعلوماتية الذين يبتغون تحقيق الربح المادي بطريقة غير مشروعة، بحيث ينطبق على فعالهم وصف الجريمة المنظمة ،أو على الأقل يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل ؛و يقترب المجرم المعلوماتي المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي[1] .

- **أما الطائفة السادسة Extreme Advocates** : فتدخل في عدادها الجماعات الإرهابية أو المتطرفة ،و التي تتكون بدورها من مجموعة من الأشخاص لديهم معتقدات و أفكار اجتماعية أو سياسية أو دينية و يرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي، و يركز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص و الممتلكات من أجل لفت الأنظار إلى ما يدعون إليه؛ وان اعتماد المؤسسة المختلفة داخل الدول على أنظمة

الحاسبات الآلية في إنجاز أعمالها و الأهمية القصوى للمعلومات التي تحتويها في أغلب الحالات قد جعل من هذه الأنظمة هدفًا جذابًا لهذه الجماعات؛ و من الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات الإرهابية المعروفة في أوربا باسم "The Red Brigades" بتدمير ما يزيد عن 60 مركزا للحاسبات الآلية خلال الثمانينات لتلفت النظر إلى أفكارها و معتقداته[2].

- **أما الطائفة السابعة The Criminally Negligent** و التي تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحاسبات الآلية، ألا و هي الإهمال الذي يترتب عليه في مجال الحاسبات الآلية و في أغلب الأحيان نتائج خطيرة قد تصل إلى حد إزهاق الروح؛ ففي نيوزلندا على سبيل المثال قام اثنان من مبرمجي الحاسبات الآلية بتغيير في أحد البرامج التي تحدد خط سير إحدى الطائرات و لم يتمكنوا من إبلاغ قائد الطائرة لهذا التغيير مما ترتب عليه تحطم الطائرة لاصطدامها بأحد الجبال و قتل 60 راكبا على متنها، و لقد تمت محاكمة المتهمين بتهمة القتل الخطأ.

1 Parker Donn B ، المرجع السابق ، ص147

2 د نائلة عادل محمد قورة ، المرجع السابق ، ص 63

المبحث الأول : أنواع الجرائم المعلوماتية

تعدد محاولات الفقه لتحديد أنواع الجرائم المعلوماتية و ذلك لصعوبة حصر هذه الأنواع بصفة دقيقة بالنظر لحداثة ظهور هذه الجريمة و كذا عدم وجود تعريف عام متفق عليه و كذا تحديد مجالها بالنظر للتطور التكنولوجي في كل صوره ، و نظراً لذلك تعددت تقسمات الجرائم المعلوماتية للجرائم المعلوماتية إلى طوائف مختلفة تتميز كل منها بسمات خاصة بها بالنظر إلى اختلاف المعيار المعتمد في التقسيم ، فهناك من قسم الجرائم المعلوماتية إلى ثلاث طوائف تتمثل في جرائم الحاسب الآلي الاقتصادية وآلي التي تهدد المصالح القومية أو السلامة الشخصية للأفراد[1].

و قسمها آخرون بالاعتماد على معيار أنماط السلوك المختلفة التي تمثل الجريمة المعلوماتية و مدى اتفاقها أو اختلافها مع القواعد التي تحكم القانون الجنائي إلى ثلاث طوائف تتمثل في الدخول و الاستعمال غير المصرح بهما لنظام الحاسب الآلي ، أما الثانية تتمثل في الاحتيال المعلوماتي و سرقة المعلومات و الطائفة الأخيرة تتمثل الجرائم التي يساعد الحاسب الآلي على ارتكابها[2] ، لكن و من الملاحظ أن هذه التقسيمات لم تراع بعض أو كل خصائص هذه الجرائم من خلال موضوعها و الحق المعتدى عليه لاعتمادها على معيار واحد للتقسيم متناسية معايير أخر، بحيث يرى بعض من الفقهاء أنه يجب مراعاة في كل محاولة للتقسيم اعتباران و هما

- التطور المستمر للجريمة المعلوماتية
- معيار الجريمة المعلوماتية نفسها أي كل ما يدخل في إطار المعلوماتية و ما يخرج منها (E/S)[3]

---

[1] Lucas ، المرجع السابق ، ص 27

[2] د نائلة عادل محمد قورة ، المرجع السابق ، ص256

[3] on appelle **Entrées–Sorties** les échanges d'informations entre le processeur et les périphériques qui lui sont associés , on appelle **Entrées–Sorties** les échanges d'informations entre le processeur et les périphériques qui lui sont associés, Les *sorties* sont les données émises par l'unité centrale à destination d'un périphérique (disque, réseau, écran…). David Fayon, L'informatique, Vuibert, 1999 p 15 ،

و مراعاة للاعتبارين السابقين ذهب الفقه الراجح إلى تقسيم الجرائم المعلوماتية إلى طائفتين رئيسيتين على محل الجريمة المعلوماتية التي تنصب على معطيات الحاسوب التي تطال المعلومات نفسها بالإضافة إلى الاعتماد على الدور الذي يقوم به الحاسب الآلي في الجريمة إذ تقتضي في ارتكاب التي النشاطات الإجرامية استخدام الحاسب الآلي.

و تتمثل الطائفة الأولى في الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي أما الطائفة الثانية تتمثل في الجرائم المعلوماتية الواقعة على النظام المعلوماتي ، و هذا ما سنتطرق إليه من خلا المطلبين المواليين.

المطلب الأول : الجرائم الواقعة بواسطة النظام المعلوماتي

يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية و يعد فيها الحاسب الآلي في هذه الطائفة من الجرائم الوسيلة التي تسهل بها النتيجة الإجرامية و مضاعفة جسامتها، حيث يهدف الجاني عادة من وراء ارتكاب هذه الجرائم تحقيق ربح مادي بطريقة غير مشروعة من خلال اعتدائه على أموال الغير ، فيستخدم المجرم المعلوماتي النظام المعلوماتي ذاته كوسيلة لتنفيذ جريمته.[1]

كما تتعدد صور الجريمة المعلوماتية المرتكبة باستخدام النظام المعلوماتي بعضها ذكرها المشرع الجزائري ، في حين أن البعض الآخر رأى الفقه امكانية تطبيق القواعد القانونية القائمة في قانون العقوبات عليها و سنتعرض لهذه الأفكار من خلال الفرعين التاليين.

الفرع الأول : الجرائم المعلوماتية الواقعة على الأشخاص

تقع هذه الجرائم على الأشخاص من خلال نوع الحق المعتدى عليه و دور النظام المعلوماتي في اقترافها.

و تتمثل هذه الاعتداءات في الجرائم الواقعة على حقوق الملكية الفكرية و الأدبية ، أما النوع الثاني تكمن في الجرائم الواقعة على حرمة الحياة الخاصة للفرد و كما نشير أنه هذه الحرمة يدخل في نطاقها أمواله.

1 د نائلة عادل محمد قورة ، المرجع السابق ، ص265

أولاً: طائفة الجرائم المعلوماتية الواقعة على حقوق الملكية الفكرية و الأدبية

يمكن أن يكون النظام المعلوماتي و سيلة فعالة للاعتداء على الملكية الفكرية و الأدبية ، و مثال ذلك استخدام النظام المعلوماتي في السطو على قاعدة معلومات التي تتضمن معلومات أياً كان نوعها ملكاً لشخص آخر دون إذنه أو علمه كمن يعتدي بنسخ مقال أو بحث في صدد الإنجاز من جهاز أو دعامات التخزين **les supports de stockage**[1] أخرى دون إذن صاحبها و ينسبها لنفسه حيث تمثل اعتداء على حق من حقوقه و الأدبية و منها المادية كون أن للمعلومات قيمة من خلال نشرها أو تسويقها ، و يندرج ضمن الحقوق الفكرية كذلك براءات الاختراع أذ تمثل فكرة للمخترع تحتوي على حق معنوي و آخر مالي للمخترع[2].

وقد نص المشرع الجزائري على حقوق الملكية و الفكرية و براءات الاختراع من خلال عدة نصوص قانونية نذكر منها المادة 38 من الدستور الجزائري التي تنص على " حرية الابتكار الفكري و الفني و العلمي مضمون للمواطن".

كما أن حقوق المؤلف يحميها القانون من خلال الامر رقم 05/03 المؤرخ في 19 07 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة و كذا الامر 07/03 المؤرخ في 19 07 2003 المتعلق ببراءة الاختراع حيث لا يجوز حجز اي مطبوع أو تسجيل أو اية وسيلة أخرى من وسائل التبليغ و الاعلام إلا بمقتضى أمر قضائي.

ثانياً: طائفة الجرائم المعلوماتية الواقعة على الحياة الخاصة

لقد كفلت جل الدول الحياة لمواطنيها بالحماية و قد حذا الدستور الجزائري بموجب المادة 39 من الدستور الجزائري "لا يجوز انتهاك حرمة حياة المواطن الخاصة ، و حرمة شرفه ، و يحميهما القانون ، سرية المراسلات و الاتصالات الخاصة بكل أشكالها مضمونة" كما يدخل في هذه الحماية حماية الأموال و الممتلكات.

1 Les supports de stockage de grande capacité, autre que le papier, permettant l'enregistrement de données، David Fayon ، المرجع السابق، ص21

2 أحمد خليفة الملط ، المرجع السابق، ص 184

ولا شك أن الحاسبات الآلية بما لها قدرة فائقة على تخزين مقدار كبير من المعلومات ، و لأهمية المعلومات التي تحتويها هذه الانظمة '، أصبحت هذه الحسابات هدفاً لمل لها من دور مهم في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مادية و معنوية مختلفة.[1]

و عليه يمكن استخدام النظام المعلوماتي في الاعتداء على حرمة الحياة الخاصة أو على الحريات العامة للفرد، كأن يقوم شخص بإعداد ملف معلوماتي يحتوي على معلومات تخص شخص آخر بدون علمه أو إذنه ، كما يقوم بنشر معلومات على شكل صور أو حقائق من خلال اختراقه لحساب شخص و تشويه السمعة أو الاطلاع على معلومات بعلم الشخص المعني و يقوم بحفظها و اطلاع الغير عليها أو أسرار مكتوبة أو سير ذاتية ، مذكرات قصد التشهير بشخص أو جماعة معينة أو بيعها لتحقيق مصالح مختلفة كالحصول على عائد مادي أو للضغط على أصحابها مقابل القيام بعمل أو الامتناع عنه[2].

كما تقع هذه الجرائم لإفشاء الأسرار سواء كانت الاسرار عامة تتعلق بالأفراد و المؤسسات المختلفة أو تخص مصالح الدولة و نظام الدفاع عنها و الأسرار المهنية.

و هذه الجرائم تسبب أضرار لأصحابها لذا حرص المشرع الجزائري على حماية الاسرار من خلال الباب الأول المتعلق بالجنايات و الجنح ضد الشيء العمومي من المادة 61 إلى المادة 96 مكرر من قانون العقوبات الجزائري بالإضافة للمادة 394 مكرر 03 من نفس القانون التي نصت " تضاعف العقوبات المنصوص عليها في هذا القسم[3] إذا استهدفت الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام ، دون إخلال بتطبيق عقوبات أشد" حيث جذا المشرع الجزائري مختلف التشريعات لا سيما عندما يكون إفشاء هذه الأسرار المتعلقة بالدفاع الوطني.

1 د نائلة عادل محمد قورة، المرجع السابق ، ص 275

2 د أحمد خليفة الملط ، المرجع السابق ، ص 190

3 القسم السابع تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات من قانون 04-15 مؤرخ في 10 نوفمبر 2004 ، الجريدة الرسمية، العدد 71، 10 نوفمبر 2004

كما تعاقب مختلف التشريعات كل من يقوم بالدخول غير المصرح له إلى النظام المعلوماتي و إفشاء معلومات توجد داخلها ، حيث حمت تلك التشريعات الأسرار المهنية حيث ألزمت أصحاب المهن على غرار المحامي و الطبيب بالمحافظة على الأسرار التي يقرها له الزبون أو العميل[1].

الفرع الثاني : الجرائم المعلوماتية الواقعة على النظم المعلوماتية الأخرى

هذا النوع من الجرائم لا يستلزم تدخلاً لإتلاف الوظائف التقنية للنظام المعلوماتي و لا تعديلا على المعلومات المعالجة ، بل يقتصر في غالب الأحيان الولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية ، أو استخدام أداة الكترونية معينة تسمح بالتقاط المعلومات و التصنت عليها لدى النظم المعلوماتية الأخرى.

أولاً: الولوج غير المشروع للمعلومات المعالجة آلياً

تقوم هذه الصورة بوجود المجرم داخل احد المراكز المعلوماتية بهدف الولوج إلى المعلومات التي تمت معالجتها آلياً و الاطلاع عليها دون تصريح و قد يكون هذا الولوج إما مباشرًا أو غير مباشر.

أما المباشر فيعد من أكثر الأفعال المرتكبة و أسهلها تنفيذاً و يتخذ عدة صور إذ يستطيع الجاني الاستيلاء على المعلومات المخزنة لدى الأنظمة بعدة طرق باستخدام آلة الطباعة أو بالقراءة المباشرة أو باستخدام مكبر الصوت ، و من أمثلة ذلك الولوج المباشر ، قيام شخص سابق بأحد البنوك الأمريكية الذي كان يعمل في النظام المعلوماتي الخاص بالبنك نقل معلومات المالية المخزنة في النظام و نقلها لرئيسه الجديد بعد حصوله على كلمة السر من زميل سابق له[2].

و أما الولوج غير المباشر ظهر بظهور تقنيات مستحدثة ، لها الصلة بالنظام المعلوماتي كالمعالجة عن بعد ، إذ هذه التقنيات أدت إلى نشوء مخاطر جديدة نتيجة للإمكانيات المستحدثة للولوج و الاستفسار عن بعد من المراكز المعلوماتية ،

1 د أحمد خليفة الملط ، المرجع السابق ، ص 200

2 د محمد سامي الشوا ، المرجع السابق ، ص 67

إذ أنه أثناء بثها تكون عرضة للالتقاط و التسجيل غير مشروعين في كل فترة من فترات هذا التحويل ما بين المرسل و الملتقط [1] ، و لعل من أبسط هذه التقنية هي تقنية البلوتوث Bluetooth[2].

ثانياً: إساءة استخدام البطاقات الائتمانية

أدى إدخال النظام المعلوماتي في مجالات عمليات البنوك إلى ظهور هذا النوع الجديد من الجرائم المعلوماتية ، التي تعد من أخطر الجرائم لاسيما في المجتمعات التي تتسم نظمها البنكية بدرجة عالية من التطور و الحداثة ، و يتخذ هذا النوع من الجرائم على صورتين :

أولاهما في الاساء في استخدام الحسابات المصرفية أو للبطاقات الائتمانية و ذلك عن طريق عدم احترام العميل المصدر إليه البطاقات الائتمانية شروط العقد المبرم بينه و بين المؤسسة المصرفية كأن يستعمل بطاقة منتهية الصلاحية أو بطاقة تم إلغاؤها أو الشراء بأكثر من قيمتها ...[3]

و أما الصورة الثانية تتمثل في استخدام الغير لتلك الحسابات أو البطاقات كأن يقوم المجرم استعمال البطاقة للحصول على سلع أو خدمات او سحب مبالغ مالية بموجبها من أجهزة التوزيع الآلي مثلاً أو السحب باستخدام بطاقات ائتمانية مزورة[4].

[1] د أحمد خليفة الملط ، المرجع السابق ، ص 196

[2] Bluetooth est une spécification de l'industrie des télécommunications. Elle utilise une technique radio courte distance destinée à simplifier les connexions entre les appareils électroniques ، David Fayon، المرجع السابق، ص25

3 د أحمد خليفة الملط ، المرجع السابق ، ص 192

4 د أحمد خليفة الملط ، المرجع نفسه ، ص 196

المطلب الثاني : الجرائم الواقعة على النظام المعلوماتي

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتي هناك نوع آخر من الجرائم المعلوماتية بالتصنيف الذي يقوم على محل الجريمة و يتمثل في الجرائم الواقعة النظام المعلوماتي نفسه التي قد تستهدف إما المكونات المادية للنظام المعلوماتي أو المكونات المنطقية و المعلومات المدرجة بالنظام .

و هذا ما سنتطرق إليه بشيء من التفصيل من خلال الفرعين التاليين :

الفرع الأول : جرائم الاعتداء على المكونات المادية للنظام المعلوماتي

يقصد بالمكونات المادية للنظام المعلوماتي تلك الأجهزة و المعدات الملحقة به و التي تستخدم في تشغيله كالأسطوانات و الكابلات ... إلخ ، و كنتيجة للطبيعة المادية لهذه المكونات فالاعتداء عليها يكون عن طريق جرائم عادية و تقليدية [1] ، كأن تكون محلاً للسرقة أو خيانة الأمانة أو الإتلاف العمدي كالحرق و التكسير أو خربشة الشريط و إفساد الأسطوانات و يترتب على ذلك ضياع للمعلومات و خسائر كبيرة[2].

و من أمثلة ذلك ما حدث في فرنسا حيث أدى إتلاف معدات مؤسسة كبيرة متخصصة في بيع الأنظمة و توثيق المعلومات الحسابية إلى خسائر مادية معتبرة حصلت ب 5 ملايين يورو[3].

و يرى البعض من الفقهاء أنه يندرج ضمن هذه الطائفة من الجرائم سرقة وقت الآلة، فقد يلجأ العاملين بالنظام المعلوماتي إلى استخدامه في أعمال خاصة بهم ، و عليه تكون واقعة السرقة منصبة على وقت الجهاز الذي يمكن تقويمه ماليا و ليس على الأشياء المادية بمعنى الكلمة ، و تجدر الإشارة أن خطورة واقعة السرقة لا تكمن في الشيء المسروق لضآلة قيمته ، بالمقارنة بما تحتويه هذه المكونات المادية من معلومات تقدر خسائرها بأموال طائلة.

1 د أحمد خليفة الملط ، المرجع السابق ، ص176

2 د ذكي ذكي امين حسونة ، جرائم الكمبيوتر و الجرائم الأخرى ، دار النهضة، القاهرة، ص471

3 Rose Philipe ، المرجع السابق ، ص 58

الفرع الثاني : جرائم الاعتداء على المكونات المنطقية للنظام المعلوماتي

تستلزم هذه الطائفة من الجرائم المعلوماتية معرفة فنية عالية في مجال البرمجة ، و قد تقع هذه الجرائم إما على البرامج التي منها البرامج التطبيقية أو برامج التشغيل.

أولاً : الجرائم الواقعة على البرامج التطبيقية

يقوم الجاني في هذه الصورة بتحديد البرنامج أولاً ثم التلاعب فيه لتحقيق أكبر قدر من الاستفادة المادية.

أ- **تعديل البرنامج** : الهدف الرئيسي من تعديل هذه البرامج يتمثل في اختلاس النقود و تكثر هذه الجرائم في مجال الحسابات[1].

ومن أمثلة ذلك قيام مبرمج في أحد البنوك الأمريكية بإدارة الحسابات بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات و قام بقيد المصاريف الزائدة في حساب خاص به أطلق عليه اسم Zzwick و حصل على إثر ذلك على مئات الدولارات كل شهر و كان من الممكن أن يستمر هذا العمل الإجرامي لولا أن البنك أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافئ أول و آخر عميل ليكتشف بعدها حقيقة هذا المبرمج[2].

ب- **التلاعب في البرامج** : يأخذ التلاعب في البرامج عدة أشكال فقد يتم عن طرق استعمال القنبلة المنطقية[3] أو عن طريق قيام أحد المبرمجين زرع برنامج فرعي غير مسموح به في البرنامج الأصلي يسمح له بالدخول غير المشروع في العناصر الضرورية لأي نظام معلوماتي ، و بهذا يصعب اكتشاف هذا البرنامج لصغره و دقته.

---

1 د أحمد خليفة الملط ، المرجع السابق ، ص 173

2 Duleroy ,Les escrocs a l'informatique ,le nouvel économiste , octobre 2002 , p 202

3 و هي عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو في كل فترة زمنية منتظمة و يتم وضعه في شبكة معلوماتية للتسهيل بالقيام بعمل غير مشروع، د أحمد خليفة الملط ، المرجع السابق ، ص 545

ثانياً: الجرائم المعلوماتية الواقعة على نظام التشغيل

تعد برامج التشغيل هي المسؤولة عن عمل النظام المعلوماتي ، من حيث قيامها بتنظيم و ضبط و ترتيب المعلومات الخاصة بالنظام.

وتقوم الجريمة في هذه الصورة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي[1] ، ويتحقق هذا النوع من الجرائم في نوعين :

أ- **المصيدة** : تتمثل هذه الصورة من خلال إعداد برنامج به أخطاء و عيوب عمداً ، لا يكتشف بعضها عند استخدام البرنامج ، إذ يترك المبرمج ممرات خيالية و تفرعات في البرنامج حتى يستطيع بعدها تنفيذ التعديلات الضرورية للولوج داخل النظام المعلوماتي و الوصول إلى كل المعلومات التي تحتويها الذاكرة.

ب- **تصميم برنامج وهمي** : و تقوم هذه الصورة من خلال قيام المبرمج بوضع برنامج يصعب اكتشافه معد خصيصاً لارتكاب الجريمة ، ومن أمثلة ذلك قيام إحدى شركات التأمين الأمريكية بواسطة مبرمجيها من تصميم برنامج وهمي يقوم بتصنيع وثائق تأمين لأشخاص و همين بلغ عددهم 000 46 بهد تقاضي هذه الشركة من اتحاد شركات التأمين عمولات من نظيراتها[2].

ثالثاً: جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتي

للمعلومة في حد ذاتها باعتبارها الأساس الذي يقوم عليه النظام المعلوماتي ، و بهذا اصبحت هدفاً للجريمة المعلوماتية من خلال التلاعب فيها أو عن طريق إتلافها.

1 د أحمد خليفة الملط ، المرجع السابق ، ص 175

2 Duleroy ، المرجع السابق ، ص 210

أ- **التلاعب في المعلومات** : يتم التلاعب في المعلومات الموجودة داخل النظام بطريق المباشر أو غير المباشر، أما الطريق المباشر يتم عن طريق ادخال معلومات بمعرفة المسؤول عن القسم المعلوماتي ، و يتم هذا التلاعب بإضافة معلومات غير مؤسسة كإضافة أسماء غير موجودين في العمل أو الإبقاء على مستخدمين تركو العمل...

في حين أن الطريقة غير المباشرة يتم عن طريق التدخل غير المباشر لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام احد وسائط التخزين أو الدعامات ، فقد قام في هذا الصدد أحد الموظفين بأحد فروع الشركة **Isoverst Gobain** بإرسال شريط ممغنط يحتوي على 139 إذن دفع ، و عند معالجته بالبنك تم رفض نسخه لعيب في الشريط ، و قد علق الخبراء أنه لو نجحت العملية لتم النصب على البنك بحوالي 21 مليون فرنك [1].

ب- **إتلاف المعلومات** : قد يهدف الجاني من خلال ارتكابه للجريمة المعلوماتية المخزنة داخل النظام ، و قد يأخذ هذا التلاف عدة صور الحذف التغير استبدال المعلومة ...إلخ

و يشكل استبدال المعلومة نوع من أنواع جرائم الغش و التزوير المعلوماتي و هو على درجة كبيرة من الخطورة لأنه في حال نجاحه يستمر لوقت طويل قبل اكتشافه و يتولد عيه اضرار كبيرة كتغير رقم بآخر أو اسم بغيره [2] ، فقد قام شخص يدعى Vladimir Loriblitt يعمل بوزارة المالية بتغير فواتير وهمية للنظام و تحويل ما تم سداده لحساب شركات وهمية الذي جنى منها 10 ملايين دولار قبل أن يتم اكتشافه[3].

أما محو المعلومات فهو من أسهل طرق الاتلاف كون أنه من خصائص الجرائم المعلوماتية في قدرة المجرم المعلوماتي من محو آثار الجريمة في فترة وجيزة لا تتعدى الضغط على زر بسيط في لوحة المفاتيح أو عن طريق الفأرة ، فمثلاً قام شخص باختلاس ما يقدر ب 00 61 دولار مرسلة من شركة تأمين إلى إحدى المراكز الجامعية عن طريق محو الحسابات القائمة في سجلات النظام المعلوماتي بالمركز و جعلها غير قابلة للتحصيل.

1 Duleroy ، المرجع نفسه ، ص 212

2 د أحمد خليفة الملط ، المرجع السابق ، ص 175

3 Duleroy ، المرجع السابق ، ص 215

تناولننا في هذا الفصل تعريف الجريمة المعلوماتية و وجدنا أن الفقه لم يتفق على تعريف موحد و جامه لها و ذلك بالنظر إلى حداثة هذا النوع من الجرائم، أظف إلى ذلك إلى الزاوية التي ينظر إلهيا كل واحد منهم عند تعريفه لها من توسع إلى تضيق، ومن تعريق تقني إلى تعريق قانوني، كما تطرقنا إلى السمات الخاصة التي تتميز بها الجريمة المعلوماتية عن غيرها من الجرائم الأخرى ووجدنا أنها جرائم عابرة للحدود و يعب اكتشافها و اثباتها كما أنها تتم بأسلوب لا يتسم بالعنف.

كما تناولنا أبرز سمات المجرم المعلوماتي و عرفنا أنه يتميز عن المجرم التقليدي بالمهارة و المعرفة و عدم ممارسة للعنف اثناء ارتكابه للجريمة و تناولنا كذلك أنواع الجريمة المعلوماتية التي يكون النظام المعلوماتي فيها محلاً للاعتداء و الجرائم التي تقع بواسطة هذا النظام المعلوماتي.

الفصل الثاني

مكافحة جرائم المعلوماتية

الفصل الثاني : مكافحة جرائم المعلوماتية

لقد شهد العالم في السنوات الأخيرة تطورًا غير مسبوق في مجالات الإعلام والاتصال نظرًا إلى توغل وانتشار وسائل التكنولوجيا والابتكارات المستحدثة في الأنشطة المعلوماتية ودخولها في جميع نواحي، الحياة بل أصبح العالم قرية صغيرة بفضلها ، وهو ما قد يترتب عليه الخطر الكبير على البنيات المختلفة جراء الاستخدام غير المشروع لهذه التقنيات و المساس بالحياة الخاصة للأفراد، والخطر الأكبر هو أن الجرائم المعلوماتية قد تستهدف الأمن القومي بارتكاب جرائم تمس جهات حكومية وأمنية، ليس هذا فحسب بل حتى الإضرار بالاقتصاد كونه أصبح يعتمد بصورة متزايدة على تقنية المعلومات الاقتصاد الرقمي مما قد يؤثر هذا الإجرام التقني تأثيرا كبيرا على اقتصاد الدولي و المحلي ، الأمر الذي أدى بمختلف إلى الإسراع من أجل محاولة التصدي لهذه الظاهرة الإجرامية المستحدثة ، فتظافرت الجهود من أجل إيجاد سبل مكافحتها بفعالية ز نجاعة أكثر.

يتضح جلياً خطورة هذا النوع من الجرائم ، حيث أن القوانين التقليدية المطبقة لم تعد مجدية نظراً لاختلاف الكبير بين الجرائم التقليدية و جرائم المعلوماتية التي يعود بالأساس إلى الطبيعة اللامادية لها و التي هي من أهم الصعوبات التي تعتري سبل مكافحتها وبفعل ما أثاره التطبيق القضائي لنصوص القوانين الجنائية على جرائم الحاسوب من مشكلات ، ولضمان عدم افلات الجناة من العدالة لعدم كفاية القوانين أو عجزها عن الانطباق على هذه الجرائم المستحدثة ، وصونًا لمبدأ الشرعية الذي يقضي بأن لا جريمة ولا عقوبة بغير نص قانوني، ، لهذه الأسباب ، ولمواجهة الخطر المحدق والخسائر الفادحة التي تسببها جرائم الحاسوب ، اتخذت المواجهة التشريعية لجرائم المعلوماتية ثلاثة مستويات :

أما المستوى الأول فهو المستوى الوطني ، فلقد سارعت دول العالم المتقدم التدابير اللازمة لمواجهة هذه النوعية من الجرائم، فبض هذه الدول حرصت على أن تُضَمن تشريعاتها بخصوص هذه الجرائم إما عن طريق نصوص مستقلة و مثال ذلك قانو اساءة استخدام الحاسب في المملكة المتحدة الصادر في 29 جوان 1990 ، و إما عن طريق تحديث قوانينها و إدماجها في قانون العقوبات ومن أبرز هذه النوعية فرنسا من خلال قانون العقوبات الجديد الصادر سنة 1992 و الذي أضاف فصلاً ثالثاً للباب الثاني من القسم الثالث تحت عنوان " انتهاكات نظم المعالجة الآلية للبيانات

atteintes aux systèmes de traitement autorisé de données Des " و يتكون هذا الفصل من المواد 1/321 إلى 7/323.[1]

و من بين المحطات التالية من محطات التجريم المعلوماتي في فرنسا فكانت عام 2004[2] عندما أضاف المشرع الفرنسي بموجبه جريمة أخرى هي جريمة التعامل في الوسائل التي تصلح أن ترتكب بها جريمة الدخول أو البقاء غير المصرح بها أو جريمة التلاعب بالمعطيات أو جريمة إعاقة وإفساد أنظمة المعالجة الآلية للمعطيات.

وتجدر الاشارة أن المشرع الجزائري قد حذا حذو المشرع الفرنسي من خلال تعديل قانون العقوبات و إدراج جرائم المعلوماتية من خلال تجريم أفعال المساس بأنظمة المعالجة الآلية للمعطيات من إحداث قسم جديد في قانون العقوبات هو القسم السابع (القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل لقانون العقوبات من المواد 394 مكرر إلى 394 مكرر7).[3]

و ثانيها على المستوى الاقليمي ، فلقد حرص المجلس الاوروبي على التصدي للاستخدام غير المشروع للكمبيوتر و شبكات المعلوماتية وفي عام 1989 نشر المجلس الأوروبي دراسة تضمنت توصيات تفعيل دور القانون لمواجهة الأفعال غير المشروعة عبر الحاسب وهي التوصية التي لحقتها دراسة أخرى في عام 1995 حول الإجراءات الجنائية في مجال الجرائم المعلوماتية، وعلى أساس المبادئ التي تضمنتها التوصيات قام المجلس الأوروبي في عام 1997 بتشكيل لجنة خبراء الجريمة عبر العالم الافتراضي وذلك بقصد إعداد اتفاقية في هذا الإطار و تجلى ذلك في اتفاقية بودابست[4] Convention on cybercrime و الموقعة في 23 نوفمبر 2001 و التي سنعكف على دراستها في المطلب الثاني من هذه الدراسة.

وثالثها على المستوى الدولي و تتمثل في جهود الامم المتحدة التي تبتذلها في هذا المضمار.

1. Clément ENDRELIN , Les moyens juridiques de lutte contre la cybercriminalité , Diplôme universitaire sécurité intérieur/extérieur dans l'Union Européen , 2011 , p76
2. القانون رقم 575 لسنة 2004 في 06/21 /2004 المتعلق بالثقة في الاقتصاد الرقمي
3. نعيم سعيداني ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة ماجستير حقوق ، جامعة الحاج لخضر باتنة، الجزائر، 2012 ، ص79
4. نعيم سعيداني ، المرجع نفسه ، ص 85

و عليه فسنقسم هذا الفصل من الدراسة إلى مبحثين ، أما المبحث الأول فسنخصصه الجهود الدولية لمكافحة جرائم المعلوماتية ففي المطلب الأول على المستوى الدولي أما المطلب الثاني على المستوى الاقليمي (المجلس الاوروبي و اتفاقية بودابست).

المبحث الثاني فسنتطرق إلى جهود المشرع الجزائري في مجال مكافحة جرائم المعلوماتية من خلال قانون العقوبات في المطلب الاول ، أما المطلب الثاني من خلال قانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال.

المبحث الأول : الجهود الدولية لمكافحة الجرائم المعلوماتية

تتسم جرائم المعلوماتية بالنظر لطبيعتها بطابع دولي ، لكن اختلاف التشريعات في تأسيس اختصاصها الجنائي نتيجة تعدد الأسس التي يقوم عليها هذا الاختصاص قد يؤدي إلى تنازع الاختصاص بين الدول ، فقد يحدث أن ترتكب الجريمة المعلوماتية في دول معينة ، و يكون المجرم المعلوماتي مرتكب هذه الجريمة أجنبياً ، فتخضع هذه الجريمة للاختصاص الجنائي للدولة الأولى استناداً إلى مبدأ الاقليمية ، وتخضع كذلك لاختصاص الدول الثانية على أساس مبدأ الاختصاص الشخصي في جانبه الايجابي.[1] و قد تكون الجريمة المرتكبة على اقليم الدولة من الجرائم التي تهدد أمن و سلامة دولة أخرى ، فتخضع للاختصاص الجنائي الاقليمي من جهة ، و تخضع لاختصاص الدولة المجني عليها استناداً إلى مبدأ الاختصاص العيني من جهة أخرى ، كما تثور فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الاقليمية ، كما لو قام الجاني ببث معلومات غير مشروعة على اقليم دولة معينة و تم الاطلاع عليها في دولة أخرى، فوفقاً لمبدأ الاقليمية فإن الاختصاص الجنائي و القضائي يثبت لكل دولة من الدول التي مستها الجريمة، سواء تلك التي وقع فيها الفعل الإجرامي (فعل البث) أو تلك التي حدثت نتيجة الفعل فيها (تلقي المعلومات غير المشروعة) ، الأمر الذي يؤدي إلى الاطاحة بمبدأ عدم جواز محاكمة الشخص عن الفعل الواحد أكثر من مرة ، و لذلك لا بد أن يكون هناك تعاون دولي يتفق مع طبيعة جرائم المعلوماتية التي تتميز بطابع خاص يقتضي أن تكون هناك ردود فهل سريعة لأن هذا التنسيق الفعال و العاجل يساعد على الحد من الأضرار الناجمة عن هذه الجرائم و كذلك تجنب المجرم المعلوماتي الافلات من العقاب و مثال ذلك ما

1. د جميل عبد الباقي الصغير ، الجوانب الاجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة ،2002 ، ص 73

قام به "أونيل دو غوزمان" الذي استخدم فيروس "أحبك I love you "[1] سنة 2000 الذي انتشر في كل أنحاء العالم عن طريق البريد الالكتروني حيث قدرت الخسارة ب 7 مليارات دولار[2] .

المطلب الأول : على المستوى الدولي

و إذا كان التعاون الدولي هو الآلية الفعال لمكافحة جرائم المعلوماتية ، فإن هذا التعاون يقتضي التخفيف من غلو الفوارق بين الأنظمة العقابية الداخلية لأن التباعد بين هذه الانظمة يجعل المجرم المعلوماتي يبحث عن الأنظمة الأكثر تسامحاً (قضية دو غوزمان التي أشرنا إليها) ، و لذلك أبرمت العديد من الاتفاقيات الدولية في مجال التعاون الدولي من أجل مكافحة جرائم المعلوماتية و تظهر معالم هذا التقارب في قبول حالات تفويض الاختصاص في اتخاذ اجراءات التحقيق و جمع الأدلة و تسليم و الاعتراف بالأحكام الجنائية ، بحيث أن هذا القانون الدولي لا ينال من سيادة الدولة ، بل بالعكس عدم التعاون يزيد من التباعد بين الأنظمة العقابية مما يساعد على تزايد هذه النوعية من الجرائم.

و في اطار دراسة حالة تعد من أبرز الأمثلة لأهمية التعاون الدولي في مجال مكافحة جرائم المعلوماتية هي عملية كاتريك Catterick Operation[3] و تتعلق هذه العملية بالابتزاز الذي قامت به شركات القمار عبر الإنترنت في الفترة من مايو إلى أكتوبر 2004 وفي هذه العملية، كان المجرمون يرسلون إلى إحدى الشركات يطلبون منها أموالا، مهددين إياها بأن يشنوا على موقعها "هجمات حجب الخدمة الموزعة" في حالة امتناعها عن الدفع، وتحدث هذه الهجمات بأن تزور آلاف أو مئات الآلاف من أجهزة الكمبيوتر من جميع أنحاء العالم موقعا معينا في الوقت نفسه،

1. هي دودة حاسوب ضربت العديد من أجهزة الكمبيوتر في عام 2000، عندما تم إرسالها كمرفق برسالة بريد إلكتروني مع النص "I LOVE YOU" في عنوان الرسالة الدودة وصلت في صناديق البريد في 4 مايو 2000، مع هذا العنوان البسيط "I LOVE YOU" ومرفق ."LOVE-LETTER-FOR-YOU.txt.vbs" عند فتح المرفق ،ترسل الدودة نسخة من نفسها للجميع في قائمة العناوين، متنكرة في زي للمستخدم. كما أنها تحدث العديد من التغييرات الضارة لنظام المستخدم. ويكيبيديا، فيروس أحبك 2014/05/14، فيروس أحبك http://ar.wikipedia.org/wiki/

2. راسل تاينر، أهمية التعاون الدولي في منع جرائم الإنترنت، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19 06 2007 ، المملكة المغربية، ص 112

3. راسل تاينر ، المرجع نفسه ، ص 114

ما يؤدي إلى تدمير الموقع و بعد تنفيذها للهجمات تعرض حوالي 57 شركة في أنحاء العالم، منها 10 شركات بالمملكة المتحدة، تجاوزت خسائرها 30 مليون جنيه إسترليني .وبالإضافة إلى الأثر الذي تتعرض له المواقع نفسها، فإن مقدار البيانات التي يتم توجيهها عبر قسم من الوصلات الرئيسة لشبكة الإنترنت يكاد يتسبب في تدمير هذه المواقع. و مع مباشرة التحقيقات لكل من المملكة المتحدة والولايات المتحدة باعتبارهما الأكثر تضرراً وقد قادتهم التحريات التي تمت بين أجهزة الشرطة في البلدين إلى لاتفيا، حيث قامت قوات الشرطة لديها بعملية مراقبة سرية أسفرت عن إلقاء القبض على 10 أشخاص يُشتَبه في تورطهم حيث تم تحديد موقع جهاز كمبيوتر تم اختراقه في مدينة بالاكوفو في روسيا.

بدأت الشرطة الروسية على إثره بإجراء تحقيق بمفردها تحول بعد ذلك إلى تحقيق فعال مشترك؛ تم توقيف عدد من الأشخاص، وضبط عدد من أجهزة الكمبيوتر ووجهت إلى المتهمين تهم الابتزاز ونشر فيروسات علي أجهزة الكمبيوتر، وحُكم عليهم بالسجن ثماني سنوات.

وعليه يجد التعاون الدولي في مجال مكافحة جرائم المعلوماتية بصفة عامة تبريره في بعض الاعتبارات منها[1] :

- أنه يعتبر خطوة على طريق تدويل القانون الجنائي ، ذلك أن ثمة قواعد موضوعية و اجرائية تهيمن على أذهان العديد من مشرعي هذه الحقبة ومن شأن تشابه هذه القواعد أن يخلق نوعاً من التقارب بين التشريعات الحالية.
- أنه يعتبر من قبيل التدابير المانعة من ارتكاب هذه النوعية من الجرائم ، لان المجرم المعلوماتي سوف يجد نفسه محاطاً بسياج مانع من الافلات من المسؤولية الجنائية عن الجريمة التي ارتكبها ، أو من العقوبة التي حكم عليه بها . فإذا ارتكب جريمته في دولة ما و تمكن من الهروب إلى دولة أخرى فإنه سوف يكون عرضة للقبض عليه أو ترحيله إلى البلد الأول ، و من شأن كل ذلك أن يجعل المجرم المعلوماتي يعزف عن سلوك سبيل الجريمة.

إن التعاون الدولي في مجال مكافحة الجريمة المعلوماتية قد يأخذ مظهران، الأول يتعلق بضرورة التعاون في إنفاذ القانون لملاحقة ومتابعة ومعاقبة المجرمين بعد ارتكاب الجريمة والتي تعبر اختصاصات قضائية متعددة ذات نظم قانونية مختلفة، ويتمثل

1. د جميل عبد الباقي الصغير ، المرجع السابق ، ص 74

في التعاون القضائي. و الثاني يتعلق بالسعي إلى اتخاذ الإجراءات والآليات ذات الطبيعة التقنية الفنية التي تكفل منع ارتكاب الجريمة في مرحلة التنفيذ[1].

أما التعاون القضائي الدولي في مواجهة الجريمة المعلوماتية يعد الآلية الرئيسية للكفاح ضد ها فإن فعالية التحقيق والملاحقة القضائية غالبا ما تقتضي الحاجة إلى مساعدة من السلطات في البلد الذي كان منشأً للجريمة، أو من السلطات في البلد الذي عبر من خلاله النشاط المجرم وهو في طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة، فقد يكون مرتكب الجريمة المعلوماتية من جنسية دولة ما مستعملا في جريمته حواسيب موجودة في دولة أخرى وتقع آثار جريمته في دولة ثالثة فمن البديهي أن يقف مبدأ السيادة ومشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها، لذا فإن التحقيقات في الجرائم المعلوماتية ومتابعة مرتكبيها قضائيا تؤكد على أهمية المساعدة القضائية[2] المتبادلة بين الدول.[3]
وتتخذ المساعدة القضائية الدولية عدة صور أهمها:

- **تبادل المعلومات**: يولي المجتمع الدولي لتبادل المعلومات أهمية قصوى بوصفه وسيلة لمكافحة الإجرام عموما والجريمة المعلوماتية خصوصا لما توفره المعلومات الصحيحة والموثوقة من مساندة لأجهزة تنفيذ القانون . ويشمل مبدأ تبادل المعلومات تقديم البيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة أجنبية وهي بصدد النظر في جريمة معلوماتية ما ، بحيث يسمح بالاتصال المباشر بين الأجهزة القضائية والأمنية في الدول المختلفة من أجل تبادل المعلومات المتعلقة بالجريمة والمجرمين[4].

- **نقل الإجراءات** :ويقصد بهذه الصورة قيام دولة ما بمقتضى اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد التحقيق في جريمة معلوماتية ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توفرت مجموعة من الشروط، أهمها

1. نعيم سعيداني ، المرجع السابق ، ص 92

2. تعرف المساعدة القضائية الدولية بأنها كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم، سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، مذكرة دكتوراه ،جامعة عين شمس، 1997 ، ص425

3. لقد نص المشرع الجزائري في القانون 04/09 المتعلق بالجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها المؤرخ في 5 أوت 2009 على مبدأ المساعدة القضائية الدولية المتبادلة في المادة 16 منه معتبرا أنه في إطار التحريات والتحقيقات القضائية الجارية لمعاينة الجرائم المعلوماتية يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني، نعيم سعيداني ، المرجع السابق، ص 89

4. وعلى المستوى التشريعي الوطني فقد نصت المادة 17 من قانون 04/09 على أن الدولة الجزائرية تستجيب لطلبات المساعدة القضائية الدولية الرامية لتبادل المعلومات وذلك في إطار الاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل ، نعيم سعيداني ، المرجع نفسه ، ص 90

التجريم المزدوج والذي يقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب نقل الإجراءات إليها بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها .بمعنى أن تكون مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة وأن تكون هذه الإجراءات ذات أهمية من شانها أن تؤدي دورا مهما في الوصول إلى الحقيقة. ولقد أقرت العديد من الاتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية، كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية[1] وكذا اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية في باليرمو سنة 2000.

– **الإنابات القضائية الدولية** : يقصد بهذه الصورة طلب اتخاذ إجراء قضائي من إجراءات الدعوى العمومية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك عند الفصل في مسألة معروضة لدى السلطة القضائية في الدولة الطالبة لتعذر قيامها بهذا الإجراء بنفسها[2].وتهدف هذه الصورة إلى تسهيل الإجراءات الجزائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية، التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى لسماع شهود أو إجراء تفتيش أو غيرها. ويحدث بدرجة متزايدة أن تشترط المعاهدات والاتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف أن تعين سلطة مركزية عادة ما تكون وزارة العدل ترسل إليها الطلبات مباشرة بدلا من المرور عبر القنوات الدبلوماسية.

– **تسليم المجرمين** : استقر الفقه القانوني على اعتبار أن تسليم المجرمين شكل من أشكال التعاون الدولي في مكافحة الجريمة، وهذا النوع من التعاون الدولي هو نتيجة طبيعية للتطورات التي حدثت في كافة المجالات ومنها مجال الاتصالات وتقنية المعلومات، حيث لم تعد الحدود القائمة بين الدول تشكل حاجزا أمام مرتكبي الجرائم، كما أن نشاطهم الإجرامي لم يعد قاصرا على إقليم معين بل امتد إلى أكثر من إقليم، حيث بات المجرم منهم يشرع في التحضير لارتكاب جريمته في دولة معينة ويشرف على تنفيذها في بلد آخر، وقد يفر إلى بلد ثالث للابتعاد عن أيدي أجهزة العدالة، فالمجرم المعلوماتي أصبح بالتبعية مجرما دوليا .ولكون أنه لا يمكن لأي دولة أن تجاوز حدودها الإقليمية لممارسة أعمالها القضائية على المجرمين الفارين، كان لابد من إيجاد آلية معينة للتعاون مع الدولة التي ينبغي اتخاذ الإجراءات القضائية فوق إقليمها،

1. اعتمدت هذه المعاهدة بموجب قرار الجمعية العامة للأمم المتحدة 45/118 بتاريخ 1990/12/14 في الجلسة 68 للجمعية العامة للأمم المتحدة وتقضي باتفاق أطرافها على أن يقدم كل منهم للآخر أكبر قدر ممكن من المساعدة المتبادلة في التحقيقات أو إجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلا في اختصاص السلطة القضائية للدولة طالبة المساعدة، سالم محمد سليمان الأوجلي، المرجع السابق، ص427

2. د جميل عبد الباقي الصغير ، المرجع السابق ، ص 83

تتمثل في تسليم المجرمين الفارين لها، وهذا الإجراء يقوم أساسا على أن الدولة التي يتواجد على إقليمها المتهم بارتكاب جريمة معلوماتية عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك، وإلا كان عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة .فهو يحقق بذلك مصلحة الدولتين الأطراف في عملية التسليم، إذ يحقق مصلحة الدولة الأولى في كونه يضمن معاقبة الفرد الذي أخل بقوانينها وفي ذات الوقت يحقق مصلحة الدولة الثانية المطلوب إليها التسليم كونه يساعدها على تطهير إقليمها من فرد خارج عن القانون، ولذلك فقد حرصت معظم الدول على سن التشريعات الخاصة بتسليم المجرمين.[1]

أما المظهر الثاني من مظاهر التعاون الدولي في مجال مكافحة الجريمة المعلوماتية فهو التعاون الفني إذ لا يقتصر هذا التعاون الدولي على المساعدة القضائية المتبادلة فحسب، وإنما يشمل كذلك المساعدة التقنية وتبادل الخبرات بين الدول، ذلك أن العنصر البشري سواء على مستوى الأجهزة القضائية أو الأجهزة الأمنية ليس بذات الجاهزية والمستوى لمواجهة الجريمة المعلوماتية، وإنما يختلف من دولة إلى أخرى بحسب تقدم تلك الدولة ورقيها. حيث نجد أن جميع الاتفاقيات الدولية أو الإقليمية ذات الصلة قد دعت صراحة إلى ضرورة وجود تعاون دولي في مجال التدريب ونقل الخبرات فيما بينها[2]، ذلك أن التقدم المتواصل في تكنولوجيات المعلومات يفرض على الجهات القضائية والأمنية أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات والإلمام بها حتى يمكن التصدي للأفعال الإجرامية التي صاحبت هذه التكنولوجيا ومن ناحية أخرى فإن إعمال القانون في مواجهة الجرائم المعلوماتية يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة في المدونة العقابية التقليدية لما تتسم به هذه الجرائم من حداثة في الأسلوب وسرعة في التنفيذ وسهولة في إخفائها ومحو آثارها، وبالتالي فإن ظهور هذه الأنماط الجديدة من الجرائم أصبح يشكل عبئا ثقيلا على عاتق الأجهزة القضائية المختصة من قضاة تحقيق وقضاة حكم .وكذا رجال الضبطية القضائية، لأجل ذلك كان لابد أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والمعرفة والقدرة في التعامل مع الجريمة المعلوماتية والمجرم المعلوماتي.

1. ومنها المشرع الجزائري الذي أخذ بهذا الإجراء كمظهر من مظاهر التعاون الدولي بين السلطات القضائية الأجنبية في قانون الإجراءات الجزائية في المواد 694 و ما يليها ، نعيم سعيداني ، المرجع السابق ، ص 92

2. انظر المادة 29 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في الدورة الخامسة و العشرون المؤرخ في 15 نوفمبر 2000، موقع الأمم المتحدة، الدورة الخامسة و العشرون، http://www.un.org/arabic/documents،2014/05/14

ومن هذا المنطلق كانت الدعوة إلى ضرورة وجود تعاون دولي في مجال تدريب رجال القضاء والضبطية القضائية للاستفادة من مهارات وتجارب الآخرين من خلال أشخاص أكفاء ومؤهلين وقادرين على نقل هذه التجارب وتلك المهارات بوسائل سهلة ميسرة. و التدريب المقصود هنا ليس التدريب التقليدي فحسب، فلا يكف أن تتوافر لدى رجال القضاء الخلفية القانونية، ولدى الضبطية القضائية خصائص عمل الُشرطي وإنما لابد من إكسابهم خبرة فنية في مجال الجريمة المعلوماتية ، وهذه الأخيرة لا تتأت دون تدريب تخصصي يراعى فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب[1].

أما بالنسبة للمنهج التدريبي فيجب أن يشمل على بيان بالمخاطر والتهديدات ونقاط الضعف وأماكن الاختراقات لشبكة المعلومات وأجهزة الحاسب الآلي وتحديد أنماط ونوعية الجرائم المعلوماتية، وبيانا لأهم الصفات التي يتميز بها المجرم المعلوماتي والدوافع وراء ارتكابه للجريمة المعلوماتية .وفيما يتعلق بمنهج التدريب على التحقيق في الجريمة المعلوماتية فإنه لابد أن يشتمل على إجراءات التحقيق، التخطيط للتحقيق، تجميع المعلومات وتحليلها، أساليب المواجهة والاستجواب، طرق مراجعة النظم الفنية للمعلومات وأساليب المعمل الجنائي ، بالإضافة إلى ما يتعلق بالتفتيش والضبط وكيفية استخدام الحاسب الآلي كأداة للمراجعة والحصول على الأدلة[2].

بالرغم من ضرورة و حتمية التعاون الدولي في مجال مكافحة الجريمة المعلوماتية والذي بات مطلبا تسعى إلى تحقيقه أغلب الدول، إلا أنه ثمة صعوبات ومعوقات تجعل هذا التعاون ليس بالأمر اليسير وذلك لوجود عدة عقبات نذكر منها:

- **عدم وجود نموذج موحد للنشاط الإجرامي** :إذ لم تتفق الأنظمة القانونية في بلدان العالم على صورة محددة ونماذج معينة يتم الاتفاق المشترك بين الدول حولها تندرج في إطار الجريمة المعلوماتية[3] ، فما يكون مجرما في بعض الأنظمة قد لا يكون كذلك في أخرى.
- **اختلاف النظم القانونية الإجرائية:** إذ بسبب هذا الاختلاف قد تكون هناك طرق للتحري والتحقيق والمحاكمة التي تثبت فعاليتها في دولة ما، قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها

1. ومن أمثلة أنماط التدريب في كندا دورات متخصصة في أساليب التحقيق في الجريمة المعلوماتية لمدة 4 أسابيع : أساسيات الحاسبات ، برمجة الحاسوب ، أمن الحاسبات و الشبكات ، الاثبات في الجريمة المعلوماتية ، د حسين بن سعيد بن سيف الغفري، المنشاوي للبحوث و الدراسات، الجهود الدولية في مواجهة جرائم الأنترنت ،الرياض، 2007 ، ص 43
2. هشام محمد فريد رستم ، المرجع السابق ، ص 496
3. عبد الفتاح بيومي حجازي ، المرجع السابق ، ص 188

كما هو الحال مثلا بالنسبة للمراقبة الإلكترونية، فإذا ما اعتبرت أن طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى .بالإضافة إلى أنه قد لا تسمح دولة ما باستخدام دليل إثبات جرى جمعه بطرق ترى هذه الدول أنها طرق غير مشروعة.

- **التجريم المزدوج** : يعتبر التجريم المزدوج من أهم شروط تسليم المجرمين، وقد يكون هذا الشرط عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجريمة المعلوماتية، سيما وأن معظم الدول ما زالت نصوصها العقابية خالية من هذا النمط الإجرامي.

وفي الحقيقة فإن المصلحة المشتركة للدول تقتضي البحث عن الوسائل التي تساعد في التغلب على هذه الصعوبات وإيجاد تعاون دولي حقيقي يتفق مع طبيعة هذا النوع المستحدث من الجرائم للتخفيف من خلو الفوارق بين الأنظمة القانونية العقابية الداخلية من خلال القضاء على العقبات و الصعوبات التي تواجه القضاء الدولي منها :

- فيما يتعلق بالعقبة الأولى المتمثلة في عدم وجود نموذج موحد للنشاط الاجرامي فإن الأمر يقتضي توحيد هذه الأنظمة القانونية[1] ، و لاستحالة هذا الأمر فإنه لا مناص من البحث عن وسيلة أخرى تساعد على ايجاد تعاون دولي يتفق مع طبيعة هذا النوع المستحدث من الجرائم و يخفف من غلو الفوارق بين الأنظمة العقابية ، و تتمثل هذه الوسيلة في التحديثات التشريعية المحلية المعنية بالجرائم المعلوماتية و ابرام اتفاقيات خاصة يراعى فيها هذا النوع من الجرائم و حصرها.
- أما العقبة الثانية المتعلقة باختلاف النظم القانونية الإجرائية نجد أن توصيات الصكوك الصادرة عن الأمم المتحدة غالباً ما تشجع الاطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة ، الشيء الذي يخفف من غلو و اختلاف النظم القانونية و الإجرائية و يفتح الباب أمام تعاون الدولي فعّال ، فمثلاً المادة 20 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة المنعقدة في باليرمو سنة 2000 تشير في هذا الصدد إلى التسليم المراقب و المراقبة الالكترونية و غيرها من أشكال المراقبة و التعقب. كما أن الاتفاقية الاوروبية للإجرام المعلوماتي أوجدت بعض الحلول التي من شأنها التغلب على هذه العقبة و التي أوجبت على الدول الأطراف فيها ضرورة تحديد نقطة اتصال تعمل لمدة 24 ساعة يومياً طوال الاسبوع لكي تؤمن المساعدة المباشرة للتحقيقات و تشمل تسهيل تطبيق الإجراءات بصفة مباشرة.

1. د حسين بن سعيد بن سيف الغفري ، المرجع السابق ، ص 43

- و لأجل القضاء على مشكلة التجريم المزدوج و الذي يعد من أهم الشروط الخاصة بتسليم المجرمين ركزت الاتجاهات و التطورات التشريعية على تخفيف التطبيق الصارم لهذا الشرط ، و ذلك بإدراج أحكام عامة في المعاهدات و الاتفاقيات المعنية بتسليم المجرمين إما بسرد الأفعال و التي تتطلب أن تجرم كجرائم أو افعال مخلة بمقتضى قوانين الدولتين معاً أو بمجرد السماح التسليم لأي سلوك يتم تجريمه و يخضع لمستوى معين من العقوبة في كل دولة.

الفرع الأول: جهود الأمم المتحدة في مجال مكافحة جرائم المعلوماتية

بذلت الأمم المتحدة جهوداً كبيرة في سبيل العمل على مكافحة جرائم المعلوماتية ، و ذلك لما تسببه هذه الجرائم من أضرار بالغة و خسائر فادحة بالإنسانية جمعاء ، و إيماناً منها بأن منع هذه الجرائم و مكافحتها يتطلبان استجابة دولية في ضوء الطابع و الأبعاد الدولية لإساءة استخدام الكمبيوتر و الجرائم المتعلقة به[1] .

توصلت منظمة الأمم المتحدة في مؤتمرها الثامن المنعقد بهافانا 1990 حول منع الجريمة و معاملة المجرمين United Nations Congress on the Revention of Crime and the Treatement of the Offender إلى اصدار قانون خاص بالجرائم المتعلقة بالحاسوب ، و أشار القرار إلى أن الأجرام الدولي لمواجهة الجرائم المستحدثة يتطلب من الدول الأعضاء اتخاذ عدة إجراءات[2] تتلخص فيما يلي :

- تحديث القوانين و أغراضها الجنائية بما في ذلك التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية الراهنة من تحقيق و قبول الأدلة على نحو ملائم و إدخال التعديلات إذا دعت الضرورة لذلك.
- اتخاذ تدابير أمن و الوقاية مع مراعاة خصوصية الأفراد و احترام حقوق الإنسان
- رفع الوعي لدى الجماهير و القضاة و الأجهزة العاملة على مكافحة هذا النوع من الجرائم.
- التعاون مع المنظمات المهتمة بهذا الموضوع ، و وضع و تدريس الآداب المتخذة في استخدام الحاسوب في المناهج التعليمية.
- حماية مصالح الدولة و حقوق ضحايا جرائم الحاسوب.

1. عواطف محمد عثمان عبد الحليم ،جرائم المعلوماتية ، مجلة العدل ، العدد الرابع و العشرون ، ص 69
2. نعيم سعيداني ، المرجع السابق ، ص 93

لكن تزايد جرائم المعلوماتية و ما تثيره من مشاكل أدى بمنظمة الأمم المتحدة إلى عقد الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية ديسمبر سنة 2000 ، رقم 55/63 الجلسة العامة ، أين أكدت على الحاجة إلى تعزيز التنسيق و التعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية ، بالإضافة الذي يمكن أن تقوم به المنظمة و المنظمات الإقليمي الأخرى.

عقدت كذلك الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة و العدالة الجنائية بالبرازيل أيام 12 إلى 19 أفريل 2010 ، حيث ناقشت فيه الدول الأعضاء ببعض التعمق مختلف التطورات الأخير في استخدام التكنولوجيا من طرف المجرمين و السلطات المختصة في مكافحة الجريمة.

تبقى منظمة الأمم المتحدة الإطار الأمثل لمكافحة جرائم المعلوماتية حيث وضعت مجموعة من القواعد الموضوعية و إجرائية[1] لمواجهة هذه النوعية من الجرائم.

أولاً القواعد الموضوعية : تتضمن هذه القواعد النص على قائمة الحد الادنى للأفعال المتعين تجريمها و اعتبارها من قبيل جرائم المعلوماتية و تحديثها دورياً و المتضمنة :

- **جريمة الاحتيال أو الغش المرتبط بالكمبيوتر** : و يشمل ذلك الادخال و الاتلاف و المحو لمعطيات الكمبيوتر أو برامجه أو القيام بأية أفعال تؤثر بمجرى المعالجة الآلية للبيانات و تؤدي إلى الحاق الخسارة أو فقدان الحيازة أو ضياع ملكية شخص و ذلك بقصد جني الفاعل منافع اقتصادية له أو للغير.
- **جريمة التزوير التي تطال برامج الكمبيوتر أو التزوير المعلوماتي** : و يشمل ذلك ادخال أو الاتلاف أو المحو أو تحوير المعطيات أو البرامج أو أية أفعال تؤثر على المجرى العادي لمعالجة البيانات ترتكب باستخدام الكمبيوتر و تعد فيما لو ارتكبت بغير هذه الطرق من قبيل أفعال التزوير المنصوص عليها في القانون الوطني.
- **جريمة تخريب و اتلاف الكمبيوتر**: و يشمل ذلك ادخال أو الاتلاف أو التخريب أو أي فعل آخر بقصد تعطيل وظيفة من وظائف الكمبيوتر أو نظام الاتصالات و الشبكات.

1. عبد الله عبد الكريم عبد الله ، جرائم المعلوماتية و الأنترنت دراسة مقارنة ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، 2007 ، ص111

- **جريمة الدخول غير المصرح به** : و هو التوصل أو الولوج دون تصريح إلى نظام أو مجموعة نظم عن طريق انتهاك إجراءات الأمن.
- **جريمة الاعتراض غير المصرح به** : و هو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام كمبيوتر أو عدة نظم او شبكة اتصالات.

ثانيًا القواعد الإجرائية : تتضمن بعض الأسس الواجب مراعاتها[1] :

- وجوب تحديد السلطات التي تقوم بإجراء التفتيش و الضبط في بيئة تكنولوجيا المعلومات، و خاصة ضبط الاشياء المتعلقة بها و تفتيش الحاسب.
- وجوب أن يكون هناك قدر كبير من التعاون الفعال بين الأطراف لكي تكون المعلومات متاحة في صورة يمكن استخدامها للأغراض القضائية في حل هذه الجرائم
- السماح للسلطات العامة باعتراض الاتصالات داخل البيئة المعلوماتية مه استخدام الأدلة التي يمكن ان يتحصل عليها.
- ادخال بعض التعديلات التشريعية في حالة الضرورة ما يتماشى مع طبيعة جرائم المعلوماتية داخل القانون الوطني و كذلك القواعد القائمة في مجال الإثبات الالكتروني من حيث مصداقية الأدلة و ما يمكن أن تثيره من مشاكل عند تطبيقها.
- يجب أن يوضع في الاعتبار كل المسائل المرتبطة ببيئة تكنولوجيا المعلومات ، مثل ضياع فرصة اقتصادية ، التجسس ، انتهاك حرمة الحياة الخاصة ، مخاطر الخسارة الاقتصادية ، كلفة إعادة بناء قواعد البيانات كما كانت و إعادتها إلى الواضع السابق قبل اجراء أي تفتيش أو تحقيق.

1. عبد الله عبد الكريم عبد الله ، المرجع نفسه ، ص 114

الفرع الثاني: جهود المنظمات الدولية في مجال مكافحة جرائم المعلوماتية

قد اتخذت مبادرات من قبل العديد من المنظمات كالاتحاد الدولي للاتصالات(ITU) ، الإنتربول/يوروبول ، منظمة التعاون الاقتصادي والتنمية (OECD) ، مؤسسة الإنترنت للأسماء والأرقام المخصصة (ICANN) والمنظمة الدولية لتوحيد المقاييس(ISO) ، واللجنة الكهروتقنية الدولية (IEC) وفرق عمل هندسة الإنترنت و FIRST منتدى الاستجابة للأحداث ومجموعات الأمن لآسيا والمحيط الهادئ، ومنظمة التعاون الاقتصادي للمحيط الهادئ وآسيا (APEC)ومنظمة الدول الأميركية (OAS) ورابطة دول جنوب شرق آسيا (ASEAN) وجامعة الدول العربية، والاتحاد الأفريقي.

أولاً : منظمة التعاون الاقتصادي والتنمية (OECD)

تهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادي و تناغم التطور الاقتصادي مع التنمية الاجتماعية ، بدأت هذه المنظمة الاهتمام بجرائم المعلوماتية منذ عام 1978 ، حيث وضعت مجموعة من الأدلة و قواعد إرشادية تتصل بتقنية المعلومات، و يعد الدليل المتعلق بحماية الخصوصية و قواعد نقل البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام بها.[1]

فأصدرت سنة 1983 تقريراً بعنوان الجرائم المرتبطة بالحاسوب و تحليل السياسة القانونية الجنائية ، حيث استعرض التقرير السياسة الجنائية القائمة و المقترحات الخاصة في عدد من الدول الأعضاء ، وتضمن التقرير الحد الأدنى من لأفعال سوء استخدام الحاسوب و التي على الدول تجريمها و تشمل هذه الأفعال[2] :

- الاستخدام أو الدخول إلى نظام و مصادر الحاسب على نحو غير مصرح به
- الإفشاء غير مصرح به للمعلومات المعالجة آلياً و النسخ و الإتلاف أو التخريب ما يحويه من بيانات و برامج و الإعاقة غير المشروعة للوصول لمصادر الحاسب من منع أو تعطيل استخدام الحاسب أو برامجه أو البيانات المخزنة داخله.

1. يوسف صغير ، الجريمة المرتكبة عبر الأنترنت ، مذكرة ماجستير حقوق ، جامعة مولود معمري تيزي وزو، الجزائر، 2013 ، ص 96
2. غازي عبد الرحمن هيان الرشيد ، الحماية القانونية من جرائم المعلوماتية (الانترنت) ،مذكرة دكتوراه ، الجامعة الإسلامية، لبنان ،2004 ، ص92

و في عام 1992 و ضعت المنظمة توصيات و إرشادات خاصة بأنظمة المعلومات و أوصت بضرورة أن تعطي التشريعات الجنائية للدول الأعضاء مبادئ عامة[1] تتمثل في :

- **حدود التجميع** : يتعين فرض قيود على تجميع البيانات.
- **نوعية البيانات** : حيث تنص على أن تتعلق البيانات بالغاية و الغرض الذي سوف تستخدم من أجله.
- **تعيين الغرض** : بحيث يكون الغرض الذي تستخدم فيه البيانات الشخصية محصورة و محددة سلفا.
- **حدود الاستخدام** : يقتضي الالتزام بعدم إفشاء البيانات الشخصية و نشرها لغير المصرح لهم بذلك.
- **الوقاية الأمنية** : ضرورة اتخاذ تدابير و إجراءات أمنية ملائمة و حازمة في إحاطة البيانات.
- **الانفتاح** : أن تكون السياسة العامة للتطوير و الخطط و التطبيقات معلنة فيما يتعلق بالبيانات ذات الطبيعة الشخصية.
- **المشاركة الفردية** : حق الأشخاص المعنية في الوصول و التعرف على البيانات التي تخصهم فضلاً عن رقابة مدى صحتها.
- **المسائلة و المحاسبة** : التي تقتضي محاسبة الأشخاص و الجهات المرخص لهم الوصول و الاطلاع على البيانات و التعامل معها في حالة تجاوز أي من الإجراءات التي تكفل حماية البيانات ذات الصفة الخاصة.

ثانياً : الأنتربول

وضعت منظمة الإنتربول[2] نظاما خاصا للتعاون ، وهو النظام الوطني الخاص بالنقطة المرجعية المركزية[3] NCRP ويوجد في كل دولة من الدول الأعضاء في الإنتربول مكتب مركزي وطني يُعد نقطة الاتصال مع الإدارات الأجنبية التي تجري تحقيقات خارج حدودها و تضم شبكة من المحققين العاملين في الوحدات الوطنية المعنية بجرائم لتيسير الاتصالات

1. د علي جبار الحسناوي ، جرائم الحاسوب و الأنترنت ، دار اليازوي العلمية للنشر و التوزيع ، عمان ، 2009 ، ص 154

2. الأنتربول بالإنجليزية Interpol هي اختصار لكلمة الشرطة الدولية بالإنجليزية International Police والاسم الكامل لها هو منظمة الشرطة الجنائية الدولية بالإنجليزية International Criminal Police Organization وهي أكبر منظمة شرطة دولية أنشئت في عام 1923 مكونة من قوات الشرطة لـ 190 دولة ، ومقرها الرئيسي في مدينة ليون بفرنسا، ويكيبيديا، منظمة الشرطة الجنائية الدولية، 2014/05/14 ، http://ar.wikipedia.org/Interpol

3. جان فرنسوا هنروت، أهمية التعاون الدولي بين عناصر الشرطة، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 جوان 2007 ، المملكة المغربية، ص 100

الميدانية بين البلدان الأعضاء وتسريعها قدر الإمكان ومن مهامها هذا النظام إنماء الاستراتيجيات والتقنيات والمعلومات بشأن أحدث الأساليب الجرمية في مجال جرائم تكنولوجيا المعلومات وهناك فرق عاملة إقليمية لإفريقيا والأمريكيتين وآسيا وجنوب المحيط الهادئ و أوروبا والشرق الأوسط وشمال إفريقيا[1].

كما قامت منظمة الإنتربول بوضع برنامجاً خاصاً لمكافحة الإجرام المعلوماتي يرتكز على التدريب والعمليات ويعمل على مواكبة التهديدات الناشئة مبادرات ويهدف هذا البرنامج[2] :

- توفيردورات تدريبية لوضع معايير مهنية والتقيد بها.
- تعزيز تبادل المعلومات بين البلدان الأعضاء عن طريق الأفرقة العاملة والمؤتمرات الإقليمية.
- تنسيق العمليات الدولية ودعمها
- إعداد قائمة عالمية بأسماء ضباط الاتصال ووضعها بتصرف المحققين في مجال الإجرام السيبيري على مدار الساعة
- مساعدة البلدان الأعضاء على التحقيق في الهجمات أو الجرائم السيبيرية عن طريق توفير خدمات في مجال التحقيق وقواعد البيانات
- إقامة شراكات استراتيجية مع المنظمات الدولية الأخرى وهيئات القطاع الخاص.
- تحديد التهديدات الناشئة وتبادل معلومات الاستخبار في هذا المجال مع البلدان الأعضاء.
- توفير بوابة آمنة على الويب لنشر معلومات ووثائق عملياتية.

1 الأنتربول ، الإجرام السبراني، 2014/05/14 ، مجالات-الإجرام/الإجرام-السيبيري/الإجرام-السيبيريhttp://www.interpol.int/ar

2 الإنتربول ، المرجع نفسه ، ص1

المطلب الثاني : على المستوى الإقليمي

تعد الاتفاقية الأوربية بمثابة دعوة موجهه إلى دول العالم للتفاعل مع الجرائم المستحدثة و التي جاءت نتيجة محاولات عديدة منذ ثمانيات القرن العشرين حتى ظهرت بشكلها ، فبتاريخ 20 أفريل 2000 تقدمت اللجنة الأوروبية لمشكلات الجريمة ولجنة الخبراء في حقل جرائم التقنية ، بمشروع اتفاقية جرائم الكمبيوتر وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من اصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت لاحقا في بودابست 2001 وتعرف باتفاقية بودابست 2001 (اتفاقية الجرائم الالكترونية – سايبر كرايم) وكان قد طرح مشروع الاتفاقية للعامة ووزع على مختلف الجهات وأطلق ضمن مواقع عديدة أوروبية وأمريكية على شبكة الأنترنت لجهة التباحث وإبداء الرأي . وتعكس الاتفاقية الجهد الواسع والمميز للاتحاد الأوروبي ولجان الخبراء فيهما المنصبة على مسائل جرائم الكمبيوتر وأغراضها منذ اكثر من عشرة أعوام[1] .

ومن أهم الأسباب التي أدي إلى إبرام الاتفاقية هو الحاجة على إتخاذ تدابير تشريعية لمكافحة جرائم المعلوماتية و مخاطرها المدمرة على الدول خاصة في ظل شيوع شبكات المعلومات و في ظل التوسع و النماء الكبير لأنظمة الحوسبة المفتوحة و نقل و تدفق المعلومات ، إضافة إلى التشديد على أهمية مكافحة كافة الأنشطة التي تستهدف أمن المعلومات و نظم الكمبيوتر.[2]

هذه التدابير التشريعية و التنظيمية لضمان ملاحقة مرتكبي هذه الجرائم وكشفها وتوفير قواعد ملائمة للتحري والتحقيق والضبط والتفتيش والمحاكمة مع التركيز على اهمية التعاون المحلي والاقليمي والدولي مع وجوب اقامة التوازن بين متطلبات تنفيذ القانون وبين وجوب احترام الحقوق الاساسية والسيادة ، ولأن هذه الاتفاقية جاءت حصيلة جهود دولية واقليمية فقد أكدت المقدمة أيضا على أهمية ما أنجز من جهود في حقل جرائم المعلوماتية من قبل الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية والاتحاد الأوربي ومجموعة الدول الصناعية وبالنتيجة فأن مشروع الاتفاقية قد ركزت على عناصر أساسية ثلاثة[3]-:

1. د. يونس عرب ، قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، 2-4 ابريل 2006، مسقط، ص15
2. عبد الله عبد الكريم عبد الله ، المرجع السابق ، ص126
3. د. يونس عرب ، المرجع السابق، ص16

- أهمية التدابير التشريعية الموضوعية) نصوص التجريم.
- أهمية التدابير التشريعية الاجرائية) النصوص الاجرائية.
- أهمية تدابير التعاون الدولي والاقليمي في مجال مكافحة الجرائم.

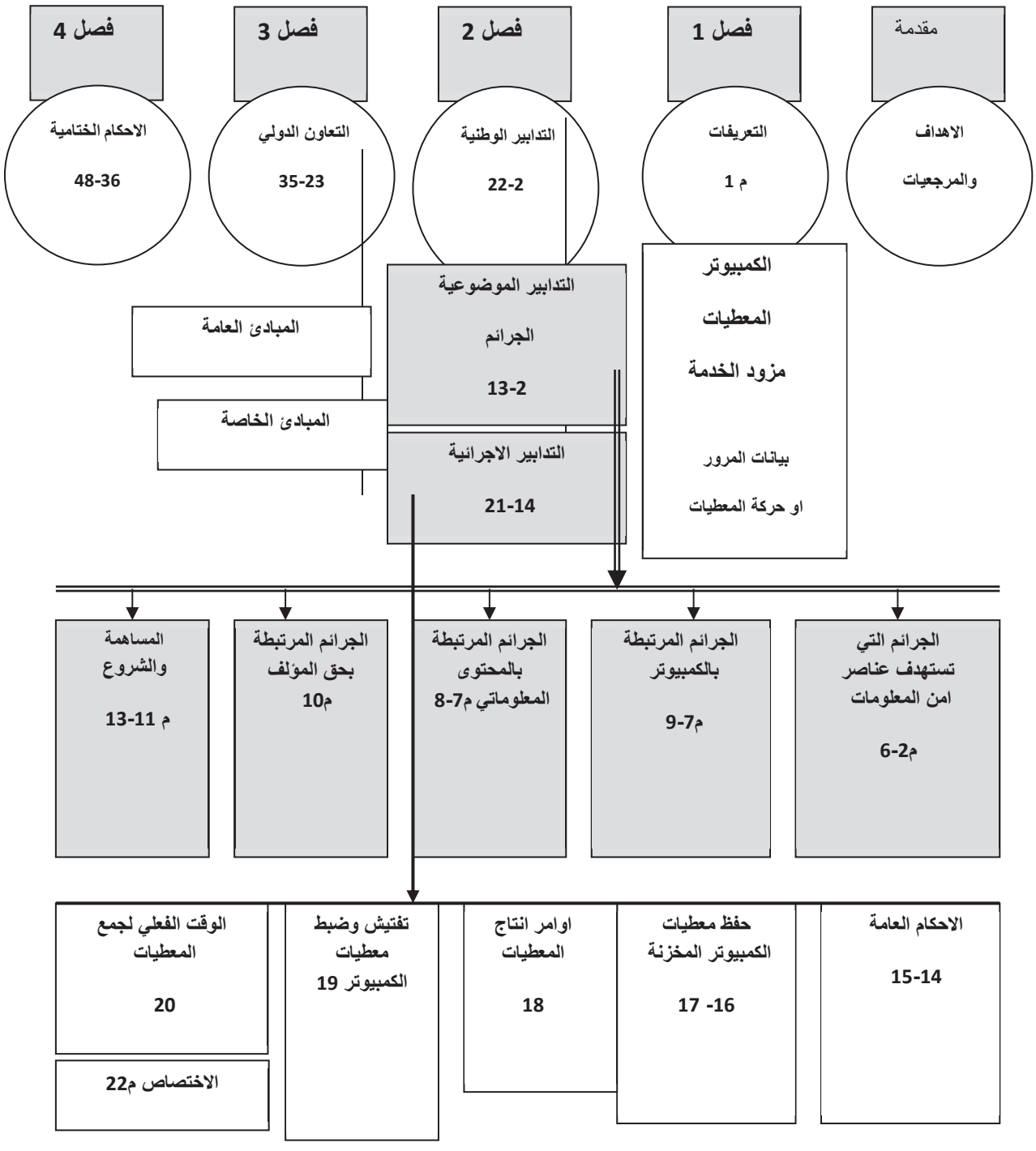
إن هذه الاتفاقية تقدم ولأول مرة إطارًا لتحديد قائمة جرائم الكمبيوتر وأنماطها وطوائفها ، إذ حتى الآن وبالرغم من الجهود التشريعية والتدابير الاقليمية والدولية على مدى السنوات الثلاثين الماضية لم تتوفر رؤية شاملة او اطار واضح يحدد قائمة الجرائم أو بين أساس التقسيم ، ولهذا فان أهم ما يسجل لهذه الاتفاقية – بعيد عن الاتفاق والخلاف على الأساس الذي اعتمدته – أنها تطرح اطارًا للتقسيم والتحديد بشأن القواعد الموضوعية لجرائم الكمبيوتر والأنترنت، وبالرجوع الى المعيار التي اعتمدته ، نجده بالأساس يقوم على فكرة دور الكمبيوتر بالجريمة[1].

تتكون الاتفاقية من مقدمة وأربعة فصول، فبعد أن استعرضت المقدمة أهداف الاتفاقية ومنطلقاتها ومرجعياتها السابقة وما تقوم عليه من جهود ارشادية وتوجيهية وتدابير اقليمية ودولية ، جاء الفصل الأول لتغطية المصطلحات الأساسية (مادة 1) ، تضمن الفصل الثاني الذي جاء تحت عنوان الإجراءات المتعين اتخاذها على المستوى الوطني ، ثلاثة أقسام : الأول ، ويضم المواد من 2–13 ويعالج النصوص الموضوعية لجرائم الكمبيوتر، والقسم الثاني ويضم المواد من 14–21 وتتعلق بالقواعد الإجرائية والقسم الثالث ويضم المادة 22 وتعلق بالاختصاص .

أما الفصل الثالث من الاتفاقية والذي جاء تحت عنوان التعاون الدولي ، فقط تضمن قسمين ، الأول تحت عنوان المبادئ العامة ويضم المواد من 23–28 والقسم الثاني ويتعلق بالنصوص الخاصة ويضم المواد من 29–35 ، أما الفصل الخامس فيتضمن الاحكام الختامية ويضم المواد من 36 – 48 .

1. د عماد مجدي عبد الملك ، جرائم الكمبيوتر و الأنترنت ، دار المطبوعات الجامعية، الإسكندرية، 2011، ص175

شكل 1: البناء العام لاتفاقية بودابست 2001



أكدت مقدمة الاتفاقية على الحاجة إلى إتخاذ تدابير تشريعية لمكافحة جرائم الكمبيوتر و الأنشطة التي تستهدف العناصر الثلاثة لأمن المعلومات ونظم الكمبيوتر وهي السرية confidentiality وسلامة المحتوى integrity وتوفر المعلومات والنظم availability ، كما أن المقدمة نجدها تلخص أهداف الاتفاقية بما يلي[1]:-

- السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنضمة للاتفاقية من غير الدول الأوروبية .
- التأكيد على أهمية التعاون الاقليمي والدولي في ميدان مكافحة جرائم الكمبيوتر والأنترنت وإيجاد مرجعية ودليل إرشادي للتدابير التشريعية الوطنية في ميدان مكافحة جرائم الكمبيوتر والأنترنت .
- ضرورة فعالية خطط العمل لمكافحة الأنشطة التي تستهدف سرية وسلامة وتوفر المعلومات وأنظمة الكمبيوتر وشبكات الكمبيوتر وأنشطة إساءة استخدام الكمبيوتر والشبكات ، بما في ذلك تحديد الإطار الموضوعي لهذه الانشطة والإطار الإجرائي المتصل بالتحقيق والتحري والمقاضاة في ميدان جرائم الكمبيوتر على المستوى الوطني والدولي .

يضم الفصل الأول مادة واحدة (المادة 1) وهي التعريفات definitions وربما تكون هذه المادة من أهم المواد في ميدان اتفاقيات تقنية المعلومات2 بسبب الخلاف الكبير بشأن تعريف اصطلاحات الكمبيوتر تبعا لزاوية الرؤيا وهدف استخدام التعريف ، إلى جانب التباين بشأن المعايير والمقاييس التقنية وربما تكون لهذه المادة أهمية استثنائية لجهة توحيد التعريفات بعدما ظهر التناقض والتباين في تشريعات جرائم الكمبيوتر التي جرى سنها في أوروبا وأمريكا واستراليا وعدد من دول شرق آسيا، كما عرفت نظام الكمبيوتر computer system ، وعرفت هذه المادة معطيات الكمبيوتر computer data تعريفاً واسعاً يشمل الحقائق والمعلومات والمفاهيم بشكل مناسب لعمليات المعالجة في نظام الكمبيوتر.

أما الفصل الثاني من الاتفاقية والمعنون (المعايير المتعين اتباعها على المستوى الوطني – measures to be taken at the national level) تضمن أقساما ثلاث ، الأول حول التدابير الموضوعية أي القانون الجنائي

1. المجلس الأوروبي ، المذكرة التفسيرية لاتفاقية بودابست 2001 النسخة المترجمة بالعربية، 2014/05/12 http://conventions.coe.int/Default.asp?pg=Treaty/Translations/TranslationsChart_en.htm#185،
2. د هلالي عبد اللاه أحمد ،جرائم المعلوماتية و أساليب المواجهة و فقاً لاتفاقية بودابست،ط1، دار النهضة، القاهرة، 2007، ص30

الموضوعي، والتي تعنى بالسلوكيات التي يجب اعتبارها جريمة جنائية، والثاني حول التدابير الإجرائية، ويتناول التدابير التي تتخذ لإجراء تحقيقات أكثر فعالية فيما يتعلق بجرائم الكمبيوتر، ويجب التأكيد على أن هذه التدابير الإجرائية يمكن استخدامها مع أية جرائم جنائية يشترك فيها نظام للكمبيوتر، والثالث حول الاختصاص، وبهذا الفصل تكون الاتفاقية قد قدمت الإطار القانوني للتدابير التشريعية الموضوعية والاجرائية المتعين اتخاذها لمواجهة جرائم الكمبيوتر والانترنت[1]، وهذا ما سيتناوله البحث بشيء من التفصيل.

الفصل الثالث تم تخصيصه للتعاون الدولي و الحث على الأطراف أن تتعاون مع بعضها البعض، في تطبيق الأصول الدولية في المواد الجنائية ، والمبادئ المتعلقة بالمساعدات القانونية المتبادلة، والمعلومات المقدمة طواعية، والمساعدة القانونية المتبادلة في حال عدم وجود وثائق دولية معمول بها، والسرية ووضع حد للاستخدام.

أما الفصل الرابع الأحكام الختامية .ويهتم هذا الفصل على وجه الخصوص بالدول غير الأوروبية كما ينص على سبل انضمام الدول غير الأعضاء إلى الاتفاقية.

الفرع الأول: القانون الجنائي الموضوعي

يعد موضوع القسم الأول من هذه الاتفاقية (المواد من 2 إلى 13) دليلاً ارشادياً لتحسن أو اصلاح و سائل منع و قمع الإجرام المعلوماتي Améliorer les moyens de prévenir et de réprimer la criminalité informatique، بتحديد أدنى القواعد العامة التي تسمح باتخاذ بعض التصرفات القانونية اتجاه هذه الجرائم و يسهل مكافحتها على المستوى الوطني و الدولي، و يحدد قائمة تسمح بتجريم بعض الأفعال و التصرفات غير المشروعة التي ترتكب على بيئة معلوماتية، بعبارة أخرى حصر جرائم المعلوماتية بتحديد الحد الأدنى في بعض الأفعال غير المشروعة التي تعد من قبيل جرائم المعلوماتية.

فإذا كانت هذه الاتفاقية تنطبق على التصرفات التي توصف على أنها جرائم مرتكبة عن طريق تكنولوجيا المعلومات، فإن المذكرة التفسيرية حرصت على ايضاح أن الاتفاقية تستخدم تكنولوجيا محايدة Neutre أي التكنولوجيا الآنية و المستقبلية، كما ركزت المذكرة التفسيرية على ضرورة ارتكاب الجرائم المحصاة دون حق وذلك عندما نصت (يشترط في تجريم

1. د طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، ص297

الأفعال في هذه الاتفاقية أن يكون القيام بالفعل دون حق (Sans droit)، كما أن كل الجرائم المدرجة يجب ان تكون مرتكبة بطريقة عمدية Facon Intentionnelle[1].

أولاً: الأفعال غير المشروعة

تناولت المواد من 2 إلى 10 الجرائم الواردة في هذه الاتفاقية

أ- **جرائم ضد سرية وسلامة و توافر البيانات و النظم المعلوماتي:** Infraction contre la systèmes confidentialité, L'intégrité et la disponibilité des données et informatique، إن الغرض من الجرائم التي تناولها هذا العنوان هو حماية سرية و سلامة و اتاحة أو تهيئة البيانات و نظم الحاسب للعمل أو التشغيل، وبالتالي يخرج من نطاق التجريم الأنشطة المشروعة و العادية و المرتبطة بتصميم الشبكات و كذلك الممارسات الاستثمارية أو التجارية المشروعة و العادية، و قد تناولتها[2] المواد من 2 إلى 6

- **الولوج غير القانوني (المادة2):** Accès Illégal و الذي يعد الجريمة الرئيسية التي تهدد سرية و أمن و سلامة المعلومات و توفرها و على ذلك فإن مجرد التدخل غير المصرح به بمعنى القرصنة* Le piratage ، أو الدخول غير المشروع في النظام يعتبر تصرفاً غير مشروع
- **الاعتراض غير القانوني (المادة3):** تهدف هذه المادة لحماية الحق في احترام نقل البيانات و أن هذه الجريمة تمثل انتهاكاً للحق في احترام الاتصالات مثل التصنت و التسجيل التقليدي للمحادثات و المراسلات بين بين الأشخاص.
- **الاعتراض على سلامة البيانات (المادة4):** الغرض من هذه المادة هو أن تكون بيانات و برامج الحاسب مكفولة بحماية مماثلة لتلك التي تتمتع بها الأشياء المادية ضد الأضرار التي تحدث عمداً من اتلاف الأجهزة المادية و المنطقية المكونة للحاسب و محو البيانات و البرامج.[3]

1.د طارق ابراهيم الدسوقي عطية، المرجع نفسه، ص302

2.د هلالي عبد اللاه أحمد، المرجع السابق، ص 68

* فالقرصنة الإلكترونية أو المعلوماتيَّة هي عمليَّة اختراق لأنظمة الحاسوب.

3ا. لمجلس الأوروبي ، المرجع السابق، ص21

- **الاعتداء على سلامة النظام (المادة5)**: تهدف هذه المادة إلى تجريم عرقلة الاستخدام الشرعي لنظام المعلومات، أو التأثير على سيرها العادي و التي تمنع او تبطئ بشكل ملموس سير عمل النظام.
- **إساءة استخدام أجهزة الحاسب (المادة6)**: تشير هذه المادة أن الأعمال غير المشروعة التي تندرج تحت النوع أ من الجرائم المذكورة أعلاه تكون في الغالب عند حيازة و سائل الدخول كحصول المجرم على معدات التشويش أو أجهزة تحاليل الشبكات التي هي في الأصل تستعمل للتحقيق من إمكانية عمل الشبكات أو أجهزة مراقبة أمن الشبكات كما قد يكون جهاز الكمبيوتر نفسه أداة المزود بالأنترنت أداة لاختراق بعض المواقع أو الحسابات الالكترونية[1]، كما تشمل الإنتاج المتعمد أو بيع أو شراء أو استيراد أو توزيع الأجهزة و الأدوات بهدف ارتكاب أي فعل المنصوص عليه في المواد 2 إلى 5 من هذه الأتفاقية.[2]

ب- **الجرائم المتصلة بالحاسب**: Infractions Informatiques و هي المادتين 7و8 والتي تتعلق بجرائم عادية يمكن في الغالب ان ترتكب عن طريق الحاسب الآلي:

- **التزوير المعلوماتي (المادة7)**: الغرض من هذه المادة في إنشاء جريمة موازية لجريمة تزوير المستندات الورقية كما تهدف إلى استكمال أوجه النقص[3] التي تعتري قانون العقوبات بالنسبة للتزوير التقليدي، و التزوير المعلوماتي يتكون من خلق Créer أو تعديل Modifier.
- **الغش المعلوماتي (المادة8)**: مع حدوث ثورة تكنولوجية تضاعفت إمكانية ارتكاب جرائم اقتصادية كالغش و بالأخص النصب ببطاقات الائتمان و المعاملات البنكية أو الودائع التي أصبحت هدفاً للنصب من خلال التلاعبات بمدخلات النظام بمعنى ادخال على النظام ببيانات غير صحيحة.

ت- **الجرائم المتصلة بالمضمون**: Infraction se rapportant au contenu هذه الجرائم المرتبطة بالمحتوى و التي تربط بإنتاج أو نشر غير المشروع للمواد الإباحية الطفولية عير النظم المعلوماتية.

1. د طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 319
2. عبد الله عبد الكريم عبد الله، المرجع السابق، ص 133
3. د طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 323

- **الجرائم المتصلة بالمواد الاباحية (المادة9)**: تسعى هذه المادة إلى تدعيم الإجراءات التي تحمي الأطفال خاصة من الاستغلال الجنسي من خلال تحديث قانون العقوبات تشمل على استخدام الحاسب الآلي في اطار ارتكاب الجرائم الجنسية ضد الأطفال كما تجرم مختلف جوانب الإنتاج و الحيازة و النشر للمواد الإباحية الطفولية.

ث- **الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية و الحقوق المجاورة:** Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes و هي الأفعال التي تعتبر عن انتهاكات واقعة على الملكية الفكرية و خاصة المؤلف من خلال المادة 10 من متخصصي النظام المعلوماتي و خصوصاً شبكة الانترنت و الأفعال[1] هي : إن إعادة إنتاج و بث الأعمال المحمية عبر الأنترنت دون موافقة حائز الحق هو أمر غير شرعي و هذه الأعمال المحمية تشمل الأعمال الأدبية و التصويرية و الموسيقية و السمعية البصرية.

ثانياً : تقرير العقوبات

أشارت المادة 13 من هذه الاتفاقية على ضرورة خضوع المنصوص عليها في المواد من 2 إلى 10 لعقوبات جزائية و بالنظر للالتزامات التي تفرضها هذه المواد فإنه يجب على الاطراف المتعاقدة استخلاص النتائج الخطيرة المترتبة على ارتكاب تلك الجرائم و إقرار عقوبات جزائية فعالة ، مناسبة و رادعة تتضمن عقوبات سالبة للحرية.

و في حالة الاشخاص الاعتباريين أن يخضعوا أيضاً لعقوبات فعالة و مناسبة و رادعة و التي يمكن أن تكون جزائية، مدنية أو ادارية، كما تركت نفس المادة المجال مفتوحاً لإمكانية فرض عقوبات أخرى أو إجراءات تتناسب مع خطورة الجرائم المرتكبة مثل قرار الحظر أو المصادرة.

1. المجلس الأوروبي، المرجع السابق، ص66

الفرع الثاني: قانون الإجراءات

إن المواد في القسم الراهن نصت بعض الإجراءات التي يجب اتخاذها على الصعيد الوطني، و التي تخدم التحريات الجنائية التي ترتكب عن طريق المنظومة المعلوماتية، و جمع الادلة ذات الطابع الالكتروني.

فتكمن أحد أصحاب المشاكل في مجال مكافحة جرائم المعلوماتية في صعوبة تحديد هوية مرتكب الجريمة و مداها و تأثيرها و المشكلة الأخرى تكمن في ضياع البيانات الالكترونية التي يمكن نقلها أو تعديلها أو محوها في ثواني معدودة[1]، فمثلاً يستطيع الشخص الذي يتحكم في البيانات أن يستخدم المنظومة المعلوماتية بمحوها مدمراً بذلك جميع الأدلة التي يقوم عليها التحقيق الجنائي، لذا تعتبر في أغلب الأحيان السرعة و السرية من المكونات الأساسية لنجاح التحريات.

تُقر الاتفاقية إجراءات تقليدية مع المناخ التكنولوجي الحديث مثل التفتيش و المصادرة و بالتوازي وضعت إجراءات جديدة[2]، كالحفظ السريع للبيانات خلال مدة زمنية محدودة وذلك بهدف إتاحة الفرصة للحصول أو جمع البيانات التي تخدم التحريات أو الإجراءات الجنائية التي يجب القيام بها، و التي بموجبها يجري الإعداد و الاتفاق على نظم حماية تسمح بالسيطرة على هذا المناخ التكنولوجي الجديد و تطوير سلطات إجرائية جديدة.

كما تشير هذا القسم إلى مجال تطبيق بنود هذه الاتفاقية من خلال المادة 14، حيث تلزم كل دولة طرف في الاتفاقية بإقرار الإجراءات التشريعية بما يسمح القانون الداخلي بها لخدمة التحريات و الإجراءات الجنائية الخاصة على :

- الجرائم الجنائية المنصوص عليها في القسم الأول من الاتفاقية.
- جميع الجرائم الجنائية الأخرى التي ترتكب عن طريق المنظومة المعلوماتية.
- جمع الأدلة الالكترونية[3] لكل جريمة من أجل التحريات أو إجراءات جنائية معينة[4].

و تشير الاتفاقية بوضوح إلى أنه يجب ان تقر الأطراف بان القانون الداخلي يتضمن معلومات رقمية أو الكترونية قد تستخدم كأدلة[5] أما القضاء و ذلك في إطار الجنائي أياً كان طبيعة الجريمة المطلوب متابعتها.

1. د طارق ابراهيم الدسوقي عطية، المرجع السابق، ص496
2. المجلس الأوروبي، المرجع السابق، ص 68
3. الدليل الالكتروني هو كل البيانات التي يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسب من إنجاز مهمة ما، عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات، دار الجامعة الجديدة، الاسكندرية، 2010 ، ص53
4. علماً أن القانون المدني الجزائري قد انتبه إلى مسألة حجية الدليل الرقمي و التوقيعات الالكترونية و قبولها من طرف القاضي في مادتيه 1/223 و 327 من قانون 10/05 المتعلق بالمنافسة، محمد فولان، الحماية القانونية لتكنولوجيات الإعلام، مجلة المحكمة العليا، الجزائر، العدد01، 2010، ص 41
5. المجلس الأوروبي، المرجع السابق، ص69

أولاً: الحفظ السريع للمعطيات المخزنة

إن الإجراءات التي تتضمنها المادة 16 و 17 تطبق على جميع البيانات المخزنة (بيانات خط السير أو بيانات المضمون[1]) و التي تم جمعها و حفظها عن طريق أصحابها ، أي أنها لا تطبق إلا عندما تكون بيانات المعلوماتية، موجودة آنفاً و في طور التخزين.

و المقصود بحفظ البيانات[2] هو الاحتفاظ السابق بالمعلومات و تخزينها مع حمايتها من كل ما يمكن أن يفسدها أو يتلف نوعيتها أو حالتها الراهنة، فالحفظ هو عملية ضمان لسلامتها و جعلها بمأمن[3]، كما تشير المادة 14 من هذه الاتفاقية أنه يجب العمل بجميع الصلاحيات و الإجراءات و ذلك لخدمة التحريات و الإجراءات الجنائية، فالاحتفاظ بالبيانات يعد صلاحية و إجراء قانوني جديد تماماً على القانون الداخلي[4]، فالأمر يتعلق بوسيلة جديدة لإجراء التحريات الهامة لمكافحة جرائم المعلوماتية و ذلك للأسباب التالية:

- نظراً لقابلية البيانات المعلوماتية للتلاشي فإنه من السهل التلاعب بها و تعديلها، و كذلك من السهل فقدان العناصر التي تعد دليلاً على وقوع جريمة ولا سيما إذا كانت الممارسة المتبعة في المعالجة و التخزين تفتقد الدقة.
- إن جزء كبير من الإجرام المعلوماتي غالباً ما يرتكب من خلال انتقال الاتصال عن طريق المنظومة المعلوماتية، و من الممكن أن تتضمن تلك الاتصالات محتوى غير مشروع.

2. فبالنسبة للنوع الأول فقد عرفها المشرع بموجب المادة 02 من قانون 04/09 المتعلق بقانون الوقاية من الجرائم المتصلة بتكنولوجيات العلوم و الاتصال، 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 أما النوع الثاني والمتعلقة بالمحتوى فلم يأت على تعريفها، وإن كانت تتعلق بمضمون الاتصال أو الرسالة أو المعلومات المنقولة عن طريق الاتصال.

3. الفرق بين حفظ البيانات و توثيق البيانات فالتعبيرين لهما معنى متقارب و لكنه يختلف في مجال المعلوماتية فالتوثيق عبارة عن عملية تخزين للبيانات و الاحتفاظ بها لفترة زمنية معينة، د طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 501

3. المجلس الأوروبي، المرجع السابق، ص71

4. د طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 504

ثانياً: تفتيش و مصادرة البيانات المعلوماتية

تهدف المادة 19 من هذه الاتفاقية إلى تحديث و تجانس التشريعات الداخلية الخاصة بالتفتيش و مصادرة البيانات المعلوماتية المخزنة للحصول على ادلة مرتبطة بتحريات و إجراءات جنائية معينة، و تنص جميع التشريعات الداخلية الخاصة بالإجراءات الجنائية على صلاحيات التفتيش و المصادرة للعناصر المادية.[1]

غير أنه فيما يتعلق بالبحث عن البيانات المعلوماتية، يتحتم وجود أحكام إجرائية إضافية حتى تضمن الحصول على البيانات المطلوبة بنفس فاعلية التفتيش و مصادرة الدعائم للمعلومات المادية و يرجع ذلك أن تتم قراءة المعطيات عن طريق جهاز معلوماتي و لكن لا يمكن مصادرتها و نقلها بنفس طريقة المستند الورقي، كما يمكن نقل الأجهزة الداعمة التي يتم عليها حفظ البيانات (قرص صلب، ديسك...إلخ)، بالإضافة لكون المنظومة المعلوماتية متصلة فيما بينها، فيكون من السهل الوصول إلى المعلومات المطلوبة من خلال هذه المنظومة في حالة عدم تخزين هذه المعلومات على جهاز الكمبيوتر موضوع أمر التفتيش، حيث تكون مخزنة في حافظة معلومات متصلة بصورة مباشرة بجهاز كمبيوتر آخر و عن بصورة غير مباشرة بواسطة نظام اتصالات كالأنترنت[2] ، عندما ألزمت الفقرة الأولى و الثانية من نفس المادة الأطراف أن تخول لسلطاتها المختصة بمكافحة الجريمة المعلوماتية الحق في فحص و الدخول على المعطيات سواء الموجودة في نظم معلومات أو جزء من هذه المنظومة مثل الأسطوانة ...إلخ[3].

كما تناولت الفقرة الثالثة السماح للسلطات المختصة بمصادرة البيانات أو الحصول عليها بطريقة مشابهة لها عن طريق نسخها بأي طريقة تقنية و التي لا تعرضها للإتلاف أو فقدانها أو جزء منها. إذا أخذنا بعين الاعتبار البعد الدولي لجرائم الإنترنت، يمكننا أن نستنتج أنه لا يمكن لدولة بمفردها أن تحقق النجاح في هذه المعركة، بل لا يتحقق ذلك إلا عن طريق التعاون على المستوى الدولي و الاقليمي .ولكننا نعلم أن التعاون يعتمد على الأنظمة القانونية للدول والتوفيق بين التشريعات الوطنية المختلفة ،كما يجب على كل البلدان أن تضع إطارا قانونيا مناسبا، سواء على المستوى الوطني أو الدولي، بحيث يكون قادرا على توفير الأدوات التشريعية وأدوات التحقيق اللازمة لمكافحة جرائم الإنترنت مع الوضع في الاعتبار مدى تعقيدها.

1. و مثال ذلك ما جاء في القسم الثالث "في الانتقال و التفتيش و القبض " من الكتاب الأول من قانون 06-22 المؤرخ في 20 ديسمبر 2006 المعدل و المتمم للأمر55-165 المؤرخ في 08 يونيو 1965 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 84، الجزائر، 24 ديسمبر 2006
2. نبيل صقر، المرجع السابق، ص 160
3. المجلس الاوروبي، المرجع السابق، ص95

المبحث الثاني: جهود المشرع الجزائري لمكافحة الجرائم المعلوماتية

عرف نظام المعلوماتية تطورا بطيئاً في الجزائر[1] بالرغم من الإمكانيات الاقتصادية و المالية و البشرية التي نزخر بها مقارنة بالكثير من دول العالم الثالث، فالمشكل لم يكن يكمن في مجال نقص العتاد المعلوماتي بقدر مت هو التخطيط العقلاني المساير للواقع إضافة على التأخر في صدور قوانين لتنظيم النظم المعلوماتية[2] ماعدا شبكة الاتصالات التي وضعت لها قوانين واكبت التطور.

فالجزائر لم تعرف قوانين قبل سنة 2004 تطبق بشكل خاص على نظام المعلوماتية أو على تكنولوجيا الإعلام و الاتصال ما عدا شبكة الاتصال السلكية و اللاسلكية و وسائل الاعلام السمعية و البصرية، و الواقع أن هناك العديد من التشريعات و الاتفاقيات الدولية التي كانت تطبق في هذا المجال، منها الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 و المتضمن قانون العقوبات و المتضمن قانون الاجراءات الجزائية و الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 و المتضمن القانون المدني، و كذا قانون 2000-03 المؤرخ في 5 أوت 2000 و المتضمن القواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية و كذا الامر رقم 03-05 المؤرخ في 19 يوليو سنة 2003 و المتعلق بحقوق و الحقوق المجاورة.

أما الاتفاقيات الدولية فهناك جملة من هذه الاتفاقيات التي صادقت الجزائر عليها و أصبحت تعتبر من النظام القانوني الجزائري، نذكر منها اتفاقية باريس لحماية الملكية الصناعية، والاتفاقية العالمية حول حق المؤلف يوليو 1971 و اتفاقية إنشاء المنظمة العالمية للفكرية الموقعة بستوكهولم 14 يوليو 1967 بالإضافة إلى بعض البروتوكولات المتعلقة بتكنولوجيا الإعلام و الاتصال[3].

و لمسايرة التطور التكنولوجي كان لا بد للجزائر من إيجاد الإطار القانوني المناسب لحماية المنظومة المعلوماتية من السلوكيات الإجرامية المستحدثة من خلال:

1. أحمد عمراني، نظام المعلومات في القانون الجزائري، المؤتمر السادس لجمعية المكتبات و المعلومات السعودية، الرياض، 2010، ص12
2. حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، مذكرة ماجستير حقوق، جامعة الحاج لخضر باتنة، الجزائر، 2012، ص 180
3. أحمد عمراني، المرجع السابق، ص14

- إدراجه لبعض الإجراءات الجزائية الخاصة بجرائم نظم المعلومات من خلاله لتعديليه لقانون الإجراءات الجزائية الأول 14/04 المؤرخ في 10 نوفمبر 2004 و الثاني قانون 06-22 المؤرخ في 20 ديسمبر 2006 بتوسيع اختصاص بعض المحاكم المختصة و اختصاص وكيل الجمهورية و قاضي التحقيق (المواد من 37-40 و329) و كذا توسيع صلاحيات الضبطية القضائية من خلال تمديد الاختصاص المحلي إلى كامل التراب الوطني (المادة16) و كذلك إمكانية تفتيش المحلات السكنية و غير السكنية في كل ساعة من ساعات الليل و النهار بإذن من وكيل الجمهورية (المادة47) مع أمكانية تفتيش المساكن دون حضور المشتبه فيه أو أصحاب السكن و دون الشهود (المادة 45)، مع إمكانية تمديد فترة التوقيف للنظر مرة واحدة في حالة التلبس (المادة 51).

أم من حيث أساليب التحريات الخاصة من اعتراض المراسلات الالكترونية (المادة 65 مكرر 5) و التسرب (المادة 65 مكرر11).[1]

- الأمر 06/03 المؤرخ في 2003/07/19 المتعلق بالعلامات المعدل والمتمم للأمر 57/66 المؤرخ في 1966/03/19 المتعلق بعلامات المصنع والعلامات التجارية والمعدل للأمر رقم 223/67 المؤرخ في 1967/10/19 المتضمن أحكام العلامات التجارية و العلامات التجارية هي كل ما يتخذ من تسميات أو رموز أو أشكال توضع على البضائع التي يبيعها التاجر أو يصنعها المنتج أو يقوم بإصلاحها أو تجهيزها أو ختمها لتمييزها عن بقية المبيعات أو المصنوعات أو الخدمات، و باعتبار أن كل برنامج من برامج الكمبيوتر يحمل اسماً خاصًا به، لذلك فقد عمد أصحاب البرامج إلى تسجيل هذا الاسم كعلامة تجارية للبرنامج، ولما كانت هذه الحماية قاصرة على الاسم دون المحتوى فقد لجا أصحاب البرامج إلى وضع الاسم مقترنا به[2].

- الأمر 14/73 المؤرخ في 1973/04/03 المعدل والمتمم بمقتضى الأمر 10/97 المؤرخ في 1997/03/06 المعدل والمتمم بموجب الأمر 05/03 المؤرخ في 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة، و ذلك عندما وسع قائمة المؤلفات المحمية حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية و كذلك بتشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما مؤلفي المصنفات

1 محمد فولان، المرجع السابق، ص 43

2 عطاء الله فشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغاربي حول القانون و المعلوماتية، أكاديمية الدراسات العليا، ليبيا، أكتوبر 2009، ص13

المعلوماتية (المادة 151 الأمر 10/97) إذ كان في السابق التعدي على الملكية الفكرية يخضع للمواد 394/390 من قانون العقوبات لكنها أخرجت بموجب الأمر 10/97 من مظلة قانون العقوبات وأصبح لها تجريم خاص إذ أن قانون العقوبات كان يقرر بموجب المادة 390 الغرامة كعقوبة للاعتداء على حق المؤلف بينما الأمر 10/97 يقرر عقوبتي الحبس والغرامة[1].

- بالإضافة إلى قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم لقانون العقوبات و تلاه قانون 09-04 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، و سنتعرض خلال هذا المبحث لكل قانون على حدا.

المطلب الأول : في ظل قانون العقوبات

إن ظهور المعلوماتية و تطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة في قانون العقوبات الجزائري على غرار قوانين العقوبات المقارن، فرض حلها البحث في الأوضاع القانونية القائمة ومدى ملاءمتها لمواجهة هذه المشاكل.
ولما كان القاضي الجزائي مقيدا عند نظره الدعوى الجنائية بمبدأ شرعية الجرائم والعقوبات فإنه لن يستطيع أن يجرم أفعالا لم ينص عليها المشرع حتى ولو كانت هذه الأفعال مستهجنة وعلى مستوى عال من الخطورة الاجتماعية والاقتصادية، وكل ما يمكنه عمله هو محاولة تفسير النصوص القائمة طبقا لقواعد التفسير المسلم بها في القانون الجنائي، وأهمها مبدأ التفسير الضيق وحظر القياس.

و قد تطرق المشرع الجزائري على غرار الدول الأخرى مثل فرنسا[2] بتجريم أفعال المساس بأنظمة الحاسب الآلي و ذلك نتيجة تأثر بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل، مما دفع المشرع الجزائري[3] إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات، والذي أفرد القسم "السابع مكرر" منه تحت عنوان "**المساس بأنظمة المعالجة الآلية**

1. عطاء الله فشار، المرجع نفسه، ص 16

2. في سنة 1994 تم تعديل قانون العقوبات الفرنسي حيث تم إضافة فصلاً ثالثا للباب الثاني تحت اسم "الاعتداءات على نظم المعالجة الآلية للمعطيات" " Des atteintes aux systèmes de traitement automatisé de données" و جاء من المادة 1/323 إلى 7/323 ، Clément ENDRELIN، المرجع السابق، ص76

3. جاء في عرض أسباب هذا التعديل: " أن التقدم التكنولوجي و انتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام مما دفع الكثير من الدول إلى النص على معاقبتها، وإن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية و أساليب المعالجة الآلية للمعطيات، و أن هذه التعديلات من شأنها سد الفراغ القانوني في بعض المجالات، و سوف يُمكن لا محالة من مواجهة بعض أشكال الإجرام الجديد"، عائشة بن قارة مصطفى، المرجع السابق، ص27

للمعطيات، **Des atteintes aux systèmes de traitement automatisé de données** " و الذي تضمن 8 مواد من المادة 394 مكرر إلى 394 مكرر7، و نص على عدة جرائم هي[1]:

- الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو محاولة ذلك (394 مكرر فقرة1).
- الدخول أو البقاء المؤدي إلى تخريب نظام تشغيل المنظومة (394 مكرر3).
- إدخال أو إزالة أو تعديل بطريق الغش معطيات في نظام المعالجة الآلية (395 مكرر1).
- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم (394 مكرر2).
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المتحصل عليها في هذا القسم (394 مكرر2).

في عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب قانون رقم 06 – 23 المؤرخ في 20 ديسمبر 2006 حيث مسّ ذلك التعديل القسم السابع مكرر و الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، و قد تم تشديد العقوبة[2] المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا القسم من قانون 04-15، و ربما يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى و شيوع ارتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الاعمار و مستويات التعليم نتيجة تبسيط وسائل تكنولوجيا المعلومات و انتشار الأنترنت كوسيلة نقل المعلومات حيث بلغ عدد مستخدمي الأنترنت ذات التدفق العالي و عبر الهاتف المحمول 11 مليون شخص لسنة 2012 [3] .

1. نبيل صقر، المرجع السابق، ص128

2. مثال ذلك: " يعاقب على الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية بالحبس من ثلاث(3) أشهر إلى سنة (1) و بغرامة مالية من 000 50 إلى 000 200 دج طبقاً لقانون 06-23 بينما كانت العقوبة على نفس الجريمة من ثلاث أشهر إلى سنة بغرامة مالية من 000 50 إلى 000 100 في قانون 04-15، عائشة بن قارة مصطفى، المرجع السابق، ص29

3. ب س ، بن حمادي يؤكد على عدد مستخدمي الأنترنت، يومية النهار، الجزائر، 1709، 2013/05/17، ص5

الفرع الأول : صور الاعتداءات

تأخذ صور الاعتداء على النظام المعلوماتي في قانون العقوبات الجزائري صورتين أساسيتين هما[1] :

- الدخول و البقاء في منظومة معلوماتية
- المساس بمنظومة معلوماتية

كما تضمن قانون العقوبات صور أخرى للغش في حين أبقى خارج دائرة التجريم بعض الأفعال منها : المساس بحقوق الأشخاص عن طريق المعلوماتية، كجمع المعلومات حول شخص و تحويل المعلومات الاسمية عن مقصدها[2].

أولا: الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات Accès et maintien frauduleux dans un système de traitement automatisé des données.

نصت عليه المادة 394 مكرر قانون العقوبات: "يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 إلى 150000 دج".

إذن فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع فيما الصورة المشددة، تتحقق بتوافر الظرف المشدد لها، و يكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.

- **فعل الدخول L'accès** : لا يقصد بالدخول هنا الدخول بالمعنى المادي، أي الدخول إلى مكان أو منزل أو حديقة، و إنما يجب أن ينظر إليه كظاهرة معنوية، تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية

1. حمزة بن عقون، المرجع السابق، ص182
2. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، الطبعة العاشرة، دار هومة، الجزائر، 2009، ص 445

للمعطيات[1]. و لم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، و لذلك تقع الجريمة بأية وسيلة أو طريقة و يستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر[2].

- **فعل البقاء Le maintien**: يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام و قد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول على النظام، وقد يجتمعان. و يكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا. و من أمثلة ذلك: إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، إذ كان يجب في هذه الحالة على المتدخل أن يقطع وجوده و ينسحب فورًا، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي. و يكون البقاء جريمة إذا تجاوز المتدخل المدة المسموح بها للبقاء بداخل النظام، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيه الرؤية و الاطلاع فقط و يتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات التلفونية، و التي يستطيع فيها الجاني الحصول على الخدمة التلفونية دون أن يدفع المقابل الواجب دفعه أو يحصل على الخدمة مدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة، و قد يجتمع الدخول غير المشروع و البقاء غير المشروع معا و ذلك في الفرض الذي لا يكون فيه الجاني الحق في الدخول إلى النظام ، و يدخل إليه فعلا ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، و يتحقق في هذا الفرض الاجتماع المادي للجرائم و إذا كانت تلك الجريمة على هذه الصورة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، إلا أنها تحقق أيضا و بصورة غير مباشرة حماية المعطيات أو المعلومات ذاتها بل يمكن من خلالها تجريم سرقة وقت الآلة ، و ذلك بالنسبة للموظف أو العامل أو غيرهما حين يسرق وقت الآلة ضد إرادة من له الحق السيطرة على النظام، و يقوم بطبع أو نسخ بعض المعلومات أو المعطيات أو البرامج.[3]

1. أمال قارة، المرجع السابق، ص42
2. د علي عبد القادر قهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة، الاسكندرية، 1999، ص 121
3. أمال قارة، المرجع السابق، ص42

أما عن الصورة المشددة لهذه الجريمة، نصت المادة 394 مكرر 3/2: " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظمة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 دج إلى 150000 دج"، على ظرفين تشدد بهما عقوبة جريمة الدخول و البقاء داخل النظام، ، و يتحقق هذان الظرفان عندما ينتج عن الدخول أو البقاء إما محو أو تعديل المعطيات التي يحتويها النظام و إما عدم صلاحية النظام لأداء وظائفه ، و يكفي لتوفر هذا الظرف وجود علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع و تلك النتيجة الضارة، و لا يشترط أن تكون تلك النتيجة الضارة مقصودة، لأن تطلب مثل هذا الشرط يكون غير معقول ، حيث أن المشرع نص على تجريم الاعتداء المقصود على النظام عن طريق محو أو تعديل المعطيات التي يحتويها باعتباره جريمة مستقلة. كما لا يشترط أن تكون تلك النتيجة مقصودة، أي على سبيل الخطأ غير ألعمدي، فالظرف المشدد هنا ظرف مادي يكفي أن توجد بينه و بين الجريمة العمدية الأساسية و هي جريمة الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافره إلا إذا أثبت الجاني انتفاء تلك العلاقة، كأن يثبت أن تعديل أو محو المعطيات أو أن عدم صلاحية النظام للقيام بوظائفه يرجع إلى القوة القاهرة أو الحادث المفاجئ.

أ- **الركن المادي:** يتمثل الركن المادي لجريمة الدخول و البقاء غير المشروع في نظام المعالجة الآلية و الذي يمتثل أساساً في النشاط الإجرامي بصورتيه البسيطة و المشددة في :

- الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات فعل البقاء.
- البقاء داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام.
- محو أو تعديل المعطيات التي يحتويها النظام.

ب- **الركن المعنوي:** الولوج و التجول و البقاء داخل نظام المعالجة الآلية للمعطيات لا يجرمان إلا تمّا عمداً، كما أن الركن المعنوي لهذه الجريمة تأخذ صورة القصد الجنائي بعنصريه العلم و الإرادة.

فيلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء و أن يعلم الجاني بأنه ليس له الحق في الدخول إلى النظام و البقاء فيه، و عليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاؤه داخل النظام مسموح به أي مشروع، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، كأن يجهل بوجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول، فإذا توافر القصد

الجنائي بعنصريه العلم و الإرادة فإنه لا يتأثر بالباعث على الدخول أو البقاء فيظل القصد قائما حتى و لو كان الباعث هو الفضول أو إثبات القدرة على المهارة و الانتصار على النظام[1].

ثانياً: المساس بمنظومة معلوماتية

يأخذ السلوك الإجرامي لهذه الجريمة إما الاعتداء العمدي على سير نظام المعالجة الآلية[2] للمعطيات أو الاعتداء العمدي على المعطيات[3].

لم يورد المشرع الجزائري نصاً خاصاً بالاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات Atteintes volontaires au fonctionnement de STAD* و اكتفى بالنص على الاعتداء على المعطيات الموجودة بداخل النظام و قد وضع الفقه معيارا للتفرقة بين الاعتداء على المعطيات و الاعتداء على النظام على أساس ما اذا كان الاعتداء وسيلة أم غاية، فاذا كان مجرد وسيلة فان الفعل يشكل جريمة الاعتداء العمدي على النظام، أما اذا كان الاعتداء غاية فان الفعل يشكل جريمة الاعتداء العمدي على المعطيات4، يتمثل هذا السلوك المادي في فعل توقيف نظام المعالجة الآلية للمعطيات من أداء نشاطه العادي و المنتظر منه القيام به، و إما في فعل إفساد نشاط أو وظائف هذا النظام، و لا يشترط أن يقع فعل التعطيل أو فعل الإفساد على كل عناصر النظام جملة، بل يكفي أن يؤثر على أحد هذه العناصر فقط سواء المادية جهاز الحاسب الآلي نفسه، شبكات الاتصال، أجهزة النقل ...الخ، أما المعنوية مثل البرامج و المعطيات[5]. و تتمثل النشاطات غير المشروعة لهذه الجريمة:

- **التعطيل (العرقلة)**: تفترض وجود عمل إيجابي دون أن يشترط المشرع أن يتم التعطيل بوسيلة معينة سواء مادية أو معنوية و سواء اقترنت بالعنف أم لا ،فأما عن الوسيلة المادية فمثلها كسر الأجهزة المادية للنظام أو تحطيم أسطوانة ، أما عن الوسيلة المعنوية فهي التي تقع على الكيانات المنطقية للنظام كالبرامج و المعطيات. و ذلك بإتباع إحدى التقنيات التالية: إدخال برنامج فيروسي، استخدام قنابل منطقية مؤقتة ، جعل النظام يتباطأ في أدائه لوظائفه إلى غيرها من التقنيات.

1. د علي عبد القادر قهوجي، المرجع السابق، ص 136
2. صت عليها المادتين 2 و 8 من اتفاقية بودابست، المجلس الأوروبي، المرجع السابق، ص8
3. هيام حاجب، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، المدرسة العليا للقضاء، الجزائر، 2008، ص47
* . **STAD** : Système de Traitement Automatisé des Données
4. هيام حاجب، المرجع نفسه، ص 48
5. عطاء الله فشار، المرجع السابق، ص27

- **الإفساد Fausser** : و هو كل فعل و إن كان لا يؤدي إلى التعطيل يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها. والافساد من هذه الزاوية يقترب من التعييب الذي يعتبر ظرفا مشددا لجريمة الدخول والبقاء غير المشروع. و الفارق بينهما يكمن في أن الإفساد في حال الظرف المشدد لا يشترط فيه أن يكون عمديا بينما يتطلب هذا الشرط بالنسبة لجريمة الاعتداء القصدي على نظام المعالجة الآلية للمعطيات. و من بين صور الإفساد أو التعييب نجد تقنية استخدام القنبلة المعلوماتية التي تدخل عن طريقها مجموعة معطيات تتكاثر داخل النظام تجعله غير صالح للاستعمال كاستخدام البرنامج المسمى بـ " حصان الطرودة " و الذي يقوم بتغيير غير محسوس في البرامج أو المعطيات[1].

أما الاعتداءات العمدية على المعطيات فلق نص المشرع الجزائري عليها في المادة 394 مكرر2 في قانون العقوبات «يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة من 500000 دج إلى 2000000 دج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريقة الغش المعطيات التي تتضمنها».

تأخذ الصورة الأولى الاعتداءات العمدية على المعطيات الموجودة داخل النظام، فالنشاط الإجرامي في جريمة الاعتداء العمدي على المعطيات يتجسد في إحدى الصور الثلاث التالية[2]:

- الإدخال L'intrusion.
- المحو 'effacement .
- التعديل Modification.

و أفعال الإدخال و المحو و التعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل و هذا يعني أن النشاط الإجرامي في هذه الجريمة إنما يرد على محل أو موضوع محدد و هو المعطيات أو المعلومات التي تمت معالجتها آليا و التي أصبحت مجرد إشارات أو رموزا تمثل تلك المعلومات، و ليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة، كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام، أي التي يحتويها النظام و تشكل جزءا منه. لا تقع الجريمة على مجرد المعلومات التي لم يتم إدخالها بعد إلى النظام أو تلك التي دخلت، و لم يتخذ حيالها إجراءات المعالجة الآلية، أما تلك التي

1. د علي عبد القادر قهوجي، المرجع السابق، ص143
2. هيام حاجب، المرجع نفسه، ص 49

في طريقها إلى المعالجة حتى و لو لم تكن المعالجة قد بدأت بالفعل تتمتع بالحماية الجنائية، و يكون هناك مجال للقول بتوافر الجريمة التامة أو الشروع على حسب الأحوال.

تجدر الإشارة إلى أن الحماية الجنائية تشمل المعطيات طالما أنها تدخل في نظام المعالجة الآلية، أي طالما كان يحتويها ذلك النظام و كانت تكون وحدة واحدة مع عناصره و يترتب على ذلك أن الجريمة لا تتحقق إذا وقع النشاط الإجرامي على المعطيات خارج النظام سواء قبل دخولها أم بعد خروجها و حتى ولو لفترة قصيرة، كما لو كانت مفرغة على قرص أو شريط ممغنط خارج النظام، فالحماية الجنائية تقتصر على المعطيات التي توجد داخل النظام أو تلك التي في طريقها إلى الدخول إليه، أو تلك التي دخلت بعد خروجها، و لا يشترط أن تقع أفعال الإدخال و المحو و تعديل المعطيات بطريق مباشر بل يمكن أن يتحقق ذلك بطريق غير مباشر سواء عن بعد أم بواسطة شخص ثالث.

- **الإدخال L'intrusion**: يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية، أم كان يوجد عليها معطيات من قبل، و يتحقق هذا الفعل في الغرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة، هاته الأخيرة ليسحب بمقتضاها النقود من أجهزة السحب الآلي و ذلك حين يستخدم رقمه الخاص و السري للدخول لكي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه، و كذلك الحامل الشرعي لبطاقة الائتمان و التي يسدد عن طريقها مبلغ أكثر من المبلغ المحدد له و بصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو الفقد أو التزوير، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب« فيروس...الخ» يضيف معطيات جديدة.
- **المحو L'effacement** : يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة و الموجودة داخل النظام أو تحطيم تلك الدعامة، أو نقل و تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.
- **التعديل Modification**: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام و استبدالها بمعطيات أخرى، و يتحقق فعل المحو و التعديل عن طريق برامج غريبة بتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها و ذلك برامج خبيثة[1] كالفيروسات[2] بصفة عامة، و هذه الأفعال المتمثلة في

1.البرامج الخبيثة Malware هي اختصار لكلمتين ، هي برامج يتم تضمينها أو إدراجها عمدًا في نظام الحاسوب لأغراض ضار ، ويكيبيديا، البرامج الخبيثة، 2014/05/14، البرامج الخبيثة http://ar.wikipedia.org/wiki/

2.فيروس الحاسوب هو برنامج خارجي صنع عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما يشبهها من عمليات، ويكيبيديا، فيروس الحاسب، 2014/05/14، فيروس الحاسب http://ar.wikipedia.org/wiki

الإدخال و المحو و التعديل وردت على سبيل الحصر فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى و لو تضمن الاعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات فلا يخضع لتلك الجريمة فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب فيما بينهما، لأن كل تلك الأفعال لا تنطوي لا على إدخال و لا على تعديل بالمعنى السابق.

أما الصورة الثانية فهي جريمة المساس العمدي بالمعطيات خارج النظام التي وفر المشرع الجزائري الحماية الجزائية للمعطيات في حد ذاتها من خلال تجريمه السلوكيات التالية:

- نص المادة 394 مكرر 2 تستهدف حماية المعطيات في حد ذاتها لأنه لم يشترط أن تكون داخل نظام معالجة آلية للمعطيات أو أن يكون قد تم معالجتها آليا، فمحل الجريمة هو المعطيات سواء كانت مخزنة، كأن تخزن في أشرطة أو أقراص أو تلك المعالجة آليا أو تلك المرسلة عن طريق منظومة معلوماتية، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.
- نص المادة 394 مكرر 2/2 يجرم أفعال الحيازة، الإفشاء، النشر، الاستعمال أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات بأهداف المنافسة غير المشروعة، الجوسسة، الإرهاب، التحريض على الفسق... الخ.

أ- الركن المادي:

يعد مساساً بالأنظمة المعلوماتية هو إحدى النشاطات غير المشروعة الواردة و المتمثلة في الصورة التالية: التعطيل أو الإفساد او المحو أو التعديل أو الإدخال و التي لا يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقط لكي يتوافر الركن المادي[1] بالإضافة إلى ما أوردته المادة 394 مكرر 2 ، تصميم أو البحث أو التجميع أو توفير أو نشر أو إتجار معلومات مختزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي و كذلك الحيازة أو الإفشاء أو استعمالها لأي غرض آخر.[2]

1. هيام حاجب، المرجع السابق، ص 48
2. حمزة بن عقون، المرجع السابق، ص185

ب- الركن المعنوي:

إن الركن المعنوي إن هذه الجريمة جريمة عمدية، إذ أن من المفترض أن أفعال العرقلة والتعطيل لا تكون إلا عمدية وهذا ما يميزه عن الاعتداء غير العمدي لسير النظام الذي يشكل ظرفا مشددا لجريمة الدخول والبقاء الغير مشروع داخل النظام وعليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة[1].

أما الصورة الأولى من الاعتداءات العمدية على المعطيات الموجودة داخل النظام كجريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل كما يجب أن يعلم الجاني بان نشاطه الجرمي يترتب عليه التلاعب في المعطيات، ويعلم أيضا أن ليس له الحق في القيام بذلك وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته، كما يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش ، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه ، وان كان الضرر قد يتحقق في الواقع نتيجة النشاط الإجرامي إلا انه ليس عنصرا في الجريمة .

الصورة الثانية فهي جريمة المساس العمدي بالمعطيات خارج النظام فان هذا المساس يجب أن يكون عمدا وبطريق الغش أي بتوافر القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش.

الفرع الثاني : الجزاءات المقررة

طبقا للمادة 13 من اتفاقية بودابست فإن العقوبات المقررة للإجرام المعلوماتي يجب أن تكون رادعة وتتضمن عقوبات مالية للحرية، والتي تتمثل في عقوبات أصلية وعقوبات تكميلية تطبق على الشخص الطبيعي، كما توجد عقوبات تطبق على الشخص المعنوي بناءًا على تبني مبدأ مسالة الشخص المعنوي الواردة في المادة 12من الاتفاقية.

1. د. علي عبد القادر القهوجي، المرجع السابق، ص 136

أولاً: العقوبات المطبقة على الشخص الطبيعي

أ- **العقوبات الأصلية** : من خلال استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا وجود تدرج داخل النظام العقابي. هذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات ،إذ نجد سلم خطورة يتضمن ثلاث درجات ،جريمة الدخول أو البقاء بالغش في الدرجة الأولى وبعدها في الدرجة الثانية جريمة الدخول والبقاء المشددة، أما الدرجة الثالثة فتحتلها الجريمة الخاصة بالمساس العمدي بالمعطيات.

- **الدخول والبقاء بالغش (الجريمة البسيطة)**: العقوبة المقررة هي 3 أشهر إلى سنة حبس و 50000 دج إلى 100000 دج غرامة (المادة 394 مكرر) .
- **الدخول والبقاء بالغش (الجريمة المشددة)**: تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة ،وتكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة من 50000 دج إلى 150000 دج إذا ترتب عن الدخول أو البقاء غير المشروع تخريب لنظام اشتغال المنظومة (المادة 394 مكرر/02-03) .
- **الاعتداء العمدي على المعطيات**: طبقا لنص المادة 394 مكرر 2 فالعقوبة المقررة للاعتداء ألعمدي على المعطيات الموجودة داخل النظام هي الحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500000 دج إلى 2000000 دج أما العقوبة المقررة لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية، العقوبة المقررة هي الحبس من شهرين إلى ثلاث سنوات وغرامة من 1000000 دج إلى 5000000 دج.

بالإضافة إلى تشديد العقوبة في الحالات التالية:

- نصت المادة 394 مكرر /2-3 على ظرف تشدد به عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام، ويتحقق هذا الظرف عندما ينتج عن الدخول و البقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة، ففي الحالة الأولى تضاعف العقوبات المقررة في الفقرة الأولى من المادة 394 مكرر ،و في الحالة الثانية تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج .

- نصت المادة 394 مكرر 3 على أن تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية وذلك إذا استهدفت الجريمة الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام

ب- **العقوبة التكميلية:** نصت المادة 394 مكرر 3 قانون العقوبات على العقوبات التكميلية إلى جانب العقوبات الأصلية و المتمثلة في:

- **المصادرة:** وهي عقوبة تكميلية تشمل الأجهزة والبرامج و الوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير حسن النية.
- **إغلاق المواقع:** والأمر يتعلق بالمواقع (Le sites) التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.
- **إغلاق المحل أو مكان الاستغلال:** إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك إغلاق المقهى الالكتروني الذي ترتكب منه مثل هذه الجرائم شرط توافر عناصر العلم لدى مالكها.

ثانياً: العقوبات المطبقة على الشخص المعنوي

مبدأ مساءلة الشخص المعنوي وارد في المادة 12 من اتفاقية بودابست، بحيث يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا كما يسأل عن الجريمة التامة أو الشروع فيها ،كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه[1].

هذا مع ملاحظة أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة.

كما تجدر الإشارة إلى أن المشرع الجزائري قد اقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي وذلك في نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات الذي ينص على أن: " العقوبات المطبقة على الشخص المعنوي في مواد الجنايات و الجنح هي:

1. عطاء الله فشار، المرجع السابق، ص 33

أ- العقوبة الاصلية:

الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة(394 مكرر 4).

ب- العقوبة التكميلية: واحدة أو أكثر من العقوبات الآتية[1]:

- حل الشخص المعنوي
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز 5 سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر أو تعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات ،وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته .

نشير بالذكر أن المشرع الجزائري لم يغفل عن معاقبة الاشتراك[2] حيث تنص المادة 394 مكرر 5 من قانون العقوبات : "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية ،يعاقب بالعقوبات المقررة بالجريمة ذاتها ".

إن الحكمة التي ارتآها المشرع من تجريم الاشتراك في مجموعة أو في اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية هو أن مثل هذه الجرائم تتم عادة في إطار مجموعات، كما أن المشرع ورغبته في توسيع نطاق العقوبة أخضع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا تمت في إطار اتفاق جنائي، بمعنى أن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص.

1. المادة 18 مكرر ، قانون 04-15ا لمؤرخ في 10 نوفمبر 2004
2. هيام حاجب، المرجع السابق، ص 51

أما عقوبة الشروع في الجريمة نصت عليه المادة 11 من اتفاقية بودابست وتبناه المشرع الجزائري في المادة 394 مكرر 7 من قانون العقوبات، فالجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي ولا عقاب على الشروع في الجنح إلا بنص.

نصت المادة 394 مكرر 7 قانون العقوبات:" يعاقب على الشروع في ارتكاب جنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها ".

يبدو من خلال هذا النص رغبة المشرع في توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية ،إذ جعل الشروع في إحدى الجرائم الماسة بالأنظمة المعلوماتية معاقب بنفس عقوبة الجريمة التامة، ومن خلال استقراء نص المادة نستنتج أن الجنحة الواردة بنص المادة 394 مكرر5 من قانون العقوبات مشمولة بهذا النص، أي أن المشرع الجزائري بهذا المنطق يكون قد تبنى فكرة الشروع في الاتفاق الجنائي.[1]

المطلب الثاني : في ظل قانون 09-04 المؤرخ في 05 أوت 2009

دفع القصور الذي عرفه قانون 04-15 و المعدل لقانون العقوبات الذي نص على حماية الجزائية جزائية نسبية لأنظمة المعلومات من خلال تجريم مختلف أنواع الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، بالمشرع الجزائري إلى سد الفراغ التشريعي الذي يعرفه مجال الجرائم المتعلقة بوسائل الإعلام و الاتصال و خاصة الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، خاصة في ظل الثورة التي تعرفها في مجال استخدام الأنترنت، و ذلك بوضع قانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، من أجل تعزيز القواعد السابقة.

تكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية و بين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة و التدخل السريع لتحديد مصدرها و التعرف على مرتكبها.

1. عطاء الله فشار، المرجع السابق، ص 35

كما أخذ المشرع في عين الاعتبار الصعوبات التي تثيرها المصطلحات القانونية المتعلقة بهذه المادة ، لذلك تم اختيار عنوان القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها حتى يكون النص مرتبطاً بتقنيات تشهد تطوراً مستمراً بقدر ما يرتبط بالأهداف و الغايات التي ترمي إليها هذه التكنولوجيا، كما أن التركيز على المجالي الإعلام و الاتصال بين مقاصد النص الذي يهدف إلى جعل المتعاملين في مجال الاتصالات السلكية و اللاسلكية شركاء في مكافحة هذا الشكل من الإجرام و الوقاية منه[1].

يتضمن قانون 09-04 على ستة فصول نلخصها في :

نص الفصل الأول على الأحكام العامة التي تبين الأهداف المتوخاة من هذا القانون، و تحدد مفهوم مصطلح التقنية الواردة فيه و كذا مجال تطبيق أحكامه، حيث عرف الجرائم المرتكبة بتكنولوجيات الاعلام و الاتصال على أنها هي الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات ، أما المنظومة المعلوماتية على أنها أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المترابطة، ويقوم واحد منها أو أكثر بمعالجة آلية المعطيات تنفيذا لبرنامج معين، أما المعطيات فعرفها المشرع الجزائري على أنها أي عملية عرض و طرح للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، كما عرف الاتصالات الالكترونية على أنها أي تراسل أو ارسال أو استقبال علامات و اشارات أو صور أو معلومات مختلفة بواسطة أي وسيلة الكترونية[2].

و جسد الفصل الثاني أحكام خاصة بمراقبة الاتصالات الالكترونية، وقد روعي في هذه القواعد خطورة التهديدات المحتملة و أهمية المصالح المحمية، وحدد الحالات التي يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات و الاتصالات الالكترونية، و قيدها بإذن مكتوب من السلطات القضائية المختصة .

1. أحمد عمراني، المرجع السابق، ص15
2. المادة 1،2،3 من قانون 09-04 المؤرخ في 5 أوت 2009

أما الفصل الثالث فتضمن القواعد الإجرائية، و هذا بالنص على قواعد إجرائية خاصة بالتفتيش و الحجز في مجال الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال، و ذلك وفقاً للمعايير العالمية المعمول بها في هذا الشأن و مع ما تضنه قانون الإجراءات الجزائية من مبادئ عامة.

الفصل الرابع تطرق إلى التزامات المتعاملين في مجال الاتصالات الالكترونية، ولاسيما إلزامية حفظ المعطيات المتعلقة بحركة السير و التي من شأنها المساعدة في الكشف عن الجرائم و مرتكبيها[1]، حيث يهدف هذا القانون إعطاء مقدمي الخدمات دوراً إيجابياً و مساعداً للسلطات العمومية في مواجهة الجرائم و الكشف عن مرتكبيها، حيث ألزم مقدمي الأنترنت على التدخل الفوري لسحب الفوري لسحب المحتويات التي بإمكانهم الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها القانون، وتخزينها أو جعل الدخول إليها غير ممكن، إضافة إلى وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول للموزعات التي تحتوي مخالفات للنظام العام والآداب العامة و إخطار المشتركين لديهم بوجودها.

أشار الفصل الخامس لوجود الهيئة الوطنية للوقاية من الإجرام المتصل بتكنولوجيات الاعلام و الاتصال و مكافحته، إذ نص القانون على إنشاء هيئة وطنية ذات وظيفة تنسيقية في مجال الوقاية من هذه الجرائم، و أحال على التنظيم تحديد كيفية تشكيل و تنظيم هذه الهيئة.

نص الفصل السادس على التعاون و المساعدة القضائية الدولية، إذ تناول قواعد الاختصاص القضائي و التعاون الدولي بوجه عام :

- فيما يخص الاختصاص القضائي فهو فضلاً عن قواعد الاختصاص العادية فقد تم توسيع اختصاص المحاكم الجزائية للنظر في الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال التي ترتكب من طرف الرعايا الأجانب عندما تكون المصالح الاستراتيجية للجزائر مستهدفة.
- فيما يتعلق بالتعاون الدولي فهو يقوم على مجوعة من المبادئ العامة في مجال التعاون الدولي لمكافحة هذا النوع من الجرائم خاصة ما يتعلق منها بالمساعدة و تبادل المعلومات، حيث تم اعتماد مبدأ التعاون على أساس المعاملة بالمثل[2].

1. المواد 10،11،12 من نفس القانون
2. أحمد عمراني، المرجع السابق، ص17

الفرع الأول : القواعد الإجرائية

أولاً: التفتيش و الحجز

أجاز هذا القانون للجهات القضائية و ضباط الشرطة القضائية الدخول و التفتيش و لو عن بعد إلى منظومة معلوماتية أو جزء منها، و كذلك المعطيات الآلية المخزنة فيها، مع إمكانية اللجوء مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي، كما يسمح هذا القانون في المادتين 5 و 6 للمحققين باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها[1]، و حجزها.

ثانياً: التعاون القضائي الدولي

تنص المادة 16 من نفس القانون على إمكانية تبادل المعلومات في الشكل الإلكتروني، أما الفقرة الثانية إمكانية استعمال وسائل الاتصال السريعة مثل البريد الإلكتروني و الفاكس في حالة الاستعجال مع القيام بالإجراءات التحفظية اللازمة و ذلك وفق مبدأ التعاون على أساس المعاملة بالمثل.

الفرع الثاني: القواعد الوقائية

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال

أنشئت بموجب المادة 14 من القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، و من مهامها :

- إدارة و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام الاتصال.
- المساعدة التقنية للجهات القضائية و الأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية.
- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي هذا النوع من الجريمة، مع تفعيل التعاون القضائي و الأمني الدولي.

1. عطاء الله فشار، المرجع السابق، ص 36

ثانياً: مراقبة الاتصالات الالكترونية

نصت المادة 4 من قانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها الحالات التي يسمح فيها باللجوء إلى المراقبة الالكترونية[1]:

- للوقاية من السلوكيات الموصوفة بجرائم الارهاب أو التخريب أو الجرائم الماسة بأمن الدولة، الدولة، بإذن من النائب العام لدى مجلس قضاء الجزائر لمدة ستة أشهر قابلة للتجديد.
- في حالة توافر معلومات على احتمال القيام بالاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الاقتصاد الوطني.
- لمقتضيات التحريات و التحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الالكترونية.
- في مجال تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

واكب المشرع الجزائري مختلف التطورات التشريعية التي تم سنها من أجل تنظيم المعاملات التي تتم من خلال الوسائط الالكترونية بما فيها الانترنت، خاصة التي تهدف إلى الحد من الاستخدام غير المشروع لها، و ذلك مراعاة منه لما يشهده العالم من تطورات كبيرة في مجال الاعلام و الاتصال خاصة الأنترنت.

و من جهة أخرى إيماناً منه بأن الجزائر ليست بمعزل عن التطورات الإجرامية التي تحدث في العالم، خاصة في ظل التنامي المتسارع لاستعمال الانترنت، فكانت محاولات المشرع الجزائي الحد من هذه الظاهرة في استحداثه للقسم السابع مكرر من قانون العقوبات 04-15 و كذا قانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحته.

1. يوسف صغير، المرع السابق، ص 113

الخاتمة

الخاتمــة

لقد بات من المحتم على شعوب العالم الانصهار في بوتقة المعلوماتية كنتيجة حتمية لمواكبة التطور التقني و التكنولوجي في ظل التحول الالكتروني لمختلف نواحي الحياة لتحقيق المجتمع الافتراضي، في ظل عالم مفتوح تتسيده المعلومات، و التي أضحت و بحق مصدر القوة و المعرفة، و أضحت المعيار المحدد لتطور و نمو الشعوب و مستقبلها، و ذلك بزيادتها للفوارق الاقتصادية و الاجتماعية القائمة بين مجتمع و آخر.

و نتيجة التطور العلمي الهائل، فإن المحاسن التي جلبتها المعلوماتية قد جلبت إلى جانبها أيضاً مخاطر عدة ناجمة عن إساءة استخدام الكمبيوتر و شبكة الانترنت و تطويعها لصالح المجرم المعلوماتي لممارسة نشاطاته الجرمية، و لهذا يرى البعض أن ارتفاع مستوى التعليم و سهولة الحصول على الجهاز رفع مستوى الأداء الاجرامي و تنوعه، أي مستوى الاتقان و الاحتراف، و من ثم تؤدي إلى ارتكاب أفعال إجرامية أكثر دقة، في التخطيط، و أكثر براعة في التنفيذ و هذا من شأنه أن يصعب إمكانية اكتشافها، فالتقنية الحديثة سهلت ظهور طائفة جديدة من الجرائم المستحدثة، والتي تعجز النصوص العقابية التقليدية على مواجهة أغلب صورها، و إن وجدت نصوص عقابية حديثة فلا بد ان تكملها استراتيجية مختلفة على المستوى الفني و التقني و القضائي، وذلك لمراقبة الأمن في مجال تقنية المعلومات أو في مجال التدريب، أو في مجال التعاون و التنسيق الدولي لمواجهة هذا النوع المعقد من السلوك الإجرامي الحديث.

و من خلال هذا البحث توصلنا إلى جملة من النتائج و الاقتراحات الآتية:

أولاً: النتائج

بالنظر لحداثة هذا السلوك الإجرامي و الذي يتجسد في الجريمة المعلوماتية، فإنه لا يوجد لحد الآن إجماع فقهي موحد على تعريف لها مما أدى القول بأن الجريمة المعلوماتية تقاوم التعريف، ومن خلال استعراضنا لمختلف التعاريف الفقيهة والتي جاءت متفاوتة بين التضييق و التوسع و من تعريف قانوني إلى تعريف تقني ، توصلنا إلى أن الإخفاق في تعريف الجريمة المعلوماتية يفسره اتجاه يسمح بسهولة إضفاء وصفها على أي واقعة لها علاقة بالحاسوب أياً كانت هذه العلاقة و أيا كان دور الحاسوب فيها، سواء كان وسيلة أو مناسبة لارتكاب الجريمة، أو كان موضوعا لها، و عليه لأننا نقترح التعريف التالي:

الخاتمــة

تعد جريمة معلوماتية كل جريمة يمكن ارتكابها بواسطة شبكة حاسوبية او داخل نظام معلوماتي، وتشمل تلك الجريمة جميع الجرائم التي يمكن ارتكابها سواء على تكنولوجيا المعلومات أو المرتكبة بواسطة المعلوماتية.

و عليه فإن الركن الشرعي للجريمة يستهدف تجريم كل أشكال الاعتداء على النظم المعلوماتية و حماية النظام يعني حماية البيانات، و بالنسبة للركن المادي للجريمة يشمل صمرتين أساسيتين هما:

- الاعتداء على نظام المعالجة الآلية للمعطيات
- الاعتداء على مضمون النظام

ومن النتائج المستخلصة و التي أثارت الكثير من الجدل في مختلف الاتجاهات القانونية، مسألة تحديد قائمة بجرائم الكمبيوتر بصفة خاصة و الانترنت بصفة عامة.

- إن جرائم الكمبيوتر تستهدف المعطيات ذات الطبيعة المعنوية، فعندما يكون جهاز الحاسوب هدفاً للجريمة فإن السلوك يستهدف المعلومات المخزنة لديه أو المنقولة لديه أو منه، باستخدام طرق تقنية في بيئة معنوية و ليست بيئة سلوكيات مادية.
- أن مبدأ الشرعية الجنائية يمنع المساءلة القانونية ما لم يتوفر النص القانوني فلا جريمة و لا عقوبة إلا بنص، و متى ما انتفى النص على تجريم مثل هذه الأفعال التي لا تطالها النصوص القائمة، امتنعت المسؤولية و تحقق القصور في مكافحة هذه النوعية من الجرائم المستحدثة.
- أن القياس في النصوص الجنائية الموضوعية محضور وغير جائز، و مؤدى ذلك امتناع قياس انماط جرائم المعلوماتية على الجرائم التقليدية التي تستهدف الأموال، كقياس سرقة المعلومات على جريمة الاستيلاء على الكهرباء بطريقة غير شرعية.
- تتسم الجريمة المعلوماتية بطابع التعقيد و الغموض إذ يصعب وضع قواعد قانونية منضبطة تحكم جميع السلوكيات، لأن هاته السلوكيات تتطور بتطور التقنية.
- هناك بعض السلوكيات الإجرامية المستحدثة يصعب تحديد الركن المادي لها، و يصعب تكييفها، كالاعتداء على البيانات الإسمية للأشخاص.

الخاتمــة

- أثارت شبكة الأنترنت اعقد المشاكل في مسألة الاختصاص القضائي و القانون الواجب التطبيق على الممارسات الإجرامية في نطاق الشبكة، مما يثير مسالة تطبيق النصوص الجزائية من حيث الزمان أو النصوص الجزائية من حيث المكان، و مدى صلاحيتها للتطبيق على هذه الممارسات، و لاسيما أنها قد تكون خاضعة للعقاب في دول و مباحة في دول أخرى.
- و من النتائج المستخلصة أيضاً مدى الحرص الكبير التي أولته الدول و المنظمات العالمية للجريمة المعلوماتية، بالنظر لخطورتها و التأثير لسلبي الكبير الذي قد يرجع عليها إذا ما تراخت في مواجهتها و مكافحتها و كذا الجهود المبذولة في هذا المجال.

و في الأخير لا يسعنا إلا بالتنويه بالسياسة التشريعية التي تسير عليها الجزائر في اطار مكافحتها للجريمة المعلوماتية، حيث أورد المشرع الجزائي قانون المساس بأنظمة المعالجة الآلية للمعطيات رقم 05-15 المؤرخ في 10 نوفمبر 2004، كما أصدر القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، لذلك خلص لدينا أن المشرع الجزائري اتسم بالإيجابية في محاربة هذا السلوك الاجرامي، ولكن لا ينفي وجود بعض النقائص.

ثانياً: الاقتراحات

في ضوء النتائج السابقة التي أظهرتها الدراسة نخلص إلى بعض التوصيات و تتمثل في:

- ضرورة إعطاء تعريف موسع للجريمة المعلوماتية، و إعطاء لكل سلوك إجرامي نص مجرم له، وذلك بالتحديد الواضح و الدقيق لصور السلوك المراد تجريمه.
- خلق ثقافة اجتماعية جديدة تصور جرائم الأنترنت علة أنها أعمال غير مشروعة مثلها مثل الأنماط الأخرى، و التأكيد على أن المجرم المعلوماتي يستهدف الإضرار بالآخرين، و سيتحق العقوبة بذل نظرات و عبارات الاعجاب.
- ضرورة تدريب و تأهيل أفراد الضبطية القضائية و كذا النيابة و القضاء على كيفية التعامل مع هذا النوع من الجرائم و تحقيق التعاون مع التقنيين من أصحاب الخبرة، وذلك بعقد دورات تدريبية بشكل دوري و دائم للاستفادة من خبراتهم و إرشادهم، ابتداءاً من مرحلة الاستدلال و جمع الأدلة، وانتهاءاً بقرارات المحاكم.

الخاتمــة

- تدريس مواد الانظمة المعلوماتية و الجرائم التي قد تنشأ منها في المدراس بشكل مبسط ثم في كليات الحقوق و المعاهد القضائية.
- النص بشكل واضح و صريح على مسؤولية الشخص المعنوي على جرائم الحاسب الآلي إفراد العقوبات المناسبة له.
- تفعيل دور الأسرة في متابعة الأبناء لوقايتهم من الآثار السلبية و المخاطر المترتبة عن الاستخدام غير الآمن لشبكات الأنترنت.
- التطوير المستمر للتشريعات القائمة بما يحقق مرونتها و مواكبتها للتطورات المتسارعة في مجال تكنولوجيا المعلومات.
- محاولة الاستفادة من الامكانيات التي يتمتع بها المجرم المعلوماتي و توظيفها في خدمة المجتمع وفقاً للقانون رقم 09-01 المتعلق بالعمل للنفع العام.
- إعطاء صلاحيات واسعة للهيئة الوطنية للوقاية من الإجرام المتصل بتكنولوجيا الاعلام و الاتصال ومكافحته.
- ضرورة التعاون الدولي لمواجهة الجرائم في بيئة المعلوماتية الالكترونية و ذلك من خلال الدخول في الاتفاقيات و معاهدات تجرم صور هذه الجرائم، ومن هذا المنطلق هذا ما يجب أن يحدث للجزائر و ضرورة انضمامها لاتفاقية بودابست 2001 لمكافحة الجريمة المعلوماتية.

الملاحق

Chapitre II – Mesures à prendre au niveau national

Section 1 – Droit pénal matériel

Titre 1 – Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 4 – Atteinte à l'intégrité des données

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Article 5 – Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Article 6 – Abus de dispositifs

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:

a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:

i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;

ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique,

dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et

b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

Titre 2 – Infractions informatiques

Article 7 – Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8 – Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui:

a par toute introduction, altération, effacement ou suppression de données informatiques;

b par toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Titre 3 – Infractions se rapportant au contenu

Article 9 – Infractions se rapportant à la pornographie enfantine

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:

a la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique;

b l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique;

c la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique;

d le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique;

e la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

2 Aux fins du paragraphe 1 ci-dessus, le terme «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle:

a un mineur se livrant à un comportement sexuellement explicite;

b une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;

c des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

3 Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.

4 Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.

Titre 4 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

3 Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.

Titre 5 – Autres formes de responsabilité et de sanctions

Article 11 – Tentative et complicité

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.

3 Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

Article 12 – Responsabilité des personnes morales

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé:

a sur un pouvoir de représentation de la personne morale;

b sur une autorité pour prendre des décisions au nom de la personne morale;

c sur une autorité pour exercer un contrôle au sein de la personne morale.

2 Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

3 Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.

4 Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

Article 13 – Sanctions et mesures

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

2 Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.

Section 2 – Droit procédural

Titre 1 – Dispositions communes

Article 14 – Portée d'application des mesures du droit de procédure

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article:

a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention;

b à toutes les autres infractions pénales commises au moyen d'un système informatique; et

c à la collecte des preuves électroniques de toute infraction pénale.

3 a Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.

b Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services:

i qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et

ii qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé,

cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

Article 15 – Conditions et sauvegardes

1 Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3 Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

Titre 2 – Conservation rapide de données informatiques stockées

Article 16 – Conservation rapide de données informatiques stockées

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2 Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 17 – Conservation et divulgation rapides de données relatives au trafic

1 Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires:

a pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; et

b pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Titre 3 – Injonction de produire

Article 18 – Injonction de produire

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:

a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et

b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

3 Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;

b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;

c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Titre 4 – Perquisition et saisie de données informatiques stockées

Article 19 – Perquisition et saisie de données informatiques stockées

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire:

a à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et

b à un support du stockage informatique permettant de stocker des données informatiques sur son territoire.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes:

a saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique;

b réaliser et conserver une copie de ces données informatiques;

c préserver l'intégrité des données informatiques stockées pertinentes;

d rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

4 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.

5 Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

Titre 5 – Collecte en temps réel de données informatiques

Article 20 – Collecte en temps réel des données relatives au trafic

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes:

a à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et

b à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes:

i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2 Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.
3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.
4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 21 – Interception de données relatives au contenu

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne :
a à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et
b à obliger un fournisseur de services, dans le cadre de ses capacités techniques:
i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou
ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,
en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.
2 Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.
3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.
4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Section 3 – Compétence

Article 22 – Compétence

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise:
a sur son territoire; ou
b à bord d'un navire battant pavillon de cette Partie; ou
c à bord d'un aéronef immatriculé selon les lois de cette Partie; ou
d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.
2 Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à 1.d du présent article ou dans une partie quelconque de ces paragraphes.
3 Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.
4 La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.
5 Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de déterminer la mieux à même d'exercer les poursuites.

قائمة المراجع

قائمة المراجع

أولاً: العربية

1. المراجع العامة

- **د. أحسن بوسقيعة** ، الوجيز في القانون الجزائي العام ، الطبعة الثالثة ، دار هومه، 2006

- **د. أحسن بوسقيعة**، الوجيز في القانون الجزائي الخاص، الجزء الأول، الطبعة العاشرة، دار هومة، الجزائر، 2009

- **د. شعبان خليفة** ، قاموس البنهاوي الموسوعي في مصطلحات المكتبات والمعلومات، دار المريخ ، 1990

- **د. منذر الشاوي** ، فلسفة القانون، مطبوعات المجمع العلمي بالعراق، بغداد 1994

2. المراجع المتخصصة

- **د أحمد خليفة الملط** ،الجرائم المعلوماتية ، الطبعة الثانية، دار الفكر الجامعي، 2006

- **د جميل عبد الباقي الصغير** ، الجوانب الاجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة ،2002

- **د ذكي ذكي امين حسونة** ، جرائم الكمبيوتر و الجرائم الأخرى ، دار النهضة، القاهرة

- **د طارق ابراهيم الدسوقي عطية**، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، 2009

- **د علي جبار الحسناوي** ، جرائم الحاسوب و الأنترنت ، دار اليازوي العلمية للنشر و التوزيع ، عمان ، 2009

- **د علي عبد القادر قهوجي**، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة، الاسكندرية، 1999،

- **د عماد مجدي عبد الملك** ، جرائم الكمبيوتر و الأنترنت ، دار المطبوعات الجامعية، الإسكندرية، 2011

- **د. عبد الفتاح بيومي حجازي** ،الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية، مصر ،2002

- **عائشة بن قارة مصطفى**، حجية الدليل الالكتروني في مجال الإثبات، دار الجامعة الجديدة، الاسكندرية، 2010

- **عبد الله عبد الكريم عبد الله** ، جرائم المعلوماتية و الأنترنت دراسة مقارنة ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، 2007

- **محمد أحمد عبابنة**، جرائم الحاسوب و أبعادها الدولية ، دار الثقافة ، عمان ، 2005

- **مسعود خثير** ،الحماية الجنائية لبرامج الكمبيوتر أساليب و ثغرات،دار الهدى، 2010

- **د. محمد سامي الشوا**، ثورة المعلومات و انعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة ،1994

- **د نائلة عادل محمد قورة** ، جرائم الحاسب الإقتصادية دراسة نظرية و تطبيقية ، ط1 ، دار النهضة العربية ، القاهرة ، 2003

- **نبيل صقر** ، جرائم الكمبيوتر و الأنترنت في التشريع الجزائري ، دار الهلال للخدمات، 2009

– د هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، ط1 ، دار النهضة العربية ، القاهرة ، 1992

- **د هشام محمد فريد رستم** ، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1995

- **د هلالي عبد اللاه أحمد** ،جرائم المعلوماتية و أساليب المواجهة و فقاً لاتفاقية بودابست،ط1، دار النهضة، القاهرة، 2007

3. النصوص القانونية

– القانون 04– 15 مؤرخ في 10 نوفمبر 2004 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، 10 نوفمبر 2004

- **القانون 06–22** المؤرخ في 20 ديسمبر 2006 المعدل و المتمم للأمر55-165 المؤرخ في 08 يونيو 1965 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 84، الجزائر، 24 ديسمبر 2006

- **القانون 09–04** المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها، الجريدة الرسمية، 47، الصادر في 16 أوت 2009 .

4. الرسائل الجامعية

أ- الدكتوراه

- **سالم محمد سليمان الأوجلي**، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، مذكرة دكتوراه ،جامعة عين شمس، 1997

- **غازي عبد الرحمن هيان الرشيد** ، الحماية القانونية من جرائم المعلوماتية (الانترنت) ،مذكرة دكتوراه ، الجامعة الإسلامية، لبنان ،2004

ب- الماجستير

- **حمزة بن عقون**، السلوك الإجرامي للمجرم المعلوماتي، مذكرة ماجستير حقوق، جامعة الحاج لخضر باتنة، الجزائر، 2012

- **سفيان سوير** ، جرائم المعلوماتية ، مذكرة ماجستير ، جامعة أبو بكر بلقايد تلمسان ،الجزائر ، 2010

- **محمد بن نصير سرحاني**، مهارات التحقيق الجنائي الفني في جرائم الحاسوب و الأنترنت، مذكرة ماجستير في العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، 2004

- **نعيم سعيداني** ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة ماجستير ، جامعة الحاج لخضر باتنة، الجزائر، 2012

- **يوسف صغير** ، الجريمة المرتكبة عبر الأنترنت ، مذكرة ماجستير ، جامعة مولود معمري تيزي وزو، الجزائر، 2013

ت- الرسائل الأخرى

- **هيام حاجب**، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، المدرسة العليا للقضاء، الجزائر، 2008

5. التظاهرات العلمية

- **أحمد عمراني**، نظام المعلومات في القانون الجزائري، المؤتمر السادس لجمعية المكتبات و المعلومات السعودية، الرياض، 2010

- **جان فرنسوا هنروت**، أهمية التعاون الدولي بين عناصر الشرطة، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية،19-20 جوان 2007

- **راسل تاينر**، أهمية التعاون الدولي في منع جرائم الإنترنت، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، 19 06 2007

- **عطاء الله فشار**، مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغاربي حول القانون و المعلوماتية، أكاديمية الدراسات العليا، ليبيا، أكتوبر 2009

- **يونس عرب** ، قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، مسقط، 2-4 أبريل 2006

6. المجلات

- **عواطف محمد عثمان عبد الحليم** ،جرائم المعلوماتية ، مجلة العدل ، العدد الرابع و العشرون

- **محمد فولان**، الحماية القانونية لتكنولوجيات الإعلام، مجلة المحكمة العليا، الجزائر، العدد01، 2010

7. التقارير

- **د حسين بن سعيد بن سيف الغفري**، المنشاوي للبحوث و الدراسات، الجهود الدولية في مواجهة جرائم الأنترنت ،الرياض، 2007

8. الصحف

- **ب س** ، بن حمادي يؤكد على عدد مستخدمي الأنترنت، يومية النهار، الجزائر، 1709، 2013/05/17

ثانيًا: المراجع باللغة الأجنبية

1. الفرنسية

A– Ouvrages

- **David Fayon**, L'informatique, Vuibert, Paris,1999
- **Tiedemann** , Fraude et autres délits d'affaire commis à l'aide d'ordinateurs , RDPC, 1984

- **Lucas** , le droit de l'informatique, vol2, Thiémis, Paris 1998
- **Piérre CATALA** , la propriété de l'information cité par f. Toubal le logiciel- analyse juridique FUDUL .L.G.D.J.1986

B– Thèses

- **Clément ENDRELIN** , Les moyens juridiques de lutte contre la cybercriminalité , Diplôme universitaire sécurité intérieur/extérieur dans l'Union Européen , 2011

C–Rapports

- **Masse** , Rapport final du conseil de l'Europe sur la criminalité en relation avec l'ordinateur, 1988
- **Rose Philipe**, La criminalité informatique à l'horizon analyse prospective, 2005
- **Duleroy** , Les escrocs a l'informatique ,le nouvel économiste , Octobre 2002

2. الانجليزية :

– Parker Donn , Computer Abus , Stanford Research , 1973

- **Totty et Hardcastle**, Computer related crime in information technology andthelaw , UK , 1986

- **Suthreland** (**Eduin H**) ,White collar criminality , Gers (Gilbert) in white collar criminal The offender in business the professions,1968

ثالثًا: مواقع الأنترنت

http://ar.wikipedia.org/wiki/ فيروس أحبك

http://www.un.org/arabic/documents

http://ar.wikipedia.org/Interpol

http://www.interpol.int/ar/الإجرام-السيبيري

http://conventions.coe.int/Default.asp?pg=Treaty/Translations/TranslationsChart_en.htm#185

http://ar.wikipedia.org/wiki/البرامج الخبيثة

http://ar.wikipedia.org/wiki/فيروس الحاسب

www.google.com