الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE Abdelhamid Ibn Badis MOSTAGANEM

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق و العلوم السياسية

قسم: القانون العام

المرجع:

مذكرة نهاية الدراسة لنيل شهادة الماستر

الجريمة المعلوماتية واثارها على التطور الاقتصادي

ميدان الحقوق و العلوم السياسية

الشعبة: حقوق

التخصص: قانون جنائي وعلوم الجنائية

من إعداد الطالب(ة):

براء منصور

تحت إشراف الأستاذ(ة):

باسم شهاب

أعضاء لجنة المناقشة

الأستاذ(ة): بن عوايلي علي	رئيسا
الأستاذ(ة): باسم شهاب	مشرفا مقررا
الأستاذ(ة): جلطي منصور	مناقشا

السنة الجامعية: 2021/2020

شكر وتقدير

اشكر الله العلي القدير الذي انعم علي بنعمة العقل والدين القائل في محكم التنزيل:

{وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ}

وعن ابي هريرة رضي الله عنه، قال صلى الله عليه وسلم

(من لا يشكر الناس، لا يشكر الله)

واثني ثناءا حسنا وايضا وفاءا وتقديرا واعترافا مني بالجميل، اتقدم بجزير الشكر لأولئك المخلصين الذين لم يدخروا جهدا في مساعدتي في مجال البحث العلمي، واخص بالذكر الاستاذ الفاضل "باسم شهاب" على

فترة الدراسة، وصاحب الفضل في توجيهي ومساعدتي في تجميع المادة البحثية، فجزاه الله كل الخير

ونتقدم بعظيم التقدير والثناء للسادة الأساتذة أعضاء لجنة المناقشة كل باسمه على قبولهم مناقشة هذا البحث

إلى كل أساتذة كلية الحقوق والعلوم السياسية لجامعة مستغانم

واخيرا اتقدم بجزيل شكري الى كل من مدوا لي يد العون والمساعدة في اخراج هذه الدراسة على اكمل وجه

اهداء

بسم الله الرحمن الرحيم

{قُلْ إِنَّ صَلَاتِي وَنُسُكِي وَمَحْيَايَ وَمَمَاتِي لِلَّهِ رَبِّ الْعَالَمِينَ}

صدق الله العظيم

اهدي هذا العمل المتواضع بالدرجة الاولى الى روح والدتي التي اخذها الموت قبل اشهر قليلة من انهائي هذه الدراسة كنت اتمناها ان تكون اول من تفرح بإنجازي لهذا البحث رحمها الله واسكنها فسيح جناته

كما اهدي هذا البحث الى روح والدي الذي لو كان موجودا لأعتز بي على ما وصلت اليه رحمه الله واسكنه فسيح جناته

واهدي هذا العمل الى روح الفقيد اخي(نعيم) رحمه الله واسكنه فسيح جناته

واهدي هذا العمل الى من قال فيهم المولى عز وجل بعد بسم الله الرحمن الرحيم

{قَالَ سَنَشُدُّ عَضُدَكَ بِأَخِيكَ وَنَجْعَلُ لَكُمَا سُلْطَانًا فَلَا يَصِلُونَ إِلَيْكُمَا ۚ بِآيَاتِنَا أَنتُمَا وَمَنِ اتَّبَعَكُمَا الْغَالِبُونَ}

الى اخواني واخواتي الذين علموني الصبر والجهد والكفاح الذين كانوا سندا لي لوقفتهم بجانبي طوال مشواري الدراسي

واهدي هذا العمل الى ابناء اخوتي واخواتي جميعا

الى كل من شجعني في انجاز ومواصلة هذا الجهد العلمي المتواضع لهم جميعا مع فائق المحبة والاحترام والعرفان

قائمة المختصرات

1- باللغة العربية

- ب.ط: بدون طبعة
- ب.ب.ن: بدون بلد النشر
- ب.س.ن: بدون سنة نشر
- ص: صفحة
- ج: جزء
- ع: عدد
- ج.ر: جريدة رسمية

2- باللغة الاجنبية

- oecd: منظمة التعاون الاقتصادي والتنمية
- rsa: العالمية لأمن المعلومات

- op-cite:operto-citato

- p:page

مقدمة

عرف العالم منذ منتصف القرن العشرين ثورة جديدة تم تسميتها بالثورة المعلوماتية، فقد اصبحت قوة لا يستهان بها في ايدي الدول والافراد، وكان التطور الهائل الذي شهده قطاعي تكنلوجيا المعلومات والاتصالات والاندماج المذهل بينهما فيما بعد المحور الاساسي الذي قامت عليه هذه الثورة.

بالرغم من المزايا الهائلة التي تحققت وتتحقق كل يوم بفضل تقنية المعلومات على جميع الأصعدة وفي شتى ميادين الحياة، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة جراء سوء استخدام هذه التقنية المتطورة، والانحراف عن الغرض المرجو منها إذ أدت إلى تفشي ظاهرة إجرامية مستحدثة ألا وهي ظاهرة الجريمة المعلوماتية.

هنا نشأ ما يسمى جرائم المعلوماتية والتي يستخدم فيها الكمبيوتر لأغراض غير شرعية، مثل سرقة الأموال عن طريق اختراق نظام الكمبيوتر الخاص بمؤسسة أو مصرف معين أو سرقة المعلومات عن طريق اختراق شبكة اتصالات معلوماتية أو يكون الاختراق لأهداف سياسية أو عسكرية أو دينية أو غير ذلك.

إن هذا النوع من الجرائم لا يتطلب جهد عضلي كبير، بل يرتكب بمجرد لمس لوحة المفاتيح إذ تحدث دمارا وخرابا في اقتصاديات كبرى للشركات، ومختلف المؤسسات الاقتصادية، ويصعب تحديد حجم الخسارة الفعلية التي تنجم عن جرائم الكمبيوتر حيث أن بعض هذه الجرائم لا يتم اكتشافها والبعض الآخر يتم اكتشافها ولكن لا يعلن عنها من قبل الشركات والمؤسسات التي تتعرض لها حتى لا يؤثر ذلك على سمعتها وثقة المتعاملين معها.

وغالبا تكون البنوك والمصارف ومراكز المعلومات المهمة هدفا لتلك الجرائم كما أن نسبة كبيرة من مرتكبي تلك الجرائم تكون من موظفي المصارف والمنشآت نفسها حيث يسهل عليهم معرفة الرموز المستخدمة للدخول إلى النظام او المستخدمة في عملية تحويل الأموال وبالتالي استخدامها في ارتكاب الجريمة.

كما ساهمت الدول في مكافحة الجريمة المعلوماتية عن طريق الاتفاقيات الدولية، حيث قامت بوضع سياسة عامة من اجل تجريم الافعال الماسة بالمعلومات، ولقد شارك في اعداد

الاتفاقيات عدة دول احست بمدى طورة هذه الجريمة، كما ان دول العالم قامت على تعديل قوانينها الداخلية ونصت على تجريم أي اختراق او دخول غير شروع الى البيانات او المعلومات.

1- اهمية البحث

لعل الأهمية الرئيسية حول هذا الموضوع تكمن في إن المعلومة أصبحت قوة اقتصادية مستحدثة، حيث برزت الآثار سلبية للجريمة المعلوماتية على الاقتصاد وبشكل مباشر على الشركات خاصة المؤسسات المصرفية حيث أنها الاكثر عرضة لهذا النوع من الجرائم، يرجع ذلك كون النقود هي السلعة التي تتعامل بها هذه المؤسسات، وقد سببت الجرائم المعلوماتية خسائر مالية فادحة سنويا لهذه الشركات بالإضافة إلى خسارة الثقة التي يضعها فيها الزبائن، وهكذا أصبحت الجرائم المعلوماتية حجر عقبة أمام نمو وازدهار المؤسسات وجذب أكبر عدد ممكن من الزبائن وكسب ثقتهم، وتفاقمت المشكلة أكثر فأكثر على الرغم من الاساليب الامنية المتطورة وأحدث التقنيات المستخدمة، والتقارير العالمية التي تصدرها الهيئات المتخصصة توضح حجم المشكلة في مختلف أنحاء العالم.

2- اسباب اختيار الموضوع

من الاسباب التي دفعتني إلى تناول هذا الموضوع بالدراسة، راجع لحداثة الموضوع، و التزايد المستمر للجرائم المعلوماتية، و كذلك الرغبة في التعمق في البحث ومواجهة النشاط الاجرامي المعلوماتي، وبيان مدى تأثير الجرائم المعلوماتية على الاقتصاد، وكيفية التوصل الى وضع حد لها عن طريق مكافحتها دوليا واقليميا.

3- اهداف الدراسة

أن الهدف الأساسي من وراء هذه الدراسة، نظرا لتزايد استخدام الحاسوب والأنترنت وتزايد التعاملات الالكترونية بين الافراد والشركات من خلال التجارة الالكترونية، فان هدفها الرئيسي حمايتها من الاعمال غير المشروعة وتجنب وسائل الاحتيال والغش و سرقة المعلومات الى اخره، وبيان كيف يمكن لهذه الجريمة ان تلحق ضرر بالاقتصاد سواء على مستوى الدول او على مستوى الشركات وكيفية مواجهتها والتصدي للضرر الناجم عنها.

4- الدراسات السابقة

لقد تم الاستعانة لدراسة موضوع البحث بعدة اطروحات ورسائل ومذكرات أهمها:

- اطروحة دكتوراه تحت عنوان الاسرار المعلوماتية و حمايتها الجزائية، لربحي عزيزة، جامعة ابي بكر بالقايد.

- اطروحة دكتوراه تحت عنوان مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي، لبدري فيصل، جامعة الجزائر 01.

- رسالة ماجستير تحت عنوان جرائم السرقة والاحتيال عبر الانترنت، لخديجة دحمان صبايحية، جامعة الجزائر.

- مذكرة ماستر تحت عنوان الجريمة المعلوماتية واثارها على النمو الاقتصادي، لامال اكرام، جامعة ام البواقي.

5- الاشكالية

من خلال ما تقدم يمكن ان نطرح الاشكالية التالية والمراد معالجتها في دراستنا وهي:

- المقصود بالجريمة المعلوماتية، وكيفية مواجهتها في التأثير على التطور الاقتصاد.

6- المنهج المتبع في الدراسة

أما المنهج المتبع في دراسة هذا الموضوع فقد اعتمدنا في سبيل الوصول إلى الاجابة على الاشكالية المطروحة على المنهج تحليلي، لان دراستها أسندت على بيان وتحليل أهم النصوص القانونية المنظمة للجرائم المعلوماتية، كما تم الاستعانة بالمنهج الوصفي، لأنه انسب المناهج لوصف الجرائم المعلوماتية.

الفصل الاول

الفصل الاول

ماهية الجريمة المعلوماتية

تمهيد

المبحث الاول: مفهوم الجريمة المعلوماتية

المطلب الاول: تعريف الجريمة المعلوماتية

الفرع الاول: موقف الهيئات الدولية والتشريعات الوطنية من تعريف الجريمة المعلوماتية

الفرع الثاني: التعريف الفقهي للجريمة المعلوماتية

الفرع الثالث: تطور الجريمة المعلوماتية

المطلب الثاني: خصائص ودوافع الجريمة المعلوماتية

الفرع الاول: خصائص الجريمة المعلوماتية

الفرع الثاني: دوافع ارتكاب الجريمة المعلوماتية

المبحث الثاني: تصنيف الجرائم المعلوماتية و تحديد مرتكبيها

المطلب الاول: تصنيف الجرائم المعلوماتية

الفرع الاول: التصنيف التشريعي للجرائم المعلوماتية

الفرع الثاني: التصنيف الفقهي للجرائم المعلوماتية

المطلب الثاني: مرتكبو الجريمة المعلوماتية

الفرع الاول: مفهوم المجرم المعلوماتي

الفرع الثاني: تصنيف مرتكبي الجرائم المعلوماتية

تمهيد

بالرغم من المزايا الهائلة التي تتدفق كل يوم وهذا بفضل تقنية المعلوماتية التي ساهمت بدورها في تطور النمط الاجتماعي والإنساني الذي أصبح يعتمد عليها بشكل كبير كالحواسيب وشبكات اتصال وتبادل المعلومات، من أجل قضاء حوائجه دون أي مجهود أو عناء كالتنقل من مكان لآخر من أجل جلب المعلومات، الا أن العالم المعاصر أصبح يواجه العديد من المشاكل، وهذا راجع إلى تفاقمها الواسع الذي أدى بدوره إلى تحولها لساحة مفتوحة لممارسة جميع أنواع الجرائم المعلوماتية الممكنة، لكن ولابد من الإشارة أنه لا وجود للجريمة المعلوماتية دون وجود الحاسوب بمكوناته المادية والمعنوية، فالحاسوب قد يكون هدفا أو أداة لارتكاب الجريمة وقبل التعرف إلى مشكلة تأثير الجرائم المعلوماتية على اقتصاد الوقت وهو ما يتطلب للتعرف على مفهوم الجريمة المعلوماتية وذلك في المبحث الأول تصنيف الجرائم المعلوماتية و تحديد مرتكبيها في المبحث الثاني.

المبحث الأول: مفهوم الجريمة المعلوماتية

لقد ترتب على الاستخدام المتزايد لنظم المعلومات إلى نشوء ما يعرف بالجريمة المعلوماتية، ولقد تعددت التوجهات حول تعريف الجريمة المعلوماتية باعتبارها جريمة مستحدثة يعتمد مرتكبها على وسائل تقنية ويكون ذا دراية كافية باستخدام النظم المعلوماتية لذلك فإنه يتوجب الإحاطة بمفهومها الدقيق.

نتيجة لحداثة الجرائم المعلوماتية وارتباطها بتكنولوجيا متطورة نحاول من خلال هذا المبحث التطرق إلى تعريف الجريمة المعلوماتية وبيان أهم الخصائص التي تميزها ،والأسباب المؤدية إلى ارتكابها.

المطلب الأول: تعريف الجريمة المعلوماتية

تعددت التعريفات التي تناولت الجريمة المعلوماتية، ويرجع ذلك إلي الخلاف الذي أثير بشأن تعريف هذه الجريمة، فالجرائم المعلوماتية هي صنف جديد من الجرائم، ذلك أنه مع ثورة المعلومات والاتصالات ظهر صنف جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى إلكترونية قد يصعب التعامل معها، لأن الجريمة المعلوماتية هي من الظواهر الحديثة، وذلك لارتباطها بتكنولوجيا جديدة هي تكنولوجيا المعلومات والاتصالات، وقد أحاط بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية لوضع تعريف جامع مانع لها.

أثيرت العديد من التساؤلات حول تحديد الطبيعة القانونية للجريمة المعلوماتية، ويرجع سبب ذلك إلى تعدد وجهات النظر بخصوص هذا النوع من الجرائم حيث ظهرت عدة آراء في محاولة فهم المقصود بالجريمة المعلوماتية، وتحديد تعريف لها مع تبيين طبيعتها القانونية، كما أن تعريف الجريمة المعلوماتية يستوجب الالمام بالجانب الموضوعي والاجرائي لها، مع دراسة العوامل المختلفة التي تتداخل في تكوين الجريمة، وللإحاطة بالأمور الفنية لها، يجب ان نبين موقف الهيئات الدولية والتشريعات الوطنية من تعريف الجريمة المعلوماتية، وكذلك تبيين المعايير التي استند عليها الفقهاء في تعريفهم للجريمة المعلوماتية، وبيان تطور الجريمة المعلوماتية.

الفرع الأول: موقف الهيئات الدولية والتشريعات الوطنية من تعريف الجريمة المعلوماتية

في أول السبعينات ازدهرت صناعة جديدة أطلق عليها صناعة المعلومات، وأصبحت مصدرا للثروة وتتصف بعظمة التعقيد التقني وضخامة ما يستثمر فيها من أموال، وأصبحت مقياسا لتقدم

الأمم[1]، وأصبح توفيرها وحسن استغلالها من الأسس الضرورية لدفع عجلة التقدم في الأمم والمجتمعات وصار توفيرها وانسيابها بمثابة النبض والعصب لجهود التنمية والتحديث والرقي المعرفي والحضاري وبات الوعي بأهميتها مظهرا ومقياسا لتقدم الدول ومن ثم بات من الضروري، بعد تفاقم الاعتداءات على الأنظمة المعلوماتية، استدعى تدخلا تشريعيا صريحا سواء على المستوى الدولي او الداخلي .

أولا: تعريف الهيئات الدولية للجريمة المعلوماتية

أن الجريمة المعلوماتية لم يقتصر صداها على القانون الداخلي بل امتد ليشمل العديد من الدول، وأمام هذا التطور التكنولوجيا الناجم عن استخدام الانترنت والحاسوب، سارعت الدول لعقد الاتفاقيات الدولية لتحديد هوية الجاني والقبض عليه ومن هنا يتجسد مبدأ التعاون الدولي في مكافحة الجرائم المعلوماتية.

يعرف خبراء منظمة التعاون الاقتصادي والتنمية(OECD) الجريمة المعلوماتية بأنها:" كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/ أو نقلها"[2]، ويتبنى هذا التعريف الفقيه الألماني(Ulrich siehr) يعتمد هذا التعريف على معيارين هما: وصف السلوك، واتصال السلوك بالمعالجة الآلية للبيانات أو نقله.

وعرف الجريمة المعلوماتية خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي (OECD) بأنها:" كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".[3]

قدمت المادة الأولى من الاتفاقية الدولية للإجرام ألمعلوماتي تعريف للنظام ألمعلوماتي على النحو التالي :"يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو ذات صلة بذلك ويقوم إحداهما أو أكثر من واحد منها تبعا للبرنامج بعمل معالجة آلية للبيانات ويقصد ببيانات الكمبيوتر أية عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل مناسب لعملية

[1]- هشام فريد رستم، جريمة الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، بحث مقدم لمؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين، مجلة الأمن العام، العدد151، سنة 1995، ص23.
[2]- موقع منظمة التعاون الاقتصادي والتنمية،www.oecd.org.
[3]- المرجع نفسه.

المعالجة داخل منظومة الكمبيوتر بما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدي وظائفها".[1]

عرفت اتفاقية بودابست في المادة الأولى منها المنظومة المعلوماتية والمعطيات المعلوماتية:

أ/المنظومة المعلوماتية: "أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها أو ذات صلة بذلك ويقوم أحدها أو أكثر من واحد منها تتبعا للبرنامج بعمل معالج آلية للمعطيات".

ب/المعطيات المعلوماتية:" أية عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل معين جاهز لعملية المعالجة داخل منظومة معلوماتية بما في ذلك البرامج الماسة لجعل منظومة معلوماتية تطبق وظيفة".[2]

عرف المؤتمر العاشر للأمم المتحدة لمنع الجريمة ومعاقبة المجرمين الجريمة المعلوماتية بأنها :"أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية".[3]

و كما عرفت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سنة 2010، و ذلك تحت الفصل الأول بعنوان أحكام عامة و ذلك من خلال المادة 02 من الاتفاقية بان جريمة تقنية المعلومات هي: "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات و ترتيبها و تنظيمها و استرجاعها و معالجتها و تطويرها و تبادلها وفقا للأوامر والتعليمات المخزنة المرتبطة سلكيا أو لا سلكيا في نظام أو شبكة".[4]

أشارت الأمم المتحدة في المدونة الصادرة عنها بشان الجريمة المعلوماتية، الى وقوع خلاف بين الخبراء حول العناصر المكونة لجرائم المعلومات، ولعل هذا ما يفسر عدم التوصل إلى تعريف متفق عليه دوليا.

---

[1]- اتفاقية بودابست الدولية حول الإجرام الالكترونية، أبرمت بتاريخ 2001/11/08، من طرف المجلس الأوروبي، وتم وضعها للتوقيع في تاريخ2001/11/23.

1- المادة (1) من اتفاقية بودابست الدولية حول الإجرام الالكترونية .

2- مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين، عقد هذا المؤتمر في فيينا، في الفترة ما بين (10-17) افريل، 2000.

[3]- لاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المنبثقة عن اجتماع مجلس الوزراء الداخلية والعدل العرب بصفة مشتركة، بمقر الأمانة العامة لجامعة الدول العربية، بالقاهرة مصر، بتاريخ 2010/12/21.

ثانيا: تعريف التشريعات الوطنية للجريمة المعلوماتية

كانت السويد أول دولة تضع قانون لتنظيم سجلات الحاسب الآلي وحماية البيانات، وقادت موجة التشريع في هذا المجال من خلال قانون عام 1973بشأن حماية البيانات.[1]

قد عرف المشرع الأمريكي المعلومات في قانون المعاملات التجارية الإلكترونية لسنة 1999 بالفقرة العاشرة من المادة الثانية بأنها تشمل البيانات والكلمات والصور والأصوات و الرسائل وبرامج الكمبيوتر الموضوعة على الأقراص المرنة وقواعد البيانات أو شبه ذلك.

كما ظهر أول نص قانوني في مجال جرائم المعلوماتية سنة 1988في فرنسا[2]، رغم أنه قبل ذلك كانت أول المحاولات لمد سلطان قانون العقوبات لحماية المال ألمعلوماتي بفرنسا من طرف وزير العدل وذلك سنة 1985، عندما تقدم بمشروع قانون عقوبات جديد، أضاف بموجبه بابا رابعا للكتاب الثالث منه بعنوان "الجرائم في المادة المعلوماتية" تكون من ثمانية مواد(من7/307إلى 8/307)، لكن هذا المشروع لم يجد سبيله للتطبيق.

لقد شهد العالم في الآونة الأخيرة تطورا مذهلا وسريعا في مجال المعلوماتية، ومنه تسارع المشرعين لسن قوانين الهدف منها هو المواجهة الموضوعية والإجرائية لهذا النوع من الجرائم، قياسا على تسارع وتيرة الاعتماد على المعلوماتية في شتى مناحي الحياة، حتى باتت ضرورة لا يمكن الاستغناء عنها، وأصبحت مقياسا لتطور الدول .

إن غالبية المشرعين تجنبوا الخوض في مسألة وضع تعريف تشريعي لنظام المعالجة الآلية للمعطيات و أوكلوا مهمة ذلك إلى الفقه والقضاء، إلا أن بعضهم من جهة أخرى اتجهوا إلى وضع تعريف لنظام المعلومات وليس لنظام المعالجة الآلية للمعلومات، ومن بين التشريعات التي عرفت النظام ألمعلوماتي نذكر.

[1]-Michael (J) Privacy and Human Rights: An international and comparative study wide special reference to developments in information technology.dartmouth(1994).p.12.

[2]- Loi n°88-19 du 05 janvier 1988 relative à la fraude informatique, JORF du 06 janvier 1988 (LOI GODFRAIn).

1- تعريف المشروع الجزائري للجرائم المعلوماتية

عرف المشروع الجزائري الجرائم المعلوماتية في الماد 02 من قانون 09/04 على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحدد في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن منظومة معلومات أو نظام الاتصالات الالكترونية".[1]

ومن خلال هذا التعريف الذي جاء به هذا القانون 09/04 نلاحظ على أن المشرع الجزائري لم يقم بتحديد درجة دور المنظومة المعلوماتية أو نظام الاتصالات الالكترونية في ارتكاب هذه الجرائم إذ حسب التعريف فانه يكفي مجرد أن ترتكب الجريمة أو يسهل ارتكابها بالمنظومة المعلوماتية أو نظام الاتصالات الالكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم حتى تلك الجرائم التي يكون فيها للتقنية المعلوماتية دور ثانوي، كما أن المشرع الجزائري لم يحدد صور السلوك المجرم الذي يرتكب أو يسهل ارتكابه منظومة معلوماتية أو نظام الاتصالات الالكترونية.

2- تعريف المشرع السعودي للجريمة المعلوماتية

عرف المشرع السعودي الجرائم المعلوماتية المادة 01 من قانون مكافحة جرائم المعلومات السعودي، الصادر بالمرسوم الملكي رقم م/17 الصادر في 1428/3/8هجري بناء على قرار مجلس الوزراء رقم (79) المؤرخ في 1428/3/7هجري الجريمة المعلوماتية بأنها: "أي فعل يرتكب متضمن استخدام الحاسوب الآلي أو الشبكة المعلوماتية بالمخالفة الأحكام هذا النظام".[2]

3- تعريف المشرع الأردني للجريمة المعلوماتية

حيث عرف هذا القانون بدوره من خلال نص المادة 2 الفقرة 10 أيضا نظام معالجة المعلومات على أنه: " النظام الإلكتروني المستخدم لإنشاء رسائل المعلومات أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو تجهيزها على أي وجه أخر".[3]

---

[1]- القانون الجرائري رقم 09/04 ، المؤرخ في 05/شعبان/2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات إعلام واتصال ومكافحتها، الجريد الرسمية العدد 47 ، الصادر في 16/شعبان/ 2009.

[2] - المرسوم السعودي رقم م/17، المؤرخ في 1428/3/7ه، المتضمن نظام مكافحة جرائم المعلوماتية، الصادر بتاريخ 1428/3/8ه.

[3]- قانون الاردني رقم 85 ، لسنة 2001 ، الجريدة الرسمية للمملكة الأردنية الهاشمية رقم 4524 ، الصادر بتاريخ 2001/12/31م.

4- تعريف المشرع الفلسطيني للجريمة المعلوماتية

عرف المشرع الفلسطيني الجرائم المعلوماتية في المادة 12 من القانون رقم (10) المتضمن الجرائم الالكترونية، على أنها "كل من استخدم الشبكة الالكترونية أو إحدى وسائل تكنولوجيا المعلومات في الوصول دون وجه حق، إلى أرقام أو بيانات وسيلة التعامل الالكترونية أو التلاعب فيها".[1]

5- تعريف المشرع الإماراتي للجريمة المعلوماتية

حيث عرف هذا القانون هو الأخر من خلال نص المادة 2 الفقرة 6، بصدد تعريف المصطلحات أيضا نظام المعلومات الإلكتروني على أنه : "نظام إلكتروني لإنشاء أو استخراج أو إرسال أو استيلام أو تخزين أو عرض أو معـالجة المعلومات أو الرسائل إلكترونيا".[2]

الفرع الثاني: التعريف الفقهي للجريمة المعلوماتية

على الرغم من تنامي جهود التصدي لظاهرة الإجرام ألمعلوماتي إلا أنه لا يوجد تعريف محدد ومتفق عليه بين الفقهاء حول مفهوم الجريمة المعلوماتية، فقد ذهب جانب من الفقه إلى تناولها بالتعريف على نحو ضيق وجانب أخر عرفها على نحو موسع .

أولا: التعريف الضيق للجريمة المعلوماتية

لقد اعتمد أنصار هذا الاتجاه في تعريفهم للجريمة المعلوماتية إذ نظر إليها من زاوية محددة و اعتمدوا على تعريفاتهم على أساس الأداة أو الوسيلة على ارتكاب الجريمة و المتمثلة في أداة الحاسب الآلي، ومن بين التعريفات التي جاء بها الفقه إذ اعتبرها على أنه " كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابها من ناحية و لملاحقته و تحقيقه من ناحية أخرى ".[3]

---

[1] - القرار الفلسطيني رقم 10، المتضمن قانون الجرائم الالكترونية الفلسطيني، الصادر بتاريخ 2018/04/17م.

[2]- قـانون إمارة دبـي رقم 02 ، لسنة 2002، متعلق بالمعـاملات والتجارة الإلكترونية ، صادر بتاريخ 12/ فبراير/ 2002.

[3]- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، د.ط، بيروت، منشورات الحلبي الحقوقية، 2005، ص28.

بمعنى يجب أن يتوافر قدر كبير من العلم بهذه التكنولوجيا لدى الجناة، والمختصين بملاحقتها من قضاة وضباط الشرطة وغيرهم.

من أهم التعريفات التي وضعها أنصار هذا الاتجاه على أنها "كل سلوك غير مشروع يكون العلم بتكنولوجيات الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية وملاحقته وتحقيقه من ناحية أخرى.[1]

من التعريفات التي وضعها أنصار هذا الاتجاه أيضا ما ذهب إليه الفقيه(MERWE) حيث يرى أن الجريمة المعلوماتية: هي الفعل غير المشروع الذي يدخل في ارتكابه الحاسب الالي أو هي الفعل الاجرامي الذي يستخدم في ارتكابه الحاسب الالي كأداة رئيسية، أو هي مختلف صور السلوك الاجرامي التي ترتكب باستخدام المعالجة الالية للبيانات.[2]

كما عرف الأستاذ (ROSENBLATT) الجريمة المعلوماتية بأنها " نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو الوصول أو التي تحول عن طريقه.[3]

حسب الدكتورة هدى فشقوش هي: "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"، أو هي "أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبط بتقنية المعلومات."[4]

ويعرفها الفقيهان الفرنسيان (le stint ,vivant) بأنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب[5]"، هذا التعريف مستند على معيار احتمال جدارة

[1]- محمد عبد الله أبو بكر، موسوعة جرائم المعلومات (جرائم الكمبيوتر والانترنت)، المكتب العربي الحديث، الإسكندرية، 2011، ص31.

[2]- طارق إبراهيم الدسوقى عطية، الامن المعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الاسكندرية، مصر، 2009 ،ص153.

[3]- يونس عرب، دليل امن المعلومات و الخصوصية (جرائم الكمبيوتر و الانترنت)، إتحاد المصارف، الجزء الأول، الأردن، 2002، ص213.

[4]- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب و الانترنت، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان، 2011، ص28.

[5]- Vivant et autres: Informatique et droit pénal. Les biens informatiques objets de fraude Lamy informatique.1991.n°3445.p1511.

الفعل بالعقاب وهو معيار غير منضبط ولا يستقيم مع تعريف القانوني، وان كان يصلح هذا التعريف في نطاق علوم الاجتماع وغيرها.

أما بالنسبة للفقه المصري، فهي تنشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال أو الأشياء المعنوية، وهناك فريق أخر يرى أن الجريمة المعلوماتية هي " عمل أو إمتناع يأتيه إضرارا بمكونات الحاسب، وشبكات الإتصال الخاصة به، التي يحميها قانون العقوبات ويفرض له عقابا "، وقد عرفها محمد علي العريان بأنها " كل فعل إيجابي أو سلبي عمدي يهدف إلى الاعتداء على تقنية المعلوماتية أية كان غرض الجاني[1]".

ويرى الأستاذ Rosenblatt بأن الجريمة المعلوماتية "هي نشاط غير مشروع موجه لنسخ و الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه".[2]

إذ يذهب أنصار هذا الاتجاه إلى أن الجرائم التي تفتقر إلى درجة المعرفة بالحاسب الآلي تعد جرائم عادية تتكفل بها النصوص التقليدية للقوانين الجنائية، و يعتبرون لا حاجة لهم في إحداث نصوص جديدة للتعامل مع هذه الأفعال، و ذلك على خلاف الجرائم التي يتوافر لها هذه المعرفة فهي بحاجة إلى نصوص خاصة تتلاءم مع طبيعتها التي تختلف عن غيرها من الجرائم التقليدية[3].

ويدخل في نطاق تعريف الجريمة المعلوماتية الضيقة، تعريف مكتب تقييم التقنية بالولايات المتحدة الأمريكية، حيث يعرف الجريمة المعلوماتية من خلال تحديد مفهوم جريمة الحاسب بأنها: "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا."[4]

و من خلال التعريفات السابقة فقد اعتمد أنصار الاتجاه الضيق في تعريفهم للجريمة المعلوماتية فانه نظروا إلى الوسيلة كأداة لارتكاب جرائمه، ما يؤخذ على التعريفات السابقة أنها جاءت قاصرة عن الإحاطة بأوجه ظاهرة الإجرام الإلكتروني، فالبعض من فقهاء هذا الاتجاه ركز على

---

[1]- محمد علي العريـــان، الجرائم المعلوماتية، دار الجامعة الجديد للنشر، كلية الحقوق جامعة الإسكندرية، الإسكندرية، 2004، ص43.

[2]- حمزة بن عقون، السلوك الإجرامي للمجرم ألمعلوماتي، رسالة ماجستير في العلوم القانونية، تخصص علم الإجرام و العقاب، جامعة باتنة، 2012/2011، ص14، نقلا عن يونس عرب، دليل أمن المعلومات والخصوصية، ص213.

[3]- احمد خليفة الملط، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، مصر، 2006، ص 86.

[4]- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي، مصر، 2006،ص99.

معيار موضوع الجريمة، والبعض الآخر ركز على وسيلة ارتكابها، والبعض الآخر على معيار النتيجة.

ثانيا: التعريف الواسع للجريمة المعلوماتية

إزاء الانتقادات التي وجهت للجريمة المعلوماتية من خلال التعريفات الضيقة، حاول بعض الفقه إعطاء تعريف موسع و ذلك لمحاولة و تفادي أوجه القصور التي شابت تعريفات الاتجاه الضيق في التصدي لظاهرة الإجرام ألمعلوماتي.

ودائما حسب أنصار هذا الاتجاه يرى البعض أن الجريمة المعلوماتية هي كل فعل ضار يستخدم الفاعل الذي يفترض أن لديه معرفة بتقنية الحاسوب نظاما حاسوبيا، أو شبكة حاسوبية، للوصول إلى البيانات، والبرامج بغية نسخها، أو تغييرها، أو حذفها، أو تزويرها، أو تخريبها، أو جعلها غير صالحة، أو حيازتها، أو توزيعها بصورة غير مشروعة[1]، أما البعض من الفقهاء يعرفونها بانها كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية (الحاسوب الآلي الرقمي و شبكة الأنترنت) بطريقة مباشرة أو غير مباشرة، كوسيلة لتنفيذ الفعل الإجرامي المستهدف.[2]

ذهب الفقيهان (Michel و Credo) إلى أن جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على بطاقات الائتمان، وانتهاك ماكينات الحساب الآلي بما تتضمنه من شيكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة الحاسب في حد ذاته وأي من مكوناته[3].

فيعرف فريق من الفقهاء الجريمة المعلوماتية بأنها: "كل سلوك إجرامي يتم بمساعدة الحاسب الآلي" أو هي: "كل جريمة تتم في محيط الحاسبات الآلية[4]".

---

[1]- كامل فريد السالك، الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية، حلب، 2000، بدون صفحة.

[2]- صغير يوسف، الجريمة المرتكبة عبر الأنترنت، رسالة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2013 ،ص09 ،نقلا عن كحلوش علي، جرائم الحاسوب وأساليب مواجهتها مجلة صادرة عن مديرية الأمن الوطني، العدد84 ،2007 ،ص 51.

[3]- طرشي نورة، مكافحة الجريمة المعلوماتية، رسالة الماجستير في القانون الجنائي، جامعة الجزائر1 ،كلية الحقوق، 2012،2011 ،ص6.

[4] -Roden (adrian), computer crime and the law, C.L.J ..,1991,vol.15,p.399.

وذهب رأى أخر من الفقه إلى تعريف الجريمة المعلوماتية بأنها:"عمل أو امتناع يأتيه الإنسان ، إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقاب."

ويرى جانب من الفقه من أنصار هذا الاتجاه الموسع بأنها:"كل سلوك اجرامى يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر."

ويعرفها Tièdement بأنها :"كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب"، من خلال هذه التعريفات يتبين لنا أن هذا الاتجاه يوسع من مفهوم الجريمة المعلوماتية، حيث أن مجرد مشاركة الحاسب الآلي في السلوك الإجرامي يضفي عليه وصف الجريمة المعلوماتية.[1]

ويعرفها:"(Tompson David) جريمة يكون متطلبا لاقترافها أن يتوفر لدى فاعلها معرفة تقنية الحاسب.[2]

كما تبنى الخبير الأمريكي Parker مفهوما واسعا للجريمة المعلوماتية و أشار على أنه:" هي كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية تنشا عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل".[3]

و إن إعطاء هذا التعريف الواسع للجريمة المعلوماتية يدخل في نطاقها كل التصرفات الغير المشروعة التي لها علاقة بالحاسوب أيا كانت هذه العلاقة و أيا كان دور الحاسوب فيها سواء كان وسيلة أو مناسبة لارتكاب التصرفات غير المشروعة أو كان موضوعا لها.

من خلال هذه التعريفات يتبين لنا أن هذا الاتجاه يوسع من مفهوم الجريمة المعلوماتية، حيث أن مجرد مشاركة الحاسب الآلي في السلوك الإجرامي يضفي عليه وصف الجريمة المعلوماتية.[4]

[1]- نائلة عادل محمد فريد قورة ، المرجع السابق ، ص30

[2]- عرب يونس، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي،2002،ص4.

[3]- نهلا عبد القادر المومني ، الجرائم المعلوماتية ، ط1 ، دار الثقافة للنشر و التوزيع ، عمان ، 2008 ، ص49.

[4]- نائلة عادل محمد فريد قورة، المرجع السابق، ص 30.

ويلاحظ من خلال التعريفات السابقة أنها قد أغلقت جانبا على قدر كبير من الأهمية في تعريف الجريمة المعلوماتية ألا وهو الدور الكبير الذي يقوم به الحاسب الآلي في هذه الجريمة، فإن كان من المتفق عليه أن الجريمة المعلوماتية قد تتخذ أحد المظهرين، يتمثل الأول في استخدام الحاسب الآلي كوسيلة لارتكاب الجريمة، والثاني في الاعتداء على الحاسب الآلي ذاته، ولهذا فإنه يثور أمامنا التساؤل الآتي، هل تعد الجريمة المعلوماتية في كل الحالات التي يستخدم فيها نظام الحاسب الآلي من أجل ارتكاب الجريمة، وفي كل الحالات التي يقع فيها اعتداء على الحاسب الآلي ونظامه، لاشك أن الإجابة على ها التساؤل تكون بالنفي.[1]

الفرع الثالث: تطـور الجـريمة المعلوماتية

لقد ظهرت جرائم الإنترنت في حقل جرائم التقنية العالية في نهاية الثمانينات، وكان ذلك من خلال العدوان الفيروس وبالأخص جريمة دودة موريس المؤرخة واقعتها في نوفمبر 1988، ولقد أطلق مصطلح جرائم الإنترنت في مؤتمر المنعقد في أستراليا في الفترة من 16-1998/2/17، وتجدر الإشارة إلى أن الكثير من الباحثين يستخدمون مصطلحات غير دقيقة للتعبير عن جرائم الإنترنت. إذ نجد البعض يستخدم مصطلح " الإجرام المعلوماتي يستخدم مصطلح "جرائم التكنولوجيا المتقدمة أو مصطلح " الغش المعلوماتي".[2]

في حين أنه يجب استخدام المصطلح الدقيق والمتماشي مع طبيعة تلك الجرائم وهو "جرائم الإنترنت"، ذلك لأن "الإجرام المعلوماتي" وإن كان يقصد التعبير عن الجرائم الواقعة عن طريق جهاز الكمبيوتر، إلا أن هذا لا يعني من جهة أخرى أن الإعتداء على المعلومة يتحقق دائما بإستخدام الكمبيوتر وخصوصا بإستخدام الإنترنت ، لذلك لأن الوسائل التقليدية هي دائما ما تكون أداة لإرتكاب تلك الجريمة، وبالتالي فالجريمة المعلوماتية قد تكون أشمل من جرائم الإنترنت وذات الشأن بالنسبة ص للغش المعلوماتي وكذا "جرائم التكنولوجيا المتقدمة"[3].

ولقد لاحظ مؤتمر القانون والإنترنت المنعقد في لشبونة/ البرتغال في 2001/01/26 أنه يجب عدم الالتفات إلى مثل هذه المصطلحات غير الدقيقة، وإعتماد مصطلح (crim cyber) دون غيره

[1]- مرجع نفسه، ص30.
[2]- نبيلة هبة هروال ، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع إستدلالات (دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية، 2013 ،ص 31.
[3]- مرجع نفسه، ص31.

للتعبير عن جرائم الأنترنت ، مع الأخذ في الإعتبار التمييز بين تلك الجرائم التي يمكن إرتكابها عبر الإنترنت[1]، مرت جرائم الأنترنت بتطور تاريخي تبعا لتطور التقنية واستخدامها، ولهذا مرت بثلاث مراحل هي.

المرحلة الأولى: من شيوع إستخدام الحواسيب من السيتينات إلى السبعينات من القرن الماضي إقتضت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر، وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم شيء عابر أم ظاهرة إجرامية مستحدثة، وإن الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة، وإن الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة ، ومع تزايد إستخدام الحواسيب الشخصية في السبعينات ظهرت عدد من الدراسات المسحية والقانونية التي إهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لامجرد سلوكيات مرفوضة.

المرحلة الثانية: في الثمانينات حيث طفا على السطح مفهوم جديد لجرائم الكمبيوتر والأنترنت وإرتبطت بعمليات إقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدميرية للملفات أو البرامج.

شاع إصطلاح "الهاكرز" المعبر عن مقتحمي النظم، لكن الحديث عن الدوافع لإرتكاب هذه الأفعال ظل محظورا في رغبة المحترفين تجاوز أمن المعلومات وإظهار تفوقهم التقني، ولكن هؤلاء المقامرون أصبحوا أداة إجرام، وظهور المجرم المعلوماتي المتفوق المدفوع بأغراض إجرامية خطيرة القدرة على إرتكاب أفعال تستهدف الإستلاء على المال أو التجسس أو الاستيلاء على البيانات السرية والإقتصادية والإجتماعية والسياسية والعسكرية.

المرحلة الثالثة : شهدت التسعينات تناميا هائلا في حقل الجرائم الإلكترونية وتغيير في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الأنترنت من تسهيل لعمليات دخول الأنظمة وإقتحام شبكة المعلومات ظهرت أنماط تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعملة المعتاد وأكثر ماموريست ضد مواقع الأنترنت التسويقية الهامة التي يتسبب إنقطاعها عن الخدمة ساعات في خسائر

[1]- عمر محمد أبو بكر بن يونس ، الجرائم الناشئة عن إستخدام الأنترنت، دار النهظة العربية ، 2004 ، ص158.

مالية بالملايين ، ونشطت جرائم نشر الفيروسات عبر المواقع الإلكترونية لما تسهله من إنتقالها إلى ملايين المستخدمين في ذات الوقت وظهرت الرسائل المنشورة على الأنترنت أو المراسلة بالبريد الإلكتروني المنطوية على الأحقاد أو المساس بكرامة وإعتبار الأشخاص أو المروجة لمواد غير القانونية أو غير المشروعة.[1]

المطلب الثاني: خصائص ودوافع الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية ذلك نتيجة ارتباطها بتقنية المعلومات والحاسب الآلي، توجد دوافع عديد تحرك المجرم ألمعلوماتي لارتكاب أفعال الاعتداء المختلفة المنطوية تحت مفهوم الجزاء ألمعلوماتي.

الفرع الأول: خصائص الجريمة المعلوماتية

نظرا للطبيعة المميزة للجريمة الإلكترونية باعتبارها تمس المعلومات هذا ما جعلها تتميز عن نظيرتها التقليدية بمجموعة من الخصائص أو السمات، إذ أن التعرف أكثر على خصائص هذه الجريمة يساعد في إيجاد الحلول لمكافحتها، من خلال هذا الفرع سوف نوضح أهم خصائص الجريمة المعلوماتية.

أولا: الجرائم المعلوماتية ترتكب بواسطة الانترنت

يعد الحاسب الآلي أداة لجريمة لأنه يمكن الشخص من الدخول على شبكة الإنترنت وقيامه بتنفيذ جريمته أي كان نوعها، بمعنى آخر أن الحاسب الآلي هو الأداة الوحيد لارتكابها أي جريمة من الجرائم التي ترتكب على شبكة الإنترنت.[2]

ثانيا: الجريمة المعلوماتية عابرة للحدود الوطنية

الجريمة المعلوماتية تتسم بالطابع الدولي، لان نظام الانترنت جعل من معظم دول العالم في حالة اتصال دائم على الخط، فالجرائم المعلوماتية لا تعترف بالحدود بين الدول وبالتالي فهي شكلا

[1]- عبد الفتاح مراد ، دور الكمبيوتر في مجال إرتكاب الجرائم الإلكترونية شرح جرائم الكمبيوتر والأنترنت، دار الكتب والوثائق المصرية، مصر، د.س.ن، ص43.

[2]- فتحية رصاع ، الحماية الجنائية للمعلومات على شبكة الإنترنت ، رسالة ماجستير في القانون العام ، كلية الحقوق والعلوم السياسية ، جامعة أبي بكر بلقايد ، تلمسان ، 2001/ 2012 ، ص42.

جديداً من أشكال الجرائم العابرة للحدود بين الدول، وهذا النوع من الجرائم لا يعترف بالحدود فقد تمتد إلى خارج حدود مرتكبيها في دولة أخرى و هنا تثور مشاكل الاختصاص والإجراءات والتحري وغير ذلك من نقاط التي تثيرها الجرائم العابرة للحدود.[1]

و لعل القدرة التي تتمتع بها الحاسبات الآلية في نقل و تبادل كميات معتبرة من المعلومات قد ترتكب جرائم في دولة ما، و يتحقق الفعل الإجرامي في دولة أخرى فهي تتميز بالتباعد الجغرافي بين الفاعل و المجني عليه.[2]

بهذه الخاصية التي تتميز بها الجريمة الإلكترونية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب التطبيق، بالإضافة إلى إشكالية تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.

ونتيجة لهذه الطبيعة الخاصة للجريمة المعلوماتية وبالنظر للخطورة التي تشكلها على المستوى الدولي، والخسائر التي قد تتسبب بها، تعالت الأصوات التي تدعو إلى التعاون الدولي من أجل التصدي لهذه الجرائم، ويتمثل التعاون الدولي في المعاهدات والاتفاقيات الدولية التي تعمل على توفير جو من التنسيق بين الدول الأعضاء وهو الأمر الذي يكفل الإيقاع بمجرمي المعلوماتية وتقديمهم للقضاء.[3]

ثالثا: صعوبة اكتشاف الجريمة المعلوماتية وإثباتها

نظرا لطبيعة الخاصة التي تتميز بها الجريمة المعلوماتية فإن إثباتها يحيط به الكثير من الصعوبات، والتي تتمثل في صعوبة اكتشاف هذه الجرائم، لأنها لا تترك أثرا خارجيا ، فالجريمة الإلكترونية لا عنف فيها ولا أثر اقتحام لسرقة مثال، وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسوب وليس لها أي أثر خارجي مرئي، وبمعنى آخر فإن الجريمة الإلكترونية هي جرائم فنية، وهي جرائم هادئة لا تتطلب العنف، ورغم ذلك فان البعض يشبه هذه

[1]- عبد الله عبد الكريم عبد الله ، جرائم المعلوماتية والانترنت الجرائم الالكترونية، منشورات الحلبي الحقوقية، طبعة 1، بيروت ، 2007 ، ص33.
[2]-جعفر حسن جاسم الطائي ، جرائم تكنولوجيا المعلومات ، دار البلدية ، عمان ، 2010 ، ص141.
[3]- نهلا عبد القادر المومني، المرجع السابق، ص51-52.

الجرائم بجرائم العنف مثل ما ذهب إليه مكتب التحقيقات الفدرالي بالواليات المتحدة الأمريكية نظرا لتماثل دوافع المتعدين على نظم الحاسوب الآلي مع مرتكبي العنف.[1]

إن سرعة التنفيذ أهم ما يميز الجريمة المعلوماتية، الذي يتم مباشرة من قبل الجاني، أو من خلال برامج خاصة بذلك، هو ما يساعد الجاني على تنفيذ جريمته بسرعة فائقة بعيدا عن مسرح الحادث، و بطريقة خفية مستترة لا يلاحظها المجني عليه ، إضافة إلى صعوبة اكتشافها، فالجرائم المعلوماتية لا يتم كشفها أو الإحساس بها إلا بعد مدة طويلة.[2]

وما يزيد الأمر صعوبة هو ضعف خبرت الشرطة ومعرفتهم الفنية بالأمور المتعلقة بالحاسب الآلي سواء تتمثل في الضعف في تحديد الدليل المعتبر، أم في انتشال ذلك الدليل والمحافظة عليه وكلها عوامل تجعل من إثبات الجرائم المعلوماتية أمر في غاية الصعوبة.[3]

رابعا: الجريمة المعلوماتية جريمة ناعمة

تتميز الجرائم المعلوماتية بأنها جرائم ناعمة، لا يتطلب منها أي نوع من المجهودات العضلية، مثل الجرائم التقليدية كالسرقة والاغتصاب والقتل، بل أنها تحتاج إلى القدرة الذهنية والعقلية للجاني، وإلمامه الجيد بتقنيات الحاسوب بحيث تمكنه هذه الميزات من ارتكاب الجريمة وخلال لحظات دون أن يترك أثرا.[4]

فالمجرم ألمعلوماتي يتعامل مع جهاز الحاسوب بمستوى تقني يوظف في أفعال غير مشروعة، كما قد يحتاج إلى وجود شبكة المعلومات الدولية، إضافة إلى الإرادة في تحقيق الغرض الإجرامي وكل هذا دون عنف.[5]

تعد الجريمة المعلوماتية أقل عنف من الجرائم التقليدية، إذ تمتاز الجريمة المعلوماتية بأنها من الجرائم الناعمة وبعيده عن العنف، فلا تتطلب لإرتكابها العنف ولا استعمال الأدوات الخطيرة

[1]- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2004، ص53.
[2]- عبد الله بن حسين آل حجراف القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية، رسالة ماجستير في قسم العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض، ص33-34.
[3]- نهلا عبد القادر المومني، المرجع السابق، ص51.
[4]- أسامة احمد المناعسة، جرائم الحاسوب الآلي، دار وائل لنشر والتوزيع، عمان، 2001، ص107.
[5]- حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه في علوم الحقوق، كلية الحقوق والعلوم السياسية ، جامعة باتنة، 2016، ص 30.

كالأسلحة وغيرها، فنقل بيانات ممنوعة أو التلاعب بأرصدة البنوك مثلا لا تحتاج الا الى لمسات ازرار، بل وتعتمد على الدراسة الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسب الآلي.[1]

الفرع الثاني: دوافع ارتكاب الجريمة المعلوماتية

لا يخفى على احد أن المجرم يرتكب جريمته نتيجة دوافع معينة، تختلف هذه الدوافع من مجرم لأخر كما قد تكون مشتركة بينهم، والأمر نفسه بالنسبة للمجرم ألمعلوماتي الذي يرتكب جريمة معلوماتية يكون الدافع فيها يختلف عن دافع مجرم معلوماتي أخر وقد تكون مشتركة بينهم، ومن بين أهم هذه الدوافع.

أولا: الدوافع المادية لارتكاب الجريمة المعلوماتية

يعتبر السعي إلى تحقيق الكسب المالي في الحقيقة غاية الفاعل، وهو من بين أكثر الدوافع تحريكا للجناة لاقتراف الجرائم المعلوماتية، ذلك أن خصائص هذه الجرائم ، وحجم الربح الكبير الممكن تحقيقه من بعضها خاصة غش الحاسوب أو الاحتيال المرتبط بالحاسوب الذي يتيح تعزيز هذا الدافع بما تحققه من ثراء فاحش، والدليل على ذلك ما حدث في فرنسا سنة 1986 حيث كان العائد من ارتكاب جناية سرقة مع حمل سلاح هو 70000فرنك فرنسي في حين أن جريمة الغش في مجال المعالجة الآلية للمعلومات حصل منها الجاني على 670.000 فرنك فرنسي أي ما يعادل أكثر من 38 مرة.[2]

فإن الطمع وحب الثراء السريع يدفع الفرد للقرصنة أو السرقة أو الاختلاس عن طريق الحاسوب للحصول على مال لتلبية حاجاته الأساسية والرغبة في الثراء السريع غير المكلف بالإضافة إلى تحقيق أغراض معنوية مقصود وذلك عن طريق عملية الجوسسة والاختراق المواقع، نتيجة تنوع

[1]- احمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، مصر، 2007، ص36.

[2] -se philippe. la criminalité informatique que sais. je 1er édition. PU 1988. P 490.Dr.

أصناف الأشخاص مرتكبي الإجرام ألمعلوماتي، أخذوا يشكلون خطرا على أنظمة الحاسب بما يشمله من المعلومات ، وكذلك على الحياة الخاصة للأفراد وأموالهم.[1]

وهناك فئة من مرتكبي الجرائم المعلوماتية يرجع ارتكابهم لها إلى الديون الناتجة من المشاكل العائلية والخسائر الضخمة من ألعاب القمار أو إدمان المخدرات، فقد تكون جميع، الوسائل بالنسبة للبعض مشروعة في هذه الحالات، فالغاية تبرر الوسيلة.[2]

ثانيا: دافع الانتقام لارتكاب الجريمة المعلوماتية

وهو من أخطر الدوافع التي تدفع إلى ارتكاب الجريمة لأنه يصدر من شخص يملك معلومات كثير عن المؤسسة التي يعمل بها، نتيجة لفصله من العمل أو تخطيه في الحوافز وتظهر خطورة الانتقام عند قيام أحد هؤلاء الموظفين بالاستعداد مسبقا لمثل هذا الموقف، حيث يقوم بزرع برنامج يحمل تعليمات بمسح كافة البيانات ويقوم الانتقام من هذه المؤسسة عن طريق تشغيل هذا البرنامج.[3]

وسوف نجد في معرض تناولنا للجريمة المعلوماتية أن دافع الانتقام من رب العمل هو المحرك الرئيسي الذي يدفع بالموظفين المستخدمين في الشركات والمؤسسات لارتكاب جرائمهم عبر الإنترنيت ضد تلك المؤسسات التي قامت بتوظيفهم، وربما تمثل أنشطة زرع الفيروسات في نظم الكمبيوتر النشاط الرئيسي والغالب لهذه الفئة من الموظفين[4]، ومن الوقائع التي تؤكد ذلك ما حدث في الولايات المتحدة الأمريكية، إذ قام أحد موظفي بإدخال فيروس لشركة التي كان يعمل سجِّلا انتقاما من تلك الشركة لأنها قامة فيها مما أدى إلى ضياع 160 من سجلات العملاء وذلك بفصله من العمل.[5]

---

[1]- نجا بن مكي، السياسة الجنائية لمكافحة الجرائم المعلوماتية، رسالة ماجستير في القانون الدولي، معهد العلوم القانونية والإدارية، قطب خنشلة، 2009/2008، ص35.

[2]- لعاقل فريال، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة ماستر في القانون العام، جامعة أكلي محند اولحاج – البويرة، 2015/2014، ص25.

[3]- أيمن عبد الحفيظ، الاتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية، ط 1، دار النهضة العربية للطبع والنشر والتوزيع، د.ب.ن، 2005، ص19.

[4]- أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية لمكافحة جرائم الكمبيوتر والانترنيت، مكتبة الوفاء القانونية، مصر، 2011، ص129.

[5]- المرجع نفسه، ص129.

ثالثا: الدوافع الذهنية لارتكاب الجريمة المعلوماتية

تتمثل هذه الدوافع في المتعة والتحدي والرغبة في فهم النظام ألمعلوماتي و إثبات الذات، وقد تكون هذه الدوافع مجرد شغف بالإلكترونيات والرغبة في تحدي وقهر النظام والتفوق على تعقيد وسائل التقنية، فاختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبيها وتسلية تغطي أوقات فراغه، وعلى صعيد آخر قد يكون إقدام المجرم الإلكتروني على ارتكاب جريمته بدافع الرغبة في قهر الأنظمة الإلكترونية والتغلب عليها، إذ يميل المجرم هنا إلى إظهار تفوقه على وسائل التكنولوجيا الحديثة، وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية، وإنما ينطلق من دافع التحدي و إثبات المقدرة. [1]

رابعا: دافع الفقر لارتكاب الجريمة المعلوماتية

الفقر من أهم الدوافع المباشرة لارتكاب الجرائم، وهذا راجع لسوء الأوضاع الاقتصادية، ومنها البطالة والكساد والرعاية الاجتماعية الضرورية، مما أدى إلى تزايد معدات الجريمة المعلوماتية بين المجرمين الذين ينتمون إلى الطبقات الفقيرة.

خامسا: الدوافع السياسية لارتكاب الجريمة المعلوماتية

هي من أهم المحفزات لارتكاب الجرائم المعلوماتية، وترتكب عن طريق شبكة الإنترنت بشكل شبه دائم لاختراق مواقع حكومية أو تعطيلها، وقد أصبحت الجريمة المعلوماتية بمثابة السلاح تستعمل بين الدول وكان المؤلف "مهن الذكاء الاقتصادي" استشرف نوع جديد من الهيمنة بعد انهيار الاتحاد السوفيتي، أضاف أن التحكم في تكنولوجيا المعلومات هو السلاح الحديث الذي يعوض السلاح التقليدي.[2]

ومن بين هذه الاختراقات ما قامت به مجموعة "كرداب" (gerdab) المتخصصة في الأمن ألمعلوماتي، عن طريق فريقا من المخترقين تسلل إلى خوادم شركة "آلتا"(elta) التابعة لصناعات

[1]- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير في العلوم القانونية، جامعة الحاج لخضر، باتنة، 2012-2013، ص61-62.

[2]- عبد اللطيف معتوق، إطار القانوني لمكافحة الجرائم المعلومات في التشريع الجزائري، رسالة ماجستير في العلوم القانونية، جامعة العقيد لخضر، باتنة، 2011-2012، ص13.

الجوية للكيان الصهيوني، وجاء ذلك لاختراق نتيجة اغتيال العالم الإيراني محسن فخري ومساعدة الكيان الصهيوني للجانب الأمريكي في اغتياله الجنرال الإيراني قاسم سليماني.[1]

سادسا: دافع التهديد لارتكاب الجريمة المعلوماتية

ينتشر هذا الدافع نتيجة الوقوع تحت تهديد وضغط من الغير في مجالات الأعمال التجارية والخاصة بالتجسس والمنافسة[2]، ونذكر في هذا الخصوص موظف يعمل بإحدى مكاتب شركة مشهورة متعددة الجنسيات والتي مركزها مدينة "Sindelfingen"بألمانيا الغربية –سابقا– حيث كان يتمتع هذا الموظف بسمعة طيبة لدى كل المنشآت العمالية، وقد لوحظ عقب اختفائه أن هذا الموظف المثالي كان يعمل في الحقيقة مع مجموعة جواسيس أنشأت خصيصا من أجل مهاجمة أنظمتها المعلوماتية، ولقد نجح الجاسوس في أن ينقل إلى ألمانيا الشرقية معلومات هامة حول منشأة تعمل في ألمانيا الغربية ولكن يجب الاعتراف أن الجاسوس كان ضحية ابتزاز وتهديد.[3]

[1] -https://www.aljazeera.net/news/politics/2020/12/23

[2]- أحمد خليفة الملط، الرجع السابق، ص90.

[3]- محمد سامي الشوا، المرجع السابق، ص53.

المبحث الثاني: تصنيف الجرائم المعلوماتية وتحديد مرتكبيها

سنحاول من خلال هذا المبحث تحديد أصناف الجرائم المعلوماتية في المطلب الأول، وبيان مرتكبو الجريمة المعلوماتية في المطلب الثاني.

المطلب الأول: تصنيف الجريمة المعلوماتية

جاء في إطار تصنيف الجريمة المعلوماتية عدة تقسيمات منها ما هو في إطار التشريع بما تسمى بالتصنيفات التشريعية، و لعل من أبرزها الاتفاقية الأوروبية المعروفة " بودابست" ، كما جاء أيضا في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، و سنسلط الضوء أيضا على مختلف التصنيفات التي جاء بها الفقه.

الفرع الأول: التصنيف التشريعي للجرائم المعلوماتية

يعالج التصنيف التشريعي الجريمة المعلوماتية بإتاحة معيار منهجي وإحصائي، إذ تصنف فيه الأفعال الإجرامية المعلوماتية بطريقة مفيدة ومنهجية، تؤدي إلى تحسين القدرة على إعداد بيانات عن الجريمة المعلوماتية ونشرها وتحليلها بدقَّة من أجل إعلام الجمهور وتكييف السياسات العامة والبرامج في مجالات منع ومكافحة الجريمة المعلوماتية.

أولا: تصنيف الجريمة المعلوماتية وفقا لاتفاقية (بودابست) في 2001

يتبين من خلال الجوانب الموضوعية للجرائم المعلوماتية، فقد جاءت في الاتفاقية من خلال نصوص المواد من المادة 2 إلى المادة 13، إذ صنفت الجرائم المعلوماتية ضمن الطوائف التالية:[1]

الطائفة الأولى: الجرائم ضد سرية و سلامة و إتاحة البيانات و النظم المعلوماتية المواد من(02 إلى 06) من الاتفاقية و تندرج ضمن هذه الطائفة الجرائم التالية:

-الولوج الغير قانوني (المادة 02)

-الاعتراض الغير قانوني (المادة 03)

[1]-انظر للمادة (2-13)، من اتفاقية بودابست الدولية حول الجرائم الالكترونية.

- الاعتداء على سلامة البيانات (المادة 04)

- الاعتداء على سلامة النظام (المادة 05)

- إساءة استخدام أجهزة الحاسب (المادة 06)[1]

الطائفة الثانية: الجرائم المعلوماتية (الجرائم المتصلة بالحاسب):

وجاء ضمن هذه الطائفة حسب نص المادتين 07 و المادة 08 من هذه الاتفاقية الجرائم الآتية :

- التزوير ألمعلوماتي حسب نص المادة 07 من الاتفاقية.

- الغش ألمعلوماتي حسب نص المادة 08 من الاتفاقية.

الطائفة الثالثة: الجرائم المتصلة بالمحتوى.

جاء في هذه الطائفة حسب نص المادة 09 من الاتفاقية على صنف واحد من الجرائم و هي الجرائم المتصلة بالمواد الإباحية للأطفال.

الطائفة الرابعة: الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية و الحقوق المجاورة .

جاء في نص المادة 10 من اتفاقية " بودابست " نصت على نوعية هذه الجرائم وذلك لأنها تقوم على الانتهاكات الواقعة على الملكية الفكرية هي احد أشكال الإجرام ألمعلوماتي ، الأكثر شيوعا ، والذي بازدياد نسبته يزداد قلق و انشغال العالم بأسره.[2]

ثانيا: تصنيف الجريمة المعلوماتية وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات

تضمنت الاتفاقية العربية الصادرة في 2010، خلال الفصل الثاني تحت عنوان التجريم كما جاء في الاتفاقية تنظيم نصوص تجريم، حيث أنها لم تصنف للجريمة المعلوماتية بل اكتفت بتنظيمها، إذ ذكرت مجموعة من الجرائم هي كالأتي.

[1]- هلالي عبد الله احمد، اتفاقية بودابست لمكافحة الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2007، ص47.
[2]- المرجع نفسه، ص91،ص127.

- جريمة الدخول غير المشروع (المادة 06) .
- جريمة الاعتراض غير المشروع (المادة 07) .
- جريمة الاعتداء على سلامة البيانات (المادة 08) .
- جريمة إساءة استخدام وسائل تقنية المعلومات (المادة 09).
- جريمة التزوير.
- جريمة الاحتيال.
- الجرائم الإباحية.
- الجرائم الأخرى المرتبطة بالإباحية.
- جريمة الاعتداء على حرمة الحياة الخاصة.[1]

كما نظمت طائفة تتضمن مجموعة من الجرائم وهي كتالي:

- الجرائم المتعلقة بالإرهاب و المرتكبة بواسطة تقنية المعلومات .

و نظمت أيضا حسب المادتين (16-17) من الاتفاقية :

- الجرائم المتعلقة بالجرائم المنظمة و المرتكبة بواسطة تقنية المعلومات (المادة 16)
- الجرائم المتعلقة بانتهاك حق المؤلف و الحقوق المجاورة (المادة 17)

و في الأخير لتنظيمها للجرائم تضمنت أيضا على:

- الاستخدام غير المشروع لأدوات الدفع المعلوماتية.
- الشروع و الاشتراك في ارتكاب الجرائم المعلوماتية.[2]

[1]- انظر للمواد(6-9)، من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.
[2]- انظر للمواد(16-17)، من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

نستنتج من خلال الاتفاقية العربية بأنها حاولت أن تغطي كل أساليب الإجرام المتعلقة بتقنية المعلومات حتى لا تجعل الدول العربية في حيرة من خلال تطرقها لمثل هذه الصور من الجرائم إذ شملت كل الأصناف الماسة بالمعلوماتية.

الفرع الثاني: التصنيف الفقهي للجرائم المعلوماتية

تعددت محاولات الفقه حول تحديد أصناف الجرائم المعلوماتية، و ذلك لصعوبة حصر هذه الأنواع بصفة دقيقة بالنظر لحادثة ظهور هذه الجريمة و بذلك أيضا لعدم وجود تعريف عام متفق عليه للجريمة المعلوماتية.

قسمنا هذا الفرع إلى تصنيف الجريمة المعلوماتية بحسب النظام كوسيلة أو محل و تصنيف الجرائم المعلوماتية بحسب جرائم الكمبيوتر و الانترنيت.

أولا: تصنيف الجرائم المعلوماتية بحسب ما إذا كان النظام وسيلة أو محل

هذا التصنيف هو الذي ترافق مع موجات التشريع في ميدان قانون تقنية المعلومات، وهو التصنيف الذي يعكس أيضا التطور التاريخي لظاهرة الجرائم المعلوماتية، ونجده التصنيف السائد في مختلف مؤلفات الفقيه الريش سيبر والمؤلفات المتأثرة به ولهذا نجد أن جرائم المعلوماتية بالاستناد إلى هذا المعيار يمكن تقسيمها ضمن الطوائف التالية.[1]

1- الجرائم المعلوماتية الواقعة على الأشخاص

تقع هذه الجرائم على الأشخاص و تنقسم بدورها إلى طائفتين بحسب نوع الحقوق المعتدى عليها و دور النظام ألمعلوماتي في اقترافه و تتمثل الطائفة الأولى في الجرائم الواقعة على حقوق الملكية الفكرية و الأدبية و تتمثل الطائفة الثانية تكمن في الجرائم الواقعة على حرمة الحياة الخاصة و سنقوم ببيانها كالأتي:[2]

[1]- خالد داودي، الجريمة المعلوماتية، دار الإعصار العلمي للنشر وتوزيع ،الطبعة الأولى، عمان، 2017، ص44.
[2]- أسامة احمد المناعسة و جلال محمد الزعبي، جرائم تقنية نظم المعلومات الالكترونية، ط2، دار الثقافة للنشر وتوزيع، عمان، 2014، ص99.

أ- طائفة الجرائم المعلوماتية الواقعة على حقوق الملكية الفكرية و الأدبية

يمكن أن يكون النظام ألمعلوماتي وسيلة فعالة للاعتداء على حقوق الملكية الفكرية و الأدبية و مثال ذلك استخدام النظام ألمعلوماتي في السطو على بنوك المعلومات التي تتضمنها برامج نظام معلوماتي أخرى أو حالة تخزين و استخدام هذه المعلومات أو التفريط فيها دون إذن من صاحبها، و ذلك لان استخدام معلومة معينة دون إذن من صاحبها يتضمن اعتداء على حق من الحقوق المعنوية إضافة إلى كونه اعتداء على قيمتها المالية كون أن المعلومة لما لها من قيمة أدبية إضافة إلى قيمتها المادية، كما يندرج أيضا ضمن الحقوق الفكرية كذلك براءات الاختراع باعتبارها تمثل فكرة للمخترع تحتوي على حق معنوي و آخر مالي للمخترع.[1]

ب- طائفة الجرائم المعلوماتية الواقعة على الحياة الخاصة

إن الأهمية التي تحتويها أنظمة الحسابات الآلية أصبح لهذه الحسابات دورا هاما في تسهيل الحصول على هذه المعلومات عن طريق الغير بإنشائها لتحقيق مصالح مختلفة.[2]

و عليه يمكن أن يستخدم النظام ألمعلوماتي في الاعتداء على حرمة الحياة الخاصة أو على الحريات العامة للفرد، كأن يقوم شخص يعمل بالنظام ألمعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص آخر بدون علمه أو إذنه، أو أن يجمع المعلومات بعلم الشخص المعني و لكن يقوم المكلف بحفظها بإطلاع الغير عليها بدون إذن صاحبها، أو أن يقوم شخص باختراق معلومات تتمثل في أسرار مكتوبة و سير ذاتية و مذكرات حياة شخصية لشخص آخر.[3]

2- الجرائم الواقعة على النظم المعلوماتية الأخرى

عليه يمكن أن يستخدم النظام ألمعلوماتي في الاعتداء على حرمة الحياة الخاصة أو على الحريات العامة للفرد، كان يقوم شخص يعمل بالنظام ألمعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص آخر بدون علمه أو إذنه، وان يجمع المعلومات بعلم الشخص المعني ولكن يقوم

[1]- احمد خليفة الملط، المرجع السابق، ص184.
[2]- نائلة عادل محمد فريد قورة، المرجع السابق، ص275.
[3]- أحمد خليفة الملط، المرجع السابق، ص187.

المكلف بحفظها باطلاع الغير عليها بدون إذن صاحبها، وان يقوم شخص آخر باختراق معلومات تتمثل في أسرار مكتوبة و سير ذاتية و كذا مذكرات حياة شخصية لشخص آخر.[1]

هذا النوع من الجرائم لا يستلزم تدخلا لإتلاف الوظائف الطبيعية للنظام ألمعلوماتي و لا تعديلا على المعلومات المعالجة، بل يقتصر في غالب الأحيان على الولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية، أو استخدام أداة إلكترونية معينة تسمح بالتقاط المعلومات و التصنت عليها لدى النظم المعلوماتية الأخرى بالإضافة إلى إساءة استخدام البطاقات الائتمانية و سوف نبين هاتين الصورتين كالآتي:

أ- الولوج غير المشروع للمعلومات المعالجة آليا

تقوم هذه الصورة بوجود المجرم ألمعلوماتي داخل أحد المراكز المعلوماتية بهدف يكون هذا الولوج إما مباشرا أو غير مباشر.

الولوج إلى المعلومات التي تمت معالجتها آليا و الإطلاع عليها من دون تصريح و قد فأما الولوج المباشر فيعد من أكثر الأفعال المرتكبة و أسهلها تنفيذا و يتخذ عدة صور إذ يستطيع الجاني الاستيلاء على المعلومات المخزنة لدى الأنظمة المعلوماتية بعدة طرق باستخدام آلة الطباعة أو استخدام شاشة النظام أو الإطلاع على المعلومة بالقراءة على ما هو مكتوب عليها أو استخدام مكبر الصوت.[2]

و من أمثلة الولوج المباشر قيام موظف سابق بأحد البنوك الفدرالية الأمريكية الذي كان يعمل في النظام ألمعلوماتي الخاص بالبنك نقل المعلومات المالية المخزنة في النظام لرئيسه الجديد بعد حصوله على كلمة السر من زميل سابق له.[3]

و أما الولوج غير المباشر ظهر بظهور تقنيات مستحدثة، لها صلة بالنظام ألمعلوماتي كالمعالجة عن بعد إذ أن هذه التقنيات أدت إلى نشوء مخاطر جديدة نتيجة للإمكانيات المستحدثة

---

[1]- المرجع نفسه، ص187.

[2]- أحمد خليفة الملط، المرجع السابق، ص190.

2- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، القاهرة، دار النهضة العربية، 1994، ص67.

3- أحمد خليفة الملط، المرجع السابق، ص192.

للولوج و الاستفسار عن بعد من المراكز المعلوماتية، إذ أنه أثناء حركتها و بثها تكون مهددة للالتقاط و التسجيل غير المشروعين في كل لحظة كتوصيل خطوط تحويلية لالتقاط المعلومات المتواجدة ما بين النظام ألمعلوماتي و النهاية الطرفية و إرسال المعلومات المختلسة إلى النهاية الطرفية عن طريق إشارات إلكترونية أو الولوج غير المشروع عن طريق نهاية طرفية بعيدة عن طريق نظام معلوماتي و معرفة كلمة السر أو مفتاح الشفرة المناسب.[1]

ب- إساءة استخدام البطاقات الائتمانية

أدى إدخال النظام ألمعلوماتي في مجالات عمليات البنوك إلى ظهور هذا النوع الجديد من الجرائم المعلوماتية و تعد من أخطر الجرائم المعلوماتية لاسيما في المجتمعات التي تتسم نظمها صورتين. البنكية بدرجة عالية من التطور و الحداثة، و يتخذ هذا النوع من الجرائم المعلوماتية صورتين، تتمثل الأولى في إساءة استخدام العميل البطاقات الائتمانية و ذلك عن طريق عدم احترام العميل المصدر إليه البطاقات الائتمانية شروط العقد المبرم بينه و بين البنك كأن يستعمل بطاقة ائتمانية انتهت مدة صلاحيتها أو بطاقة تم إلغاؤها أو الشراء بأكثر من قيمتها.[2]

3- الجرائم الخاصة بنظم المعالجة الآلية للمعلومات

يقتضي من خلال هذا الوضع معالجة صورتين تتمثل الاولى في الاعتداء على وظائف نظم معالجة المعلومات و تتمثل الصورة الثانية في الاستعمال غير المشروع لنظم المعالجة الآلية للمعلومات، و تندرج تحت هذين الصورتين العديد من السلوكيات التي تشكل بمجموعها الجرائم الواقعة على نظم المعالجة الآلية للمعلومات.[3]

من صور الجرائم الاعتداءات على وظائف نظم المعالجة الآلية للمعلومات هي أي فعل يؤدي إلى منع نظام المعالجة الآلية من القيام بوظائفه الاعتيادية كتعطيل النظام مثلا عن القيام بوظائفه يعد من أبرزها و تتمثل الصورة الثانية في الاستعمال غير المشروع لنظم المعالجة الآلية للمعلومات

1- جزار منصورية، الجريمة المعلوماتية، مذكرة ماستر في الحقوق، تخصص علم الإجرام والعلوم الجنائية، جامعة عبد الحميد بن باديس، 2016-2017،ص31.

[3]- محمود احمد عبابنة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر وتوزيع، عمان، 2009،ص85.

و يندرج ضمن هذه الطائفة في صورة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية و تتمثل في صورة كافية في سرقة منفعة الحاسب الآلي.[1]

4- الجرائم الواقعة على المعلومات داخل أنظمة المعالجة الآلية

اعتبار أن المعلومات نتاجا لمعالجة البيانات، إذ تختلف البيانات عن المعلومات، كما أنها أيضا تختلف المعلومات عن برامج الحاسب الآلي و من صور الاعتداء على المعلومات، سرقة المال ألمعلوماتي أو إتلافه أو تزويره.[2]

إذ لا نتطرق إلى تفصيل هذه الاعتداءات من خلال تصنيفها، فانه سيتم معالجة هذه الأصناف من خلال ذلك لكي نبين شيء من التفصيل و التوضيح من خلال أركان لكل جريمة على حدا في حين جاء على لسان الفقيه "martin wasik" لتقسيمه لجرائم الحاسب الآلي أيضا إلى طوائف ثلاثة مختلفة، إذ تتمثل الطائفة الأولى في دخول و استعمال غير المصرح به لنظام الحاسب الآلي و يندرج تحت الطائفة الثانية أيضا المتمثلة في الاحتيال ألمعلوماتي و سرقة المعلومات، و جاء في الطائفة الثالثة إلى الجرائم التي تساعد الحاسب الآلي على ارتكابها و الأفعال التي تساعد على ارتكاب جرائم الحسابات الآلية.[3]

ثانيا: تصنيف الجرائم المعلوماتية بحسب جرائم الكمبيوتر والانترنت

في نطاق هذا التصنيف يتوجب التمييز بين الأفعال التي تستهدف المعلومات في نطاق نظام الكمبيوتر ذاته وبين الأنشطة التي تستهدف الشبكات ذاتها أو المعلومات المنقولة عنها، أيضا الأنشطة التي تستهدف مواقع الانترنت وخوادمها من نظم الكمبيوتر الكبيرة والعملاقة.[4]

إذ يحضر البعض أنشطة جرائم الانترنيت بتلك المتعلقة بالاعتداء على المواقع و تعطيلها او تشويهها أو تعطيل تقديم الخدمة، و كذلك أنشطة المحتوى الضار، كترويج المواد الإباحية و

[1]- مرجع نفسه، ص85.
[2]- مرجع نفسه، ص92.
[3]- نائلة عادل محمد فريد قورة، المرجع السابق، ص243-ص244.
[4] -Https://universitylifestyle.net/7/4/2021.

المقامرة، و أنشطة أثارة الأحقاد والتحرش، والإزعاج و مختلف صور الأنشطة التي تستخدم في البريد الالكترونية المراسلات الالكترونية.[1]

أما جرائم الكمبيوتر فإنها وفق هذا التقسيم تعاد إلى الأنشطة التي تستهدف المعلومات و البرامج المخزنة داخل نظم الكمبيوتر و تحديدا أنشطة التزوير و احتيال الكمبيوتر و سرقة وقت الحاسوب و اعتراض المعطيات خلال النقل مع انه مفهوم يتصل بالشبكات أكثر من نظم الكمبيوتر مع الإضافة للتدخل غير المصرح به و الذي يتوزع ضمن هذا التقسيم بين دخول غير مصرح به و الذي يتوزع ضمن هذا التقسيم بين الدخول مصرح به للشبكات فيتبع لمفهوم جرائم الانترنيت.[2]

المطلب الثاني: مرتكبو الجريمة المعلوماتية

تبرز خصوصية الجريمة المعلوماتية بصورة أكثر وضوحا في أسلوب ارتكابها و طريقتها، فإذا كانت الجرائم تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف كما هو الحال في بعض الجرائم التقليدية كالسرقة والاختطاف، فان الجريمة المعلوماتية لا تحتاج الى العنف بطبيعتها، بل كل ما تحتاجه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة[3]، من هنا قمنا بتقسيم هذا المطلب إلى فرعين تناولنا في الفرع الأول مفهوم المجرم ألمعلوماتي وتناولنا في الفرع الثاني أصناف المجرم ألمعلوماتي.

الفرع الأول: مفهوم المجرم ألمعلوماتي

هناك تفرقة تقليدية في دارسات علم الإجرام، تقوم على التمييز بين الإجرام الطبيعي والإجرام الاصطناعي –المكتسب– ونادي بهذه التفرقة عالم الإجرام الإيطالي–جار فالو–، ولقد ثار جدال فقهي يدور حول النوع الذي ينتمي إليه المجرم ألمعلوماتي.[4]، وما يمكن القول في هذا الصدد أن

[1]- عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، ط1، دار المستقبل للنشر و التوزيع ، عمان، 2009، ص138.
[2]- مرجع نفسه، ص139.
[3]- نهلا عبد القادر المومني، المرجع السابق، ص57-58.
[4]- عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في الجريمة و المجرم ألمعلوماتي، دار الفكر الجامعي، مصر، 2000، ص95.

المجرم ألمعلوماتي يمثل بالنسبة للمجموعات التقليدية أي (الإجرام الطبيعي) شخصية مستقلة قائمة بذاتها، فهو من جهة مثال منفرد " للمجرم الذكي" ومن جهة إنسان اجتماعي بطبيعته.[1]

أولا: تعريف المجرم ألمعلوماتي

تعرفه الأستاذة "خليلي سهام" هو المجرم الذي له القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الالكتروني الرقمي و ملحقاته ووسائل الاتصال الرقمية، ذلك بأداء فعل أو الامتناع عنه، مما يحدث اضطرابات في المجتمع الدولي أو المحلي نتيجة لمخالفة قواعد الضبط الاجتماعي محليا أو دوليا باعتباره مرتكب جرائم الأذكياء نظرا لخصوصية الركن المادي للجريمة المعلوماتية.[2]

فهو نتاج التقدم ألمعلوماتي في مجال المعلومات والاتصال، هذا التقدم الذي قدم للدول وأجهزتها الأمنية الكثير من التسهيلات والإمكانيات التي تسهم في رفع كفاءتها وتطوير قدرتها على التصدي للجريمة المعلوماتية إلا انه في المقابل أدى ويؤدي في الوقت ذاته إلى تطوير وتحديث الجريمة من حيث الأساليب والمضامين، خاصة في ظل اتجاه التنظيمات أو العناصر الإجرامية التي توظف بعض مخرجات تكنولوجيا المعلوماتية في أنشطتها و ممارستها، فتجاوز بذلك هذا التقدم بقدرات وإمكانيات أجهزة الدولة الرقابية، وأصبح يهدد أمنها وامن مواطنيها.[3]

المجرم المعلوماتي هو كل شخص سواء طفل، او رجل، او انثى، ياتي افعالا ارادية تشكل سلوكا ايجابيا او سلبيا باستخدام تقنية المعلوماتية لاحداث نموذج اجرامي بالاعتداء على حق او مصلحة، وسمات المجرم المعلوماتي تشبه في كثير من الاحيان سمات المجرمين ذوي الياقات البيضاء[4]، حيث ان كل من هؤلاء المجرمين قد يكونوا من ذوي المناصب الرفيعة و المستوى العالي، ومن ذوي التخصصات و الكفاءات العالية، يتمتعون بالذكاء والقدرة على التكيف الاجتماعي في

[1]- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات؛ الطبعة الثانية، دار النهضة العربية، مصر، 1998، ص24.

[2] -https://platform.almanha.com/files/2/115333.

[3]- مرجع نفسه.

[4]- مصطلح المجرمين ذوي الياقات البيضاء، مصطلح حديث نسبيا، اول من اطلقه هو عالم الاجتماع" suther land" حيث وضح ان هذه الجرائم ترتكيب من قبل الطبقة الراقية في المجتمع، ذوي المناصب الادارية الكبيرة، تشمل انواعا مختلفة من الجرائم، كغسيل الاموال وتجارة الرقيق، وتزوير العلامات التجارية وغير ذلك من الجرائم التي يقومون بارتكابها وهم جالسون في مكاتبهم الفخمة.

المحيط الذي يعيشون فيه، بل ان بعضهم يتمتع باحترام وثقة عالية من الاشخاص المحيطين بهم في مجال العمل او في المحيط الاجتماعي.[1]

ثانيا: خصائص المجرم ألمعلوماتي

يمكن أن نستخلص مجموعة من الخصائص التي يتميز بها المجرم ألمعلوماتي، والتي يساعد التعرف عليها مواجهة هذا النمط الجديد من المجرمين، ويعد الأستاذ "parker" واحد من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامه والمجرم ألمعلوماتي بصفة خاصة، ويرى "parker" أن المجرم ألمعلوماتي وإن كان يتميز ببعض الخصائص إلا انه في النهاية لا يخرج عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه.[2]

وفيما يلي عرضا لبعض الخصائص العديدة للمجرم ألمعلوماتي والتي في الغالب تميزه عن غيره من المجرمين العاديين.

1- المجرم ألمعلوماتي مجرم محترف

يتمتع المجرم ألمعلوماتي باحترافية كبيرة في تنفيذ جرائمه، حيث أنه يرتكب هذه الجرائم عن طريق الكمبيوتر الأمر يقتضى الكثير من الدقة والتخصص والاحترافية في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية.[3]

2- المجرم ألمعلوماتي مجرم غير عنيف

المجرم ألمعلوماتي من المجرمين الذين لا يلجئون إلى العنف بتاتا في تنفيذ جرائمهم وذلك لأنه ينتمي إلى إجرام الحيلة فهو لا يلجا إلى العنف في ارتكاب جرائمه، و هذا النوع من الجرائم لا يستلزم

[1] -www.minishawi.com.

[2] -Parker (Donn B) Figding computer crime A neur Framework for protecting information 1998/P 11.

[3]- دورثي إي ديننغ، قراصنة أنظمة الكمبيوتر إعداد، ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر،واشنطن، ترجمة : آمنة علي يوسف، ديسمبر 1998 ،ص 88.

أي قدر من العناء للقيام به، فضلا عما تقدم، فالمجرم ألمعلوماتي مجرم ذكي، يتمتع بالتكيف الاجتماعي و يتمتع بالمهارة والمعرفة وأحيانا على درجة عالية من الثقافة.[1]

3- المجرم ألمعلوماتي مجرم ذكي

إن المجرم ألمعلوماتي ينتمي إلى ما يمكن أن نطلق عليه تقنيات التدمير الناعمة، وبمعنى آخر يكفي أن يقوم المجرم ألمعلوماتي بالتلاعب في بيانات وبرامج الحاسب الآلي بمحو هذه البيانات أو تعطيل استخدامها، فهو يحاول أن يحقق أهدافه بهدوء، و يتطلب كثيرا من الدقة والتخصص في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما يحدث في البنوك مثال، فالشخص القادر على فعل كل هذا بكل تأكيد ليس في زمرة الأغبياء.[2]

تتطلب الجرائم المعلوماتية مقدر عقلية وذهنية عميقة خاصة في الجرائم المالية التي تؤدي إلى خسارة مادية كبير تلحق بالمجني عليه، إذ يلجأ المجرم ألمعلوماتي إلى استخدام العنف أو الإتلاف المادي، بل يستخدم مقدرته العقلية ويحاول تحقيق أهدافه، وبمقارنة الإجرام ألمعلوماتي هو عكس التقليدي حيث يلاحظ عمليات الإجرام التقليدي الذي يميل إلى العنف أما الإجرام ألمعلوماتي يسعى إلى معرفة طرق جديد من أجل اختراق الحواجز الأمنية في البيئة الإلكترونية ومن ثم نيل مبتغاة دون عنف أو إتلاف مادي بل يحاول أن يحقق أهدافه بهدوء، وعند مقارنة الإجرام التقليدي بالإجرام ألمعلوماتي فهذا الأخير لا يميل إلى العنف هو إجراء الأذكياء أما الإجرام التقليدي فهو إجرام عنف، فالمجرم ألمعلوماتي يسعى بشغف إلى معرفة طرق جديد مبتكر لا يعرفها أحد سواه وذلك من جل اختراق الحواجز الأمنية في البيئة الإلكترونية ومن ثم نيل مبتغاة.[3]

4- المجرم ألمعلوماتي مجرم يتمتع بالخبرة المهارة

يرى الخبير" دون باركر" أن المهارة هي أبرز خصائص مجرم تكنولوجيا المعلومات، فتنفيذ الجريمة التقنية يتطلب قدرا من المهارة يتمتع بها الفاعل والتي قد يكتسبها عن طريق الدارسة

[1]- آمنة علي يوسف، المرجع السابق، ص88.
[2]- نسرين عبد الحميد نبيه، الجريمة المعلوماتية و المجرم ألمعلوماتي، منشأة المعارف، جلال حزي و شركائه، الإسكندرية، 2008، ص120.
[3]- نهلا عبد القادر المومني، المرجