تاريخ الاستلام:.2022/05/08 تاريخ القبول: 2022/12/08.

الجريمة المعلوماتية في القانون الدولي و الجزائري

Information crime in international and Algerian law

خلدون عيشة

جامعة زيان عاشور بالجلفة (الجزائر)

achwak17@yahoo.com

ملخص:

ترتكب الجريمة المعلوماتية في نطاق تقنيات التكنولوجيا و الإعلام و الإتصال التي يتزايد إستخدامها بإستمرار من طرف الإنسان من أجل التطور و التغيير، إلا أنها تسببت في ظهور هذا النوع من الجرائم التي لم تعطى تعريفا موحدا ، و المتميزة بخصوصية معينة في كل عناصرها جعلت من الصعب تطبيق أحكام الجريمة التقليدية عليها خاصة من حيث الكشف عنها و الوقاية منها و مكافحتها.

و نظرا لتأثير هذه الجريمة المستحدثة على حرمة حياة الأفراد و أموالهم و كذا على نشاط و أنظمة كل الدول بما فيها الجزائر ، فقد تصدت لها بعقد إتفاقيات تم على أساسها سن مجموعة من القوانين المجرمة للأفعال الخاصة بها ، و كذا إقرار أجهزة خاصة لمتابعتها و مكافحتها بكل الطرق و الوسائل المتناسبة مع نوعيتها الحديثة.

كلمات مفتاحية: الجريمة المعلوماتية، النظام المعلوماتي ، المعالجة الآلية للمعلومات ، الإنترنت ، معاهدة بودابست .

Abstract:

Information crime is committed within the scope of technology, information and communication technologies that are constantly being used by humans for development and change. The provisions of the traditional crime, especially in terms of detection, prevention and control.

In view of the impact of this newly created crime on the sanctity of individuals' lives and money, as well as on the activities and systems of all countries, including Algeria, it has dealt with it by concluding agreements on the basis of which a set of laws were enacted criminalizing its own acts, as well as the adoption of special bodies to follow up and combat it with all Methods and means commensurate with its modern quality.

Keywords: : information crime, information system, automated processing of information, the Internet, Budapest Treaty.

1- مقدمة:

إن لإنتشار ثورة المعلومات و تطور تكنولوجيات الإعلام و الإتصال التي يعرفها العالم حاليا شقين ، الأول إيجابي يتمثل فيما تعرفه الدول من تطور و إزدهار في كل المجالات سواء الثقافية أو السياسية أو الإجتماعية أو الإقتصادية ، التي طغى عليها ما يسمى بالرقمنة أو التعامل الإلكتروني الذي ساهم في نجاح و سرعة إنجاز مشاريع و نشاطات الدول.

أما الشق الثاني سلبي يتمثل في تعرض الدول بسبب إنتشار و توسع الإنترنت إلى ما يسمى بالجريمة المعلوماتية أو الإلكترونية العابرة للحدود الدولية ، و التي طالت مصالح و أموال الأشخاص و المؤسسات التجارية و البنكية و التأمينية و الصحية، و كذا نشاطات و مشاريع الدول في كل المجالات بما فيها العسكرية و الإقتصادية التي أثرت على توجهات و سياسات الدول فيما بينها و حتى على نمو وتطو إقتصادها ، الأمر الذي جعلها تسعى جاهدة لمكافحة هذه الجريمة الإلكترونية المستحدثة و المتميزة بخصائص تختلف تماما عن خصائص الجريمة التقليدية ، الأمر الذي جعل جهود الدول تتكاثف من أجل التصدي لها سواء بشكل جماعي عن طريق الإتفاقيات و المعاهدات التي تساعد التعاون الدولي فيما بينها ، أو بشكل فردي عن طريق سن تشريعات خاصة لمواجهتها و محاربتها .

لذا نتساءل عن ما يميز هذه الجريمة المستحدثة و طرق و سبل تصدي الدول لها و محاربتها؟

و سنقوم بالإجابة على الإشكالية المطروحة بإتباع المنهج الوصفي التحليلي لكل من :

المحور الأول : مظاهر خصوصية الجريمة المعلوماتية

المحور الثاني : تصدي الدول للجريمة المعلوماتية

2-المحور الأول : مظاهر خصوصية الجريمة المعلوماتية

يتعرض المجتمع الحالي إلى حدوث نوعين من الجرائم الأولى تقليدية تقسم إلى جناية و جنحة و مخالفة ، و ثانية معلوماتية أو إلكترونية تقسم إلى أنواع حسب المعيار المستعمل في تحديدها.

بحيث نلاحظ أن للجريمة المعلوماتية عند مقارنتها بالجريمة التقليدية خصوصية معينة و متميزة تتجلى بداية من خلال تعريفها و طبيعتها و الخصائص المميزة لها ، و كذا صفات كل من مرتكبها و الضحية المجني عليها في المجال الإلكتروني، إضافة لأركانها و محلها و التي سنتعرف عليها تباعا على النحو التالي:

2-1: تعريف الجريمة المعلوماتية و الطبيعة القانونية لها

قبل التعرض لتعريف الجريمة المعلوماتية نقوم بتقسيم هذا المصطلح إلى جزئين : الأول الجريمة و الثاني المعلوماتية و تعريفهما:

الجريمة : يعرفها البعض بأنها: " فعل أو امتناع يحظره القانون و يقرر عقوبة لمرتكبه."[1]

كما عرفت بأنها:" فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيرا احترازيا.[2]

المعلوماتية: يقصد بها المعالجة الآلية للمعلومات ، و هي ترجمة للمصطلح الفرنسي Informatique

و تعني تكنولوجيا تجميع و معالجة و إرسال المعلومات بواسطة الكمبيوتر.[3]

و حول تعريف الجريمة المعلوماتية فإنه بسبب كون هذه الجريمة حديثة و مختلفة عن الجريمة التقليدية فهي تتمتع بخصوصية من حيث تعريفها، و هذا ما جعل الفقه الجنائي لم يتمكن من الوصول إلى تسمية موحدة للجريمة المرتبطة بإستعمال كل من الإنترنت و الإعلام الآلي ، لذا أطلقت عليها أسماء متعددة منها جرائم الكمبيوتر، جرائم التقنية العالية ، الجريمة المستحدثة ، جرائم إساءة إستخدام الكمبيوتر، جرائم الإحتيال بواسطة الكمبيوتر ، جرائم الهاكرز أو الإختراقات،الجرائم الإلكترونية ، الجرائم المعلوماتية ....و هي

مصطلحات إنعكست على تعريف هذه الجريمة التي من الأدق تسميتها بالجريمة المعلوماتية لما يشمله هذا المصطلح من إشارة للكمبيوتر أو ما يسمى بالحاسب و كل التقنيات المستعملة في التعامل مع المعلومات.

إنطلاقا من تنوع الأسماء السالفة للذكر للجريمة المعلوماتية لم يتفق الفقه على تقديم تعريف جامع و مانع لها ، بسبب تعلقها بتكنولوجيا الإعلام و الإتصال التي تتطور بإستمرار، و التي تنوع وسائل إرتكابها و أشكالها و صورها .

لذا إختلف الفقه في إختيار الزاوية أو المعيار المعتمد في تعريف هذه الجريمة سواء كان معيار المعرفة التقنية بالمعلوماتية أو معيار أداة أو وسيلة ارتكاب الجريمة أو معيار موضوعها أو محلها، منقسما بذلك إلى فريق ضيق من تعريفها وفريق آخر وسعه.

2-1- 1:التعريف الفقهي الضيق للجريمة المعلوماتية:

لقد ربط أنصار هذا الإتجاه الفقهي هذه الجريمة بضرورة توفر أكبر قدر من المعرفة عند فاعلها ، مثل تعريف الفقيه دفيد تمسون لها على كونها:" جرائم يكون متطلبا لإقترافها أن يتوفر لدى الفاعل معرفة بتقنية الحاسب."[4]

كما عرفها جانب فقهي آخر بأنها: " كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لإرتكابه من ناحية و ملاحقته من ناحية أخرى."[5]

كما عرفت بأنها :" نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقه.[6]

2-1-2 : التعريف الفقهي الموسع للجريمة المعلوماتية:

لقد ربط أنصار هذا الإتجاه الفقهي هذه الجريمة بضرورة توفر أداة أو وسيلة الحاسب الآلي ، مثل تعريفها بأنها: " كل سلوك غير مشروع أو غير أخلاقي ، أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها."[7]

أما فريق آخر فقد وسع من تعريف هذه الجريمة لتشمل أي فعل متعمد مرتبط بأي طريقة كانت ، يتسبب في إمكانية حصول الفاعل على مكسب أو تحمل المجني عليه الخسارة ، و هذا ما أكده تعريف الخبير الأمريكي باركور للجريمة المعلوماتية على أنها : " كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ترتبت عنه خسارة تلحق المجني عليه أو مكسب يحققه الجاني ."[8]

و مما سبق يمكن القول بأن الفقه قد توصل إلى تعريف الجريمة المعلوماتية بأنها : " كل فعل أو امتناع من شأنه الاعتداء على الأموال المعنوية (معطيات الحاسب) يكون ناتجا بطريقة مباشرة و غير مباشرة لتدخل التقنية المعلوماتية."

و هو تعريف شامل قائم على عدة معايير، الأول تمثل في إيراد التعريف للسلوك (كل فعل أو امتناع)، و الثاني تناول محل أو موضوع الاعتداء(الأموال المعنوية) ، أما الثالث هو اتصال السلوك بمحل الاعتداء عن طريق تدخل التقنية المعلوماتية.[9]

إضافة لتعريف شامل أخر أكد بأنها : كل فعل أو إمتناع يتم إعداده أو التخطيط له ، بحيث يتم بموجبه إستخدام أي نوع من الحواسيب الآلية سواء كانت حاسب شخصي أو شبكات الحاسب الآلي أو الإنترنت أو وسائل التواصل الإجتماعي، لتسهيل إرتكاب جريمة أو عمل مخالف للقانون ، أو تلك الأفعال التي تقع على الشبكات نفسها عن طريق إختراقها بقصد تخزينها أو تعطيلها أو تحريف أو محو البيانات أو البرامج التي تحويها.[10]

من هذه التعريفات السابقة يمكننا القول بأن الجريمة المعلوماتية جريمة جديدة تختلف عن الجريمة التقليدية كونها تتميز بخصائص مختلفة متعلقة بكل من إستعمال الحاسوب فيها سواء كان هو أداة الجريمة أو محلها عن طريق إتصاله بشبكة الإنترنت ، و كذلك تعلق محلها بمجموعة من المعطيات و البيانات الإلكترونية سواء الخاصة بالأشخاص أو المؤسسات و المتعرضة للتغيير الغير مشروع و الضار بالغير.

2-1-3 : التعريف التشريعي للجريمة المعلوماتية:

مادامت الجريمة المعلوماتية من الجرائم المستحدثة في الوقت الراهن ، فقد إهتمت الدول بإيجاد نظام قانوني يتلاءم مع خصوصيتها و يساهم في القضاء عليها ، حاولت من خلاله إعطاء تعريف لها كجريمة مختلفة عن الجريمة التقليدية تتطلب وجود جهاز الكمبيوتر و تطال النظام المعلوماتي ، مثل تعريف المشرع الكويتي لها من خلال القانون رقم 63 لسنة 2015 الذي نص من خلال مادته الأولى على أنها : "كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون."

أما القانون السعودي لمكافحة الجريمة المعلوماتية فقد عرفها بأنها : " أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام."

أما المشرع الجزائري فلم يقم بتعريفها إنطلاقا من قانون العقوبات المعدل رقم 15/04 المؤرخ في 2004/11/10 ، الذي إكتفى من خلاله بتناول العقاب الخاص ببعض الأفعال ذات الطابع المعلوماتي من خلال فصله المعنون ب "الجرائم الماسة بنظام المعالجة الآلية للمعطيات."

و تداركا منه لهذا القصور في معالجته الدقيقة لهذا الموضوع ، بحيث أطلق على الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال إنطلاقا من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها ، و الذي عرفها على أنها: " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية."[11]

و مما يلاحظ على هذا النص القانوني أن المشرع الجزائري تبنى معيار دور النظام المعلوماتي لتحديد معالم الجريمة مسميا الجرائم الموجهة ضد النظام المعلوماتي بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

كما يلاحظ على المشرع الجزائري بأنه لم يحدد صورة السلوك المجرم الذي يرتكب أو يسهل ارتكابه ضد منظومة معلوماتية.[12]

2-1-4 :طبيعة الجرائم المعلوماتية :

بسبب كون هذه الجرائم جديدة و مختلفة عن الجرائم التقليدية ، فقد إختلف الفقه حول تحديد طبيعتها على النحو التالي:

أ-الطبيعة الخاصة للجرائم المعلوماتية : تتميز هذه الجرائم بكونها مستحدثة ظهرت نتيجة التطور الهائل في المجال التكنولوجي،الذي جعلها من الجرائم الصعبة بسب طبيعتها الخاصة التي تجعلها تطال المعلومات التي إختلف الفقه في تحديد مفهومها و طبيعتها ، و التي كانت السبب في تسميتها بالجرائم المعلوماتية التي يقول بعض الفقه أثناء محاولته لتحديد طبيعتها الخاصة ، " يجب أن نعترف أننا بصدد ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي ، ففي معظم حالات إرتكاب الجريمة ندخل في مجال المعالجة الإلكترونية للبيانات."[13]

و قد إنقسم الفقه حول الوضع القانوني للمعلومات إلى إتجاهين ، الأول تبناه الفقه التقليدي الذي أكد بأن المعلومات لها طبيعة من نوع خاص و تتمتع بحماية قانونية ، أما الثاني تبناه الفقه الحديث الذي بين أن المعلومات عبارة عن مجموعة من القيم المستحدثة تقتضي حماية قانونية.

ب-الجرائم المعلوماتية جرائم أموال: هذه الجرائم تتم بصورتين ، الأولى يستخدم فيها الحاسب الآلي ، مثل تزييف العملة أو التزوير في محررات رسمية أو الإختلاس و كذا الدخول غير المشروع للبيانات و المعلومات المخزنة على الحاسب ، و الثانية الجرائم الواقعة على الحاسب الآلي بمشتملاته المادية و المعنوية مثل تعديل و إزالة و تقليد بيانات الحاسب و كذا تخريب و إتلاف مكوناته المادية ، و في الحالتين هي جرائم أموال لأن موضعها دائما مال .[14]

ج-الجرائم المعلوماتية جرائم أشخاص: يستخدم الحاسب الآلي في إرتكاب جرائم يكون محلها الأشخاص ، مثل جرائم الذم و القدح و التحقير، و جرائم إفشاء الأسرار سواء التجارية أو الشخصية ، و جرائم التهديد و الإبتزاز و الإعتداء على الحياة الخاصة عبر الإنترنت.[15]

د-الجرائم المعلوماتية جرائم أمن دولة و جرائم مخلة بالثقة العامة و الآداب العامة:يمكن إستعمال الوسائل الإلكترونية للمساس بأمن الدولة الذي ينقسم إلى قسمين ، الخارجي الذي يمس بجرائم التجسس و الإتصال مع العدو ، و الداخلي الذي يمس بجرائم إثارة الفتن و المساس بالوحدة الوطنية ، إضافة لإستعمال الوسائل الإلكترونية في جرائم المساس بالثقة العامة و الآداب العامة مثل نشر برامج إباحية أو إقتنائها من أجل توزيعها و نشرها.[16]

هـ-الجرائم المعلوماتية جرائم إقتصادية : لكونها جرائم تخالف السياسة الإقتصادية القائمة على دعم الثقة و الإئتمان ، و منها التزوير الذي يطال الأوراق المالية و تزييف العملات المتداولة ، الأمر الذي يترتب عليه إلحاق الضرر بالمركز الإقتصادي للدولة.

مما سبق يمكننا القول أن للجريمة المعلوماتية طبيعة خاصة ، لأن هذا الإجرام المعلوماتي يتعلق بكل سلوك غير مشروع يطال المعالجة الآلية للبيانات و كذا إدخال المعلومات و نقلها ، مما يجعلنا نضمه إلى نطاق القانون الجنائي المتميز بعجزه عن مواكبة التطور المعلوماتي الحاصل حاليا في كل المجالات ، مما يجعله خاليا من النصوص القانونية المناسبة لهذا النوع من الجرائم.

2-2 : خصائص الجريمة المعلوماتية:

تتميز الجريمة المعلوماتية عند مقارنتها بالجريمة التقليدية بمجموعة من الخصائص تتمثل في :

أ/وقوع الجريمة المعلوماتية في بيئة المعالجة الآلية للبيانات و المعلومات: يتطلب قيام هذه الجريمة التعامل مع بيانات مجهزة و مجمعة للدخول للنظام العلوماتي من أجل معالجتها إلكترونيا ،عن طريق تصحيحها أو تعديلها أو دمجها أو تخزينها أو إسترجاعها أو طباعتها من طرف الفاعل المتقن لإرتكابها خاصة في جرائم التزوير و التقليد.[17]

ب/الجريمة المعلوماتية ذات طابع تقني: هي صفة تجعل من السهل إخفاء معالم الجريمة المعلوماتية و من الصعوبة تتبع مرتكبها ، بحيث يصعب على المحقق التقليدي التعامل معها و متابعتها و الكشف عنها وإقامة الدليل عليها ، فهي جرائم تتسم بالغموض و التحقيق فيها يختلف عن التحقيق في الجرائم التقليدية.[18]

ج/أهداف و دوافع إرتكاب الجرائم المعلوماتية: لكل أنواع الجرائم دوافع إلا أنها تختلف في الجريمة المعلوماتية التي تنقسم لدوافع شخصية تتمثل في السعي للربح الفاحش أو رغبة تحقيق التفوق على الأنظمة المعلوماتية التي لا يتقنها إلا البعض ، إضافة لدوافع خارجية قد تكون إنتقامية من صاحب العمل أو لأهداف أخطر منها و المتمثلة في عمليات السطو على أموال المؤسسات الكبرى في أي دولة و كذا الجوسسة على أنظمتها و نشاطها و حتى أمنها لحساب جهات معينة.[19]

د/ الجريمة المعلوماتية جريمة دولية: تتميز هذه الجريمة بكونها جريمة عابرة للحدود ، بحيث يتعدى إرتكابها الحدود الإقليمية للدول عن طريقها تنفيذها في دولة و ظهور أضرارها في دولة أخرى، مما يثير إشكال حول الإختصاص القضائي و القانون الواجب التطبيق في محاكمة الجاني ، أي ما هي الدولة المختصة بمحاكمة مقترفها ، فهل هي التي أرتكب على إقليمها السلوك الإجرامي أم الدولة التي يتواجد فيها المجني عليه أو دولة الجاني.[20]

ح/خاصية صعوبة الإكتشاف و الإثبات: تتميز الجريمة المعلوماتية بكونها جريمة لا تترك آثار ملموسة ، مثل الشهود الذين يمكن الاستدلال بأقوالهم و لا أدلة مادية يمكن فحصها لكونها تقع في بيئة إفتراضية يتم فيها تناول المعلومات و نقلها بواسطة نبضات إلكترونية غير مرئية.[21]

خ/الجريمة المعلوماتية سريعة التنفيذ: لا يتطلب تنفيذ الجريمة المعلوماتية وقت ، بحيث تنفذ بمجرد الضغط على لوحة المفاتيح لنقل المبالغ الضخمة من مكان إلى آخر ، أو الإطلاع على أكبر قدر من المعلومات المعالجة و المخزنة في جهاز الحاسب الآلي، فأغلب صورها و أشكالها ينفذ دون إستخدام أي وسائل أو معدات أو برامج معينة ، حتى أن الأمر لا يتطلب تواجد مرتكبها في مكان تنفيذها الذي يتم من خلال الدخول لشبكة الإنترنت أو القيام بأعمال سرقة أموال أو معلومات أو تغييرها.

د/خاصية الجاذبية: بسبب ما يمثله كل من الكمبيوتر و الإنترنت من ثروة للمجرمين و الإجرام المنظم ، فقد أصبحت أكثر جاذبية لإنتشار الأموال و غسلها و توظيفها في تطوير تقنيات و أساليب ، تمكن من الدخول إلى الشبكات و سرقة المعلومات وبيعها أو سرقة البنوك أو إعتراض العمليات المالية و تحويل مسارها و إستعمال أرقام البطاقات.[22]

ذ/الجرائم المعلوماتية جرائم ناعمة : يتميز هذا النوع من الجرائم بعدم بذل أي مجهود عضلي أو جسدي من طرف فاعلها ، بعكس الكثير من الجرائم الأخرى مثل القتل و السرقة.. التي تحتاج لهذا النوع من المجهود لإتمامها.

فهي جرائم ناعمة تمكن من نقل البيانات و المعلومات من حاسب لآخر ، و التي تسهل السطو على أرصدة المؤسسات أو الشركات.[23]

ه/الطابع الخفي للجريمة المعلوماتية: تتميز الجريمة المعلوماتية الناتجة عن إستخدام الإنترنت بكونها جريمة خفية بالنسبة للمجني عليه ، بسبب إستعمال الجاني لأساليب متقدمة في التلاعب بالنبضات و الذبذبات الإلكترونية، التي يتمكن الجناة من إخفائها بواسطة أساليب معقدة لم تتمكن التشريعات المختلفة من التصدي لها.[24]

و/ أعراض النخبة : ميزة يتصف بها المختصين في تقنية الحاسب الآلي و الأنظمة المعلوماتية ،إنطلاقا من إعتقادهم أنه يمكنهم ممارسة كل الهوايات التابعة لهذه التقنية الإلكترونية ، و التي تجعلهم يبالغون في إستعمال الحاسب الآلي و الأنظمة المعلوماتية بشكل غير قانوني يؤدي إلى إرتكابهم جرائم خطيرة .[25]

نستنتج من تناولنا لخصائص هذا النوع من الجرائم أنها كثيرة الإختلاف عن الجرائم التقليدية ، التي تحكمها النصوص القانونية التقليدية التي وضعت وفقا لمعايير معينة ، لا تنطبق على مجال المعلومات ، التي من أهم مميزاتها أنه يصعب فيها الإثبات و كذا ملاحقة الجناة الذين ينتمون لدول لا تربطهم أي إتفاقية بالدولة التي تحقق فيها السلوك الإجرامي المعلوماتي أو جزء منه .

2-3 : أطراف الجريمة المعلوماتية:

للجريمة المعلوماتية أطراف مثل الجريمة التقليدية و المتمثلة في كل من الجاني المسمى بالمجرم المعلوماتي المعروف بالخصوصية في هذه الجريمة و كذا المجني علية أو الضحية.

2-3-1 :المجرم العلوماتي : الجرائم المعلوماتية بإعتبارها من الجرائم المستحدثة فإنها لا تحتاج إلا إلى القدرة الذهنية للجاني المتميز بالإلمام بتقنيات الحاسوب و تكنولوجيا المعلومات ، و التي تمكنه من القيام بجريمته بشكل سريع و دون ترك أي أثر.[26]

و يعد المجرم المعلوماتي الذي لا يمكن إلا أن يكون شخصا طبيعيا و ليس معنويا من المجرمين الذين يمتازون بالمهارة في تكنولوجيا المعلومات و الحاسوب، حيث تمكنه قدراته الذهنية و العقلية و الفنية من التعامل مع أجهزة الحاسوب التي يمكنه فتح ملفات البيانات و المعلومات فيها و التأثير عليها وإختراقها أثناء إرتكابه الجرائم المعلوماتية بسهولة و في وقت وجيز جدا ، بعكس المجرمين في الجرائم الأخرى حيث يمتاز بعضهم بقلة الإختصاص و المعرفة في جرائمهم.[27]

وللمجرم المعلوماتي عدة أصناف تتمثل في فئة صغار مجرمي المعلوماتية الذين يرتكبون هذه الجرائم بهدف التسلية و المزاح دون أي نية للإضرار بالغير، و فئة القراصنة الهواة أو المخترقون الذين يدخلون أنظمة الحاسبات الآلية بشكل غير مشروع لإكتساب الخبرة و المهارة دون أي هدف للتخريب و إلحاق الضرر، و فئة القراصنة المحترفين المشكلة لأخطر فئة من المجرمين تهدف لتحقيق الكسب المالي الذي جعلها تتسبب في أضرار كبيرة مقارنة بباقي الفئات.[28]

2-3-2 :المجني عليه في الجريمة المعلوماتية: يقع هذا النوع من الجرائم على كل من الشخص الطبيعي و الشخص المعنوي، الذي يشكل المجني عليه في الغالب المتمثل في الأشخاص الإعتبارية التي تستعمل الحواسيب في القيام بنشاطاتها، مثل البنوك و الشركات الكبرى و المؤسسات الحكومية و الوزارات و الهيئات المالية..[29]

و بالمقابل قد يتعرض الشخص الطبيعي للجرائم الإلكترونية الماسة بأسراره الشخصية و التجارية من أجل الحصول على الأموال أو المعلومات التي تعتبر بدورها هدف وقوع هذه الجريمة على الأشخاص المعنوية السالفة الذكر.[30]

و الملاحظ على المجني عليه في هذا النوع من الجرائم أنه يكون له دور ضئيل و سلبي إلى حد كبير ، بسبب أنه يفضل الإبقاء عل ما لحقه من إعتداء سرا ، بواسطة تكتمه على ما لحقه من أضرار ناتجة عن الجريمة الإلكترونية رغبة منه في الحفاظ على مركزه الإجتماعي أو سمعته التجارية المرتبة عنها ثقة العملاء به ، التي لا يرغب في فقدها حفاظا على قوة مؤسسته.

2-4 :أركان الجريمة المعلوماتية و محلها:

للجريمة المعلوماتية مثل أي جريمة أخرى أركان لا تقوم إلا بوجودها و محل أو موضوع معين تقع عليه.

2-4-1: أركان للجريمة المعلوماتية: لها ثلاثة تتمثل في كل من ، الركن الشرعي المتمثل في الصفة غير المشروعة للفعل ، بحيث تتمثل قاعدة التجريم و العقاب للجرائم الإلكترونية فيما ورد النص عليه في القانون الخاص بجرائم أنظمة المعلومات ، وكذا الركن المادي المتمثل في شكل الجريمة الذي تبرز به إلى العالم الخارجي ، إضافة للركن العنوي المتمثل في الإرادة التي يقترن بها الفعل سواء في صورة القصد أو الخطأ.[31]

و الملاحظ أن غالبية أنظمة المعالجة الآلية للمعطيات تتمتع بنظام حماية فنية ، يساعد على إثبات أركان الجريمة خاصة ركنها المعنوي.[32]

2-4-2 : محل الجريمة المعلوماتية : يتمثل في أحد أو كل العناصر التي تستهدفها هذه الجريمة و المتمثلة في:

أ- المعلومات : قد تشمل الجرائم المعلوماتية سرقة أو تغيير أو حذف المعلومات، عن طريق إختراق بريد إلكتروني و العبث بمحتوياته أو سرقة معلومات موقع ما أو إنتهاك حقوق الملكية الفكرية.

ب-الأجهزة : تطال أيضا الجرائم المعلوماتية أجهزة الكمبيوتر عن طريق تعطيلها أو تخريبها بواسطة إرسال الفيروسات و برامج الأنظمة الهجومية التي تتلف أنظمتها، مما يؤدي إلى شلل كل الأنشطة المرتبطة بجهاز الكمبيوتر المركزي المرتبطة به أنشطة أخرى.

ج-الأشخاص أو الجهات: تستهدف العديد من الجرائم المعلوماتية أشخاص أو جهات معينة بواسطة التهديد أو الإبتزاز أو سرقة المال بإستخدام بطاقات مصرفية و إئتمانية للغير، أو توجيه تعليمات إرهابية ضدهم.[33]

3-المحور الثاني : تصدي الدول للجريمة المعلوماتية

إن ما عرفته الدول من تقدم تكنولوجي و إنتشار واسع لوسائل الإتصال الحديثة ، ساهم في تقدمها و إزدهارها في كل مجالات الحياة ، إلا أنه أدى في نفس الوقت إلى بروز أشكال جديدة من الجرائم ، دفع الدول إلى التصدي إليها عن طريق عقدتها لمعاهدات تنظم محاربتها و ردعها تشريعيا عن طريق سن نصوص قانونية و إحداث أجهزة خاصة للحد من إنتشارها.

3-1 : التصدي للجريمة المعلوماتية إنطلاقا من الإتفاقيات الدولية :

مادامت الجريمة المعلوماتية جريمة عالمية ، فقد عرفت تعاونا دوليا لمحاربتها من خلال جملة من المعاهدات و الإتفاقيات الدولية المتتابعة ، و التي من أهمها إتفاقية بودابست في سنة 2001 و كذا الإتفاقية العربية لمكافحتها في سنة 2010 المتضمنتين مجموعة من الأحكام نتعرف عليها من خلال تناول كل من :

3-1-1 :التصدي للجريمة المعلوماتية إنطلاقا من معاهدة بودابست لمكافحة جرائم الإنترنت لسنة 2001 :

تمثل هذه الإتفاقية حصيلة المجهودات العالمية في الوصول إلى قانون عالمي لمكافحة الجريمة الإلكترونية ، بحيث تلزم الدول الأعضاء فيها و المتمثلة في الدول الأوروبية و كذا غير الأوروبية الموقعة عليها أو المنظمة إليها، بإتخاذ الإجراءات و التدابير التشريعية الملائمة لتجريم تسع جرائم تتعلق بالتقنية الإقتصادية و الملكية الفكرية و المحتوى الضار أو غير القانوني والمتمثلة في:

1-الدخول غير القانوني المتعمد أو ما يسمى بالدخول غير المصرح به المتمثل في الدخول المتعمد إلى نظام كمبيوتر أو جزء منه دون حق أو إذن ، سواء أكان بنية إنتهاك وسائل الأمن أو بنية الحصول على معطيات الكمبيوتر أو لأي نية غير مشروعة.[34]

2-الإعتراض غير القانوني و دون حق ، بواسطة وسائل تكنولوجية للبيانات المرسلة غير العامة إلى أو من نظام كمبيوتر ، و كذلك إعتراض الإشعاعات الكهرومغناطيسية المنبعثة من نظام كمبيوتر تحمل مثل هذه المعطيات.

3-التدخل المتعمد في المعطيات بتدميرها أو حذفها أو تشويهها و إفسادها أو تبديلها أو تغييرها أو تعديلها أو كبتها أو إخمادها.[35]

4-التدخل المتعمد في الأنظمة بإرتكاب مجموعة الأفعال المتعلقة بالتدخل في المعطيات لتحميل أداء و عمل الأنظمة بالتدمير و الحذف و التعديل و التعطيل ، إضافة لوسيلة البث أو الإرسال .[36]

5-إساءة إستخدام الأجهزة و التي تتم إنطلاقا من القيام ببيع أو شراء أو إستخدام أو إستيراد أي وسائل ، بما فيها برامج الكمبيوتر بهدف إرتكاب أي فعل جرمي ضار بنظام المعلوماتية.[37]

6-التزوير المتعمد بإستخدام الكمبيوتر و ذلك بإدخال أو تعديل أو حذف أو إخفاء بيانات الكمبيوتر على نحو يظهر بيانات غير أصلية لتكون مقبولة قانونا و كأنها بيانات أصلية.[38]

7-الإحتيال المتعمد بإستخدام الكمبيوتر بدون حق ، و على نحو يسبب خسارة الغير لممتلكاته عن طريق إدخال أو حذف أو تعديل أو كتم بيانات الكمبيوتر ، أو من خلال التدخل بعمليات نظام الكمبيوتر أو برامجه بغية الحصول على منفعة إقتصادية لنفسه أو لغيره.[39]

8-الجرائم المرتبطة بدعارة الأطفال و التي محاربتها تؤدي إلى حمايتهم على أساس تحديد السن الأفضل لحماية الأطفال والمحدد أدناه من طرف كل دولة بما يناسبها.[40]

9-الجرائم المرتبطة بحق المؤلف أو الحقوق المجاورة ، و التي أوجبت المعاهدة بصددها على الدول الأعضاء إتخاذ تدابير تشريعية تجرم الإعتداء عليها و المرتكبة عمدا بغرض تجاري و بإستخدام نظام الكمبيوتر، وفقا لما تحدده القوانين الوطنية للدول الأعضاء المتوافقة مع إتفاقية بيرن لحماية المصنفات الأدبية و الفنية ، و إتفاقية تريبس و كذا إتفاقية الويبو لحق المؤلف و الأداء و الفنوغرامات.[41]

كما أنها بالمقابل أكدت على إجراءات جنائية جديدة تتعلق بهذا النوع من الجرائم و المتمثلة في كل من :

الحفظ السريع للمعطيات المخزنة ، تجميع المعلومات الخاصة بالمشتركين ، التفتيش المعلوماتي ، إجراء التنصت ، التعاون الدولي ، تحديد المصطلحات القانونية القريبة من مجال التكنولوجيا و المتناسبة مع هذا النوع الإجرامي الجديد.

و بهذا نستنتج بأن إتفاقية بودابست أعتبرت مرجعا قانونيا هاما في مجال محاربة الإجرام المعلوماتي ، سواء بالنسبة لبعض الإتفافيات الدولية اللاحقة ذات الصلة ، أو بالنسبة للتشريعات الداخلية لبعض الدول ، إنطلاقا من تحقيق أهدافها المتعلقة بسعيها لتحقيق وحدة التدابير التشريعية بين الدول الأوربية و غيرها من الدول المنظمة لها، و تأكيدها على أهمية التعاون الدولي الإقليمي و الدولي في ميدان مكافحة الجرائم الإلكترونية ، و كذا تحقيقها للتوازن بين حماية حقوق الإنسان الأساسية المعلن عنها في المواثيق الدولية السابقة و حقوقه المتعلقة بالمجال الإلكتروني من حرية الوصول للمعلومات و الأفكار و حيازتها و حرية البحث العلمي.

3-1-2 :التصدي للجريمة المعلوماتية إنطلاقا من الإتفاقية العربية لمكافحة الجريمة الإلكترونية لسنة 2010:

هي إتفاقية إنبثقت بتاريخ 2010/12/21 عن معاهدة بودابست التي أخذت منها أحكامها ، خاصة فيما يخص القواعد الإجرائية سواء من حيث نطاق تطبيقها أو قواعدها و التي أوجبت على الدول الأطراف فيها ملاءمتها مع قوانينها الوطنية، خاصة الأبحاث الجنائية لتدابير التحفظ على بيانات الكمبيوتر المخزنة و كشفها و إصدار الأوامر بتسليمها ، و إجراءات التفتيش على المعلومات المخزنة و حجزها و التجميع الفوري لها و إعتراض محتواها.

إضافة لإلزامها لكل طرف فيها بتبني الإجراءات الضرورية لمد إختصاصها على أي نوع من الجرائم المنصوص عليها في هذه الإتفاقية في حال إرتكاب الجريمة بشكل كلي أو جزئي.[42]

3-2: تصدي المنظومة التشريعية الغربية للجريمة المعلوماتية:

لقد إهتمت العديد من الدول الأوروبية بالجرائم الإلكترونية من خلال تخصيص تشريعات لها مثل:

-السويد: إصدار لأول تشريع خاص بها و المسمى بقانون البيانات السويدي لسنة 1973 .

-الولايات المتحدة الأمريكية: القانون الخاص بحماية أنظمة الحاسوب لفترة ما بين 1986 و 1985 ثم قانونها لسنة 1986 ، ثم التصنيف الجديد الذي قامت به وزارة العدل سنة 2000 لجرائم الكمبيوتر المتضمنة السطو على بيانات الكمبيوترو إستخدامه في جرائم القرصنة و سرقة الأسرار التجارية، و تزوير الماركات التجارية و العملة و الإتجار بالأسلحة النارية و المخدرات و غسل الأموال عبر شبكة الإنترنت.[43]

-بريطانيا: القانون الخاص بمكافحة التزوير و التزييف لسنة 1981 المتضمن للطرق و الوسائل الإلكترونية و كذا قانونها الخاص بإساءة إستخدام الحاسوب لسنة 1990 ،الذي قسم الجرائم الإلكترونية إلى ثلاث حالات ، الأولى تتعلق بالدخول غير المصرح به لنظام الحاسوب ، و الثانية تخص الدخول غير المصرح به بنية إرتكاب أو تسهيل إرتكاب جرائم أخرى، أما الثالثة تتعلق بالقيام بالتعديل أو التحويل غير المصرح به لنظام الحاسوب بقصد إضعافه أو تعطيله.[44]

-كندا: قانونها الجنائي الذي تضمن تعديله لسنة 1985 قواعد خاصة بجرائم الحاسب الآلي و الإنترنت ،و كذا عقوباتها وعقوبات جرائم التدمير أو الدخول غير المشروع لأنظمة الحاسب الآلي.

-فرنسا:قانونها الخاص بالجريمة الإلكترونية رقم 19-88 لسنة 1988 المعدل سنة 1993 و المتضمن في قانون العقوبات الفرنسي في مادته رقم 462 التي جرمت كل ولوج إلى نظام المعالجة الآلية أو البقاء فيه بطريق غير مشروع و ما يترتب عليه من آثار، و كذا عقوبات أصلية و تكميلية لكل من الشخصين الطبيعي و المعنوي ، إضافة للقانون رقم 575-2004 الخاص بالثقة في الإقتصاد الرقمي الذي شدد في عقوبات الجرائم الإلكترونية حماية للتعاملات الإقتصادية.

-ألمانيا: قانونها المؤرخ في 1986/05/15 الخاص بعدد من الجرائم الإلكترونية .

-الدانمارك : قانونها لسنة 1985 المتعلق بجرائم الحاسوب المشدد على محاولة الإطلاع على الأسرارا التجارية .

-النرويج: قانونها لسنة 1985 المجرم لمختلف العمليات المتسببة في الإضرار بأنظمة الحاسب الآلي و المتمثلة في الوصول غير المصرح به للبيانات المخزنة و التسبب في إتلافها و تعطيلها.[45]

3-3 : تصدي المنظومة التشريعية العربية للجريمة المعلوماتية :

لقد أدى إنتشار إستعمال الإنترنت في كل أنحاء العالم بما فيها الدول العربية إلى ظهور الجريمة المعلوماتية على مستواها ، الأمر الذي جعلها تسن مجموعة من التشريعات المتعلقة بمكافحتها و المتمثلة في كل من :

-**الإمارات العربية المتحدة :** قانون الإتحاد رقم 2 لسنة 2006 الخاص بمكافحة جرائم المعلومات ، التي من بينها جريمة إختراق المواقع و الأنظمة الإلكترونية ، التنصت أو إعتراض المراسلات عبر شبكة الإنترنت ، إستخدام الإنترنت في الإبتزاز و التهديد، سرقة بيانات البطاقات الإلكترونية....[46]

-**مصر**:قانون التوقيع الإلكتروني رقم 15 لسنة 2004 الذي جرم الأفعال الخاصة بالحصول على توقيع أو وسيط أو محور إلكتروني بدون وجه حق ،أو إعتراضه أو تعطيله عن أداء وظيفته .[47]

-**تونس**: قانون التجارة الإلكترونية رقم 83 لسنة 2000 المؤرخ في 2000/08/09 الخاص بالمبادلات الإلكترونية ، و الذي يعتبر أول تشريع يتعرض للجرائم المعلوماتية المتعلقة بكل من التوقيع و البيع الإلكتروني و كذا المصادقة الإلكترونية.[48]

-**سلطنة عمان :** قانون خاص بجرائم الحاسب الآلي عاقبت من خلاله كل الأفعال المؤدية إلى الإلتقاط غير المشروع للمعلومات ، و كذا التأثير عليها بواسطة الإتلاف و المحو و التغيير و التسريب.

إضافة لدول عربية أخرى التي إتجه تشريعها لتجريم الأفعال الماسة بالنظام الإلكتروني بشكل غير قانوني ، مثل **الأردن** من خلال مشروع قانون جرائم الإنترنت الإلكترونية الذي جرم إستخدام شبكة الإنترنت أو موقع إلكتروني لخرق الحياة الخاصة للآخرين ، بما فيها إستعمال خطاب الكراهية و إستغلال الأطفال.

3-4 : تصدي المنظومة التشريعية الجزائرية للجريمة المعلوماتية:

حاول المشرع الجزائري مثل مشرعي القوانين المقارنة التصدي للجريمة الإلكترونية عن طريق إصدار مجموعة من القوانين المحددة لأنواع هذه الجرائم و عقوباتها و كذا تحديد الهياكل و الأجهزة المكلفة بالتصدي لها على النحو التالي:

3-4-1 : القوانين العامة الموضوعية المنظمة للجريمة المعلوماتية:

-القانون رقم 04-15 المعدل و المتمم لقانون العقوبات رقم 66-156المتعلق بالقسم السابع من قانون العقوبات الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات.[49]

- القانون رقم 06-22 المعدل و المتمم لقانون الإجراءات الجزائية رقم 66-155 ، و الخاص بالإعتراض للمراسلات و تسجيل الأصوات و إلتقاط الصور.[50]

-القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها ، من خلال تحديده لكل مايخص المنظومة المعلوماتية و مقدمو الخدمات و معطيات تسيير الإتصالات الإلكترونية من مراقبة و تفتيش و حجز و حفظ للمعطيات المعلوماتية.[51]

فقد تضمن هذا القانون ستة فصول ، الأول منها لأحكام عامة تحدد مفهوم المصطلحات المستعملة فيه و مجال تطبيقه ، من خلال وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية و تجميع و تسجيل محتواه في حينها ، و القيام بإجراءات التفتيش و الحجز داخل منظومة معلومة ، و فصلت باقي الفصول هذه الإجراءات مبينة كيفية تطبيقها لمحاربة الجريمة المعلوماتية و الوقاية منها ، بحيث تقسم إجراءات التحري في هذا المجال حسب ما نص عليه القانون إلى مايلي:

مراقبة الإتصالات الإلكترونية ، تفتيش المنظومة المعلوماتية ، حجز المعطيات المعلوماتية ، حفظ المعطيات المتعلقة بحركة السير.

و رغم ما أتى به هذا القانون فقد تعرض للإنتقاد على أساس عدم وضوح معنى الكثير من مصطلحاته ، و كذا عدم تعرضه لحقوق و واجبات المتعاملين بالأجهزة الإلكترونية خاصة الكمبيوتر و الهواتف الذكية إضافة لشبكة الإنترنت.

3-4-2 : القوانين الخاصة المنظمة للجريمة المعلوماتية:

-الأمر رقم 03-05 المتعلق بحقوق المؤلف و الحقوق المجاورة الذي نص على توفير الحماية لبرامج الحاسب الآلي و إخضاعها لقوانين الملكية الفكرية مقرا عقوبة الحبس و الغرامة لكل من يعتدي على هذه المصنفات.[52]

-القانون رقم 03-200 المحدد للقواعد العامة المتعلقة بالبريد و الإتصالات السلكية و اللاسلكية الذي نص على تسهيل عملية إجراء التحويلات المالية إلكترونيا و إستعمال الحوالات الإلكترونية.[53]

-القانون رقم 08-01 المعدل و المتمم للقانون رقم 83-01 المتعلق بالتأمينات ، المتطرق للجريمة الإلكترونية إنطلاقا من البطاقة الإلكترونية المسلمة من هيئات الضمان الإجتماعي و ما يطرأ عليها من إستعمالات غير مشروعة ترتب آثارا سلبية و غير قانونية عليها تضر بصاحبها.[54]

3-4-3 : أنواع الجرائم المعلوماتية في التشريع الجزائري:

لقد تناولت الجرائم المعلوماتية نظام المعالجة الآلية للمعطيات الذي إرتأينا تحديد تعريفه ثم تحديد الجرائم المتعلقة به.

لقد عرفت الإتفاقية الدولية للإجرام المعلوماتي النظام المعلوماتي بنصها على أنه:" يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو التي ذات صلة بذلك ، و يقوم أحدها أو أكثر من واحد منها تبعا للبرنامج بعمل معالجة آلية البيانات."[55]

كما يعرفه بعض الفقه بكونه مجموع العمليات المنجزة بواسطة وسائل الإعلام الآلي المرتبطة بتجميع ، تسجيل، إعداد ، حفظ و تخزين معلومات إسمية و أيضا كل العمليات من طبيعة واحدة مرتبطة بإستغلال الملفات أو قاعدة المعطيات و خاصة ربط أو تخزين أو فحص أو نشر معلومات اسمية .[56]

و لقد قسم المشرع الجزائري الجريمة المعلوماتية إلى نوعين ، الأولى جرائم مرتكبة بواسطة النظام المعلوماتي المتمثل في وسائل تكنولوجيا الإعلام و الإتصال ، و الثاني الجرائم الواقعة على النظام المعلوماتي المتناولة من قبل قانون العقوبات.

3-4-3-1 :الجرائم المعلوماتية المرتكبة بواسطة النظام المعلوماتي: هي الجرائم المرتكبة بإستعمال الحاسب الآلي و المتمثلة في :

1-الجرائم المعلوماتية الواقعة على الأشخاص: هي الجرائم الماسة بحقوق الشخص الطبيعي و المتمثلة في :

أ-الجرائم المعلوماتية الواقعة على خصوصية الحياة الخاصة:

تعتبر حرمة الحياة الخاصة من الأمور المكرسة حمايتها من خلال الدستور الجزائري الذي نص على سرية المعلومات الشخصية و حظر الإعتداء عليها بأي شكل كان [57] ، إلا أنه يتم الإعتداء عليها بواسطة الحاسب الآلي الذي يسهل الحصول على المعلومات المخزنة التي من المفروض تميزها بالخصوصية و السرية ، عن طريق إختراقها لإستعمالها في إرتكاب أفعال غير مشروعة تتمثل في الإطلاع عليها و كذا عرضها للغير دون علم صاحبها الذي قد يتعرض للتهديد و الإبتزاز مقابل نشرها.

ب-الجرائم المعلوماتية الواقعة على حقوق الملكية الفكرية:

يكرس و يضمن الدستور الجزائري مجموعة من الحقوق الأساسية و الحريات ، التي من بينها حرية الإبداع الفكري ، بمافي ذلك أبعاده العلمية و الفنية المضمونة ، و الحقوق المترتبة عليه المحمية قانونا.[58]

لكل مؤلف أو منتج حقوق ملكية و براءات إختراع يمكن الإعتداء عليها بواسطة النظام المعلوماتي ، الذي يمس بالحق المعنوي و المالي لصاحب المعلومات التي تم إختراقها ثم تخزينها و إستخدامها دون إذن صاحبها ، الذي نص القانون على حماية معلوماته إنطلاقا من الأمر رقم 03-05 المتعلق بحقوق المؤلف و الحقوق المجاورة [59]، و كذا حماية إنجازاته إنطلاقا من الأمر رقم 03-07 الخاص ببراءات الإختراع.[60]

2-**الجرائم المعلوماتية الواقعة على النظم المعلوماتية الأخرى:** هي الجرائم التي تتم بواسطة الحاسب الآلي الذي يمكن الجاني من دخول مركز المعالجة المعلوماتية للقيام بعدة أفعال غير مشروعة ، منها الإستيلاء على المعلومات المخزنة بواسطة ألة الطباعة أو شاشة النظام أو القراءة ، و كذا إساءة إستعمال البطاقة الإئتمانية عن طريق عدم إحترام العميل لشروط العقد الذي يربطه بالبنك ، أو إستعمالها رغم إنتهاء صلاحيتها أو إلغائها ، أو إستعمالها من قبل سارقها للحصول على السلع و الخدمات.[61]

3-**الجرائم الإلكترونية الواقعة على الأسرار:** يتم في هذه الجريمة إستعمال النظام المعلوماتي للحصول على الأسرارسواء كانت عامة متعلقة بالدولة التي يتم التجسس على أسرارها العسكرية و الإقتصادية ، أو خاصة متعلقة بالمؤسسات المهنية التي يتم الحصول على أسرارها من أجل نشرها بهدف الحصول على المال أو الضغط عليها.[62]

3-4-3-2: الجرائم المعلوماتية الواقعة على النظام المعلوماتي:

لقد قام المشرع الجزائري بتعديل قانون العقوبات رقم 66-156 بموجب القانون رقم 04-15 ، الذي تناول القسم السابع المكرر في قانون العقوبات تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" ، و الذي عدل بدوره متناولا الجرائم الإلكترونية المتمثلة في :

1-الدخول أو البقاء عن طريق الغش(غير مشروع) في نظام المعالجة الآلية للمعطيات.[63]

2-تخريب (الإعتداء على سير) نظام المعالجة الآلية للمعطيات.[64]

3-المساس بسلامة المعطيات(الإعتداء العمدي على المعطيات بواسطة كل من الإدخال ، أو الإزالة أو المحو ،أو التعديل) .[65]

4-تجميع و توفير المعطيات المتحصل عليهاعن طريق منظومة معلوماتية للغير، من أجل إرتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[66]

5-إستعمال و التصرف في المعطيات المتحصل عليها من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[67]

6-تجريم المشاركة في مجموعة أو إتفاق مسبق لإرتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[68]

7-تجريم محاولة إرتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[69]

8-تشديد العقوبات في حالة إستهداف الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام.[70]

من خلال إستقراء هذه النصوص القانونية المتعلقة بمجموعة الأفعال المجرمة إنطلاقا من المواد رقم 394 مكرر إلى 394 مكرر 7 من قانون العقوبات ، يتبين لنا أن المشرع الجزائري حاول إستدراك الفراغ القانوني و مسايرة التطور الخاص بمجال الإجرام المعلوماتي ، بإستحداثة نصوص تجريمية للحد من الإعتداءات ضد الأنظمة المعلوماتية بموجب القانون رقم 15/04 ، معتمدا نفس المنهج الفرنسي في الحماية القانونية للمعالجة الآلية للمعطيات الصادر سنة 1988 و المعدل بتاريخ 1994/03/01 ، و الذي منع الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات، و عاقب على كل تخريب لمحتويات النظام ،أو إعاقة تشغيله ، أو تزوير الوثائق المعلوماتية ، و أغفل الإعتداءات الماسة بمتوجات الإعلام الآلي و المتمثلة في نصوص التزوير المعلوماتي.

3-4-4 : العقوبات المقررة للجرائم المعلوماتية:

تنقسم إلى عقوبات أصلية و أخرى تكميلية تطبق على كل من الشخص الطبيعي و كذا المعنوي على النحو التالي:

3-4-4-1 :العقوبات الموقعة على الشخص الطبيعي : تتمثل في كل من :

أ-العقوبات الأصلية : تتمثل في عقوبة الحبس التي تتراوح مدتها من شهرين إلى ثلاث سنوات حسب الفعل المرتكب إلكترونيا ، و الغرامة التي تتراوح قيمتها من50.000 د ج إلى 5.000.000 د ج حسب الفعل المرتكب إلكترونيا و ما يترتب عنه من آثار.[71]

فهي عقوبات تطبق على الشخص الطبيعي سواء في حال إرتكابه الجريمة أو الشروع فيها أو المشاركة فيها بحيث تضاعف و تشدد في حال ترتيبها لآثار ضارة بالنظام المعلوماتي أو إستهدافها للدفاع الوطني أو الهيئات و المؤسسات العامة.[72]

من خلال إستقراء النصوص القانونية المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية ، تبين لنا تدرج داخل النظام العقابي المتوقف على درجة الخطورة الإجرامية للتصرفات ، بحيث نص على جريمة الدخول أو البقاء في صورتها البسيطة و المشددة ، ثم على جريمة الإعتداء العمدي على المعطيات كونها أشد خطورة و تستهدف المعطيات الموجودة داخل النظام بما فيها البيانات و البرامج.

-عقوبة الإشتراك : بإستقراء المادة رقم 394 مكرر 5 نلاحظ أن المشرع الجزائري لم يخرج عن القواعد العامة لعقوبة الشريك ، حيث حدد لها نفس عقوبة الفاعل الأصلي ، لأن جرائم الإعتداء على نظم المعالجة الآلية للمعطيات تتم أغلبها في شكل جماعات يتم إتفاقهم بمجرد إنتقال كلمة السر بينهم سواء كانوا أشخاص طبيعية أو معنوية.

-عقوبة الشروع : بإستقراء نص المادة رقم 394 مكرر 7 نلاحظ رغبة المشرع في توسيع نطاق العقوبة ، بحيث تشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية ، إذ جعل الشروع في إحداها معاقب عليه بنفس عقوبة الجريمة التامة.

ب-العقوبات التكميلية : تتمثل في مصادرة الأجهزة و البرامج و الوسائل المستخدمة في إرتكاب الجريمة الماسة بالأنظمة المعلوماتية مع مراعاة حقوق الغير حسن النية ، و إغلاق المواقع التي تكون محلا لهذه الجرائم ، و إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد أرتكبت بعلم مالكها.[73]

3-4-4-2 : العقوبات الموقعة على الشخص المعنوي:

تتمثل في عقوبة الغرامة المالية التي تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.[74]

أي أن المشرع الجزائري قد عاقب الشخص المعنوي في حالة إرتكابه لإحدى جرائم الإعتداء على نظام المعالجة الآلية للبيانات بغرامة مالية مرتفعة جدا مقارنة بالغرامة الموقعة على الشخص الطبيعي ، مع التأكيد على أن المسؤولية الجزائية للشخص المعنوي ، لا تغني عن مساءلة الأشخاص الطبيعية بصفتهم فاعلين أو شركاء في الجريمة.

و كنتيجة للحماية الجنائية المعلوماتية من خلال النصوص السابقة الذكر بموجب القانون رقم 15/04 المعدل ، تعتبر حماية فعالة لما تمتاز به من شمولية ، بحيث جاءت هذه النصوص لتشمل أغلب الجرائم التي قد تمس نظام المعالجة الآلية للمعطيات بصفة عامة ، كما تضمنت أغلب الجرائم التي قد تمس البيانات و المعطيات القانونية لهذا النظام.

3-4-5 : الهياكل الخاصة بالتصدي للجرائم المعلوماتية : تتمثل في

3-4-5-1 : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال:

أنشئت بموجب القانون رقم 09-04الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ، بحيث تقوم بتفعيل التعاون القضائي الأمني الدولي و إدارة و تنسيق العمليات الوقائية و المساعدة التقنية للجهات القضائية و الأمنية ، مع إمكانية تقديمها لخبرات قضائية عند الإعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستيراتيجية للإقتصاد الوطني.[75]

3-4-5-2 : الهيئات القضائية الجزائية المتخصصة :

أنشئت بموجب القانون رقم 04-14 المؤرخ في 2004/11/10 المعدل و المتمم لقانون الإجراءات الجزائية ، لتهتم بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، على أساس إختصاصها الإقليمي الموسع طبقا للمرسوم التنفيذي رقم 86-34 المؤرخ في 2006/01/05 ، الذي يجعلها تنظر في القضايا المتصلة بتكنولوجيا الإعلام و الإتصال المرتكبة في الخارج ، حتى و لو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني.[76]

3-4-5-3 : المعهد الوطني للأدلة الجنائية و علم الإجرام:

يتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة ، تضمن إنجاز الخبرة ، التكوين و التعليم و تقديم المساعدات التقنية ، بحيث تتكفل دائرة الإعلام الآلي و الإلكتروني بمعالجة و تحليل و تقديم كل دليل رقمي يساعد العدالة ، كما تقدم المساعدة التقنية للمحققين في المعاينات .[77]

3-4-5-4 : المديرية العامة للأمن الوطني :

تتصدى للجريمة الإلكترونية من عدة جوانب ، منها الجانب القانوني المهتمة بتطبيقه ، و الجانب التوعوي الذي سمح لها بتنظيم دروس توعية في مختلف المراحل الدراسية ، وكذا المشاركة في الملتقيات و الندوات الوطنية ذات الصلة بالتوعية بخطورة هذا النوع من الجرائم ، و كذا تأكيدا لعضويتها الفعالة في المنظمة الدولية للشرطة الجنائية INTERPOL التي تسهل التبادل المعلوماتي الدولي و تسهل الإجراءات القضائية الخاصة بتسليم المجرمين و مباشرة الإنابات القضائية و نشر أوامر القبض للمبحوث عنهم دوليا.[78]

4. خاتمة:

الجريمة المعلوماتية جريمة مستحدثة لم يتم الإتفاق على تعريف موحد لها و تتميز بخصوصية في كل عناصرها مقارنة بالجريمة التقليدية ، بحيث تشكل مخاطر كبيرة على حرمة حياة الأفراد و حقوقهم و كذا مصالح الدول ، بما يترتب عليها من مساس بمعلومات و أموال الأشخاص و المؤسسات سواء كانت عامة أو خاصة ذات التعاملات بالحاسب الآلي ، و حتى معلومات الدول و حكوماتها خاصة في ميادين الإقتصاد و الأمن و الدفاع و المشاريع التصنيعية في كل المجالات ، مما جعلها تسارع في التصدي لها و محاربتها إنطلاقا من عقد إتفاقيات تضم مجموعة مبادئ و أحكام تعكس وطنيا بواسطة وضع تشريعات و أجهزة تتصدى لهذه الجريمة ، مثل ما فعلت الجزائر من سن قوانين عامة و أخرى خاصة بها ، و أنشأت مجموعة من الأجهزة التي تساهم في الوقاية من هذه الجرائم الإلكترونية التي تتم بواسطة النظام المعلوماتي أو تتم على محتواه و مكافحتها.

و رغم ما أوردنا في البحث من طرق تصدي دولية لهذه الجريمة إلا أنه نظرا لخطورتها نقترح مايلي:

1-إعطاء تعريف جامع و موحد لهذه الجريمة المستحدثة من أجل تسهيل الوصول إلى حلها.

2-ضرورة إصدار قانون خاص بالجرائم المعلوماتية و طرق مكافحتها.

3-ضرورة سن إجراءات متناسبة مع هذا النوع من الجرائم بخصوص عمليات التحري عنها و كشفها و الحماية منها.

4-إنشاء محاكم متخصصة في الجرائم المعلوماتية في كل المجالس القضائية لمجابهتها.

5-ضرورة تكوين و تأهيل الجهات العاملة في مجال مكافحة الجرائم المعلوماتية مثل أفراد الضبطية القضائية و كذا النيابة العامة ، بشكل يساعد على حسن تعاملها مع هذا النوع من الجرائم.

6-ضرورة تفعيل التعاون الدولي لمكافحة هذه الجرائم العابرة للحدود من خلال سن مجموعة من التشريعات الوطنية المستمدة الأحكام من الإتفاقيات الدولية و الإقليمية الخاصة بمكافحة هذه الجرائم.

7-رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الإنترنت .

8-ضرورة حماية المواقع الإلكترونية سواء الخاصة بالأفراد أو العامة المتعلقة بالأشخاص المعنوية سواء كانت شركات أو بنوك أو مرافق الدولة ، من كل أنواع الإختراقات الغير مشروعة بواسطة وضع أنظمة حماية مناسبة مثل جدار النار المتصدي لحدوث الجرائم الإلكترونية.

9-و أخيرا ضرورة نشر التوعية حول الجرائم المعلوماتية و مخاطرها داخل المجتمعات ، عن طريق تعريف الأفراد و مسؤولي المؤسسات بكيفية الحفاظ على معلوماتهم الخاصة و التجارية و المالية...

5. قائمة المراجع:

[1]/ محمد زكي أبو عامر ، قانون العقوبات –القسم العام ، الطبعة الأولى ، دار المطبوعات الجامعية ، 1986 ، ص 35.

[2]/ محمود نجيب حسني ، شرح قانون العقوبات –القسم العام ، الطبعة السادسة، دار النهضة العربية، 1989 ، ص 40 و ما بعدها.

[3]/ خالد ممدوح إبراهيم ، أمن الجريمة الإلكترونية ، الدار الجامعية ، الإسكندرية ، 2010 ، ص 43.

[4]/ طارق إبراهيم الدسوقي عطية ،الأمن المعلوماتي : النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة للنشر، الاسكندرية ، 2009،ص 154.

[5]/ خالد ممدوح إبراهيم ، حوكمة الإنترنت ، الطبعة الأولى ، دار الفكر الجامعي ، الإسكندرية ، 2011 ، ص 357.

[6]/ خالد ممدوح إبراهيم ، أمن الجريمة الإلكترونية، مرجع سابق ، ص 42.

[7] / خالد ممدوح إبراهيم ، حوكمة الإنترنت، مرجع سابق ، ص 357.

[8] / قارة أمال ، الجريمة المعلوماتية ، رسالة ماجستير في القانون الجنائي و العلوم الجنائية ،كلية الحقوق بجامعة الجزائر1، 2002، ص 18.

[9]/ محمود أحمد عبابنة ، جرائم الحاسوب و أبعادها الدولية ، دار الثقافة للنشر و التوزيع ، عمان ، الأردن ، 2009 ، ص 19.

[10]/ عبد الله دغش العجمي ، المشكلات العملية و القانونية للجرائم الإلكترونية – دراسة مقارنة – رسالة ماجستير ، جامعة الشرق الأوسط ، 2014 ، ص 14.

[11]/ المادة رقم 02 من القانون رقم 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها ، ج ر 47 الصادرة في 2009/08/16.

[12] / سوير سفيان ، جرائم المعلوماتية ، رسالة ماجستير في العلوم الجنائية و علم الإجرام ، جامعة تلمسان ، 2011/2010 ، ص 11.

[13]/ محمود أحمد عبابنة ، محمد معمر الرازقي ، جرائم الحاسوب و أبعادها الدولية ، دار الثقافة للنشر و التوزيع ، 2005 ، ص 21.

[14]/ أسامة أحمد المناعسة ، جلال محمد الزغبي ، جرائم الحاسب الآلي و الإنترنت ، دراسة تحليلية مقارنة ، دار وائل للنشر و التوزيع ، 2001 ، ص 97.

[15]/ عبد الله دغش العجمي ، مرجع سابق ، ص 18.

[16]/ أسامة أحمد المناعسة ، جلال محمد الزغبي ، مرجع سابق ، ص 99.

[17]/ أحمد خليفة الملط ، الجرائم العلوماتية ، دار الفكر الجامعي ، الإسكندرية ، 2005، ص 105.

[18]/ خالد ممدوح إبراهيم ، أمن الجريمة الإلكترونية ، مرجع سابق ، ص 11.

[19]/ أحمد خليفة الملط ، مرجع سابق ، ص 98 و ما بعدها.

[20]/ سعيد نعيم ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ، شهادة ماجستيرفي العلوم القانونية ، جامعة الحاج لخضر بباتنة ، 2013/2012 ، ص 35.

[21] / نفس المرجع ، ص 34.

[22] / حفوطة الأمير عبد القادر ، غرداين حسام ، الجريمة الإلكترونية و آليات التحدي لها ، مداخلة في الملتقى الوطني الموسوم بآليات مكافحة الجرائم الإلكترونية في التشريع الجزائري ، الجزائر ، 2017/03/29 ، ص 93.

[23]/ ذياب موسى البدانية ، الجرائم الإلكترونية –المفهوم و الأسباب- مداخلة في الملتقى العلمي حول الجرائم المستحدثة في ظل الغيرات و التحولات الإقليمية و الدولية ، الأردن ، بتاريخ 2014/04/02.

[24]/ صغير يوسف ، الجريمة المرتكبة عبر الإنترنت ، مذكرة ماجستير في القانون الدولي للأعمال ،كلية الحقوق و العلوم السياسية ، جامعة مولود معمري بتيزي وزو ، 2013 ، ص ص 14، 15

[25]/ أحمد خليفة الملط ، مرجع سابق ، ص 103.

[26]/ محمد حماد مرهج الهيثي ، التكنولوجيا الحديثة و القانون الجنائي ، الطبعة الأولى، دار الثقافة للنشر و التوزيع ، عمان ، 2004، ص 166.

[27] / عبد الفتاح بيومي حجازي ، مكافحة جرائم الكمبيوترو الإنترنت في القانون العربي، دار الكتب العربية ، الطبعة الأولى، مصر، 2007 ، ص 83 و ما بعدها.

[28]/ محمد علي العريان ، الجرائم المعلوماتية ، دار الجامعة الجديدة ، الإسكندرية ، 2011 ، ص 80.

[29]/ محمد عبد الله قاسم ، الحماية الجنائية للمعلومات الإلكترونية ، دار الكتب القانونية ، الطبعة الأولى ، مصر ، 2010 ، ص 148.

[30]/ عبد الله دغش العجمي ، مرجع سابق ، ص34.

[31]/ محمد الجبور ، الوسيط في قانون العقوبات ، القسم العام ، الطبعة الأولى ، دار وائل ، عمان ، 2012 ، ص 59.

[32] / نفس المرجع ، ص 160.

[33]/ عبد الله دغش العجمي ، مرجع سابق ، ص 35 و مابعدها.

[34]/المادة رقم 02 من معاهدة بودابست الموقعة في 2001 /11/23 بالعاصمة المجرية بودابست و المتعلقة بمواجهة الجريمة المعلوماتية

[35]/المادة رقم 03 من نفس المرجع.

[36]/المادة رقم 05 من نفس المرجع.

[37]/المادة رقم 06 من نفس المرجع.

[38]/المادة رقم07 من نفس المرجع.

[39]/المادة رقم 08 من نفس المرجع

[40]/المادة رقم 09 من نفس المرجع.

[41]/المادة رقم 10 من نفس المرجع.

[42]/عبد المالك صاولي ، ، تشريعات الجريمة الإلكترونية في البيئة الإعلامية العالمية ، مجلة الحقوق و العلوم السياسية ، جامعة عباس لغرور بخنشلة العدد 10 جوان 2018 ، ص 466.

[43]/ ممدوح عبد الحميد عبد اللطيف، جرائم إستخدام شبكة المعلومات العالمية ، مداخلة في مؤتمر القانون و الكمبيوتر و الإنترنت ،كلية الشريعة و القانون ، بجامعة الإمارات ، 2000، ص 05.

[44]/ نمديلي رحيمة ، خصوصية الجريمة الإلكترونية في القانون الجزائري و القوانين المقارنة ، مداخلة في المؤتمرالدولي الرابع عشر المتعلق بالجرائم الإلكترونية ، طرابلس في 24-25 مارس 2017 ، ص 11.

[45]/ عبد المالك صاولي ، مرجع سابق ، ص ص 464 ، 465.

[46]/ عبد الله عبد الكريم عبد الله ، جرائم المعلومات و الإنترنت ، منشورات الحلبي الحقوقية ، بيروت ، 2007 ،ص 63.

[47]/ عبد الفتاح بيومي الحجازي ، التوقيع الإلكتروني في النظم القانونية المقارنة ، دار الفكر الجامعي ، الإسكندرية ، 2005 ،ص 556.

[48]/ عبد الله عبد الكريم عبد الله ، مرجع سابق ، ص 85.

[49]/ القانون رقم 04-15 المؤرخ في 2004/11/10 المعدل و المتمم لقانون العقوبات رقم 66-156 ، ج ر العدد 71 لسنة 2004.

[50]/ القانون رقم 06-22 المؤرخ في 2006/12/20 المعدل و المتمم لقانون الإجراءات الجزائية رقم 66-155 ، ج ر العدد 84 الصادر في 2006/12/24 .

[51]/ المواد من رقم 02 إلى 12 من القانون رقم 09-04 المؤرخ في 2009/08/05 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها ، ج ر العدد 47 الصادر في 2009/08/16.

[52]/ الأمر رقم 03-05 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف و الحقوق المجاورة ، ج ر العدد 44 الصادر في 2003/07/23.

[53]/ القانون رقم 2000-03 المؤرخ في 2000/08/05 المتعلق بالبريد و الإتصالات السلكية و اللاسلكية ، ج ر العدد 48 الصادر في 2000/08/06.

[54]/ القانون رقم 08-01 المؤرخ في 2008/01/23 المعدل و المتمم للقانون رقم 83-01 المتعلق بالتأمينات ، ج ر العدد 4 الصادر في 2008/01/27.

[55]/ المادة رقم 01 من إتفاقية بودابست الموقعة في 2001 /11/23 السالفة الذكر.

[56]/ بدري فيصل ، مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي ، أطروحة دكتوراه ،كلية الحقوق بجامعة الجزائر 1 ، 2018/2017 ، ص 155.

[57]/ المواد رقم 35 و 39 و 47 من المرسوم الرئاسي رقم 20-442 المؤرخ في 2020/12/30 المتعلق بالتعديل الدستوري المصادق عليه في إستفتاء 2020/11/01 ، ج ر العدد 88 الصادر في 2020/12/30.

[58]/ المادة رقم 74 من المرسوم الرئاسي رقم 20-442 المتضمن التعديل الدستوري لسنة 2020 السالف الذكر.

[59]/ الأمر رقم 03-05 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف و الحقوق المجاورة السالف الذكر.

[60]/ الأمر رقم 03-07 المؤرخ في 2003/07/19 المتعلق ببراءات الإختراع ، ج ر العدد 44 الصادر في 2003/07/23.

[61]/ سوير سفيان ، مرجع سابق ، ص 35 و مابعدها.

[62]/ صغير يوسف ، مرجع سابق ، ص 54.

[63]/ المادة رقم 394 مكرر فقرة 01 من قانون العقوبات رقم 04-15 المعدل و المتمم للأمر رقم 156/66 السالف الذكر.

[64]/ المادة رقم 394 مكرر فقرة03 من نفس المرجع.

[65]/ المادة رقم 394 مكرر 01 من نفس المرجع.

[66]/ المادة رقم 394 مكرر 02 فقرة 01 من نفس المرجع.

[67]/ المادة رقم 394 مكرر 02 فقرة 02 من نفس المرجع.

[68]/ المادة رقم 394 مكرر 05 من نفس المرجع .

[69]/ المادة رقم 394 مكرر 07 من نفس المرجع.

[70]/ المادة رقم 394 مكرر 03 من نفس المرجع .

[71]/ المواد رقم 394 مكرر و 394 مكرر 1 و 394 مكرر 2 من نفس المرجع.

[72]/ المادة رقم 394 مكرر 03 من نفس المرجع.

[73]/ المادة رقم 394 مكرر 06 من نفس المرجع.

[74]/ المادة رقم 394 مكرر 04 من قانون العقوبات رقم 04-15 المعدل و المتمم للأمر رقم 156/66 السالف الذكر.

[75]/ المواد من 13 إلى 18 من القانون رقم 09-04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها السالف الذكر.

[76]/ المادة رقم 15 من نفس المرجع.

[77]/ فضيلة عاقلي ، الجريم الإلكترونية و إجراءات مواجهتهامن خلال التشريع الجزائري ، مداخلة في المؤتمر الدولي الرابع عشر حول الجرائم الإلكترونية المنعقد في طرابلس بتاريخ 25/24 مارس 2017 ، ص 19.

[78]/ علي عبد القادر القهوجي ، الحماية الجنائية لبرامج الحاسب الآلي ، دار الجامعة للطباعة و النشر ، بيروت ، 1999 ، ص 120.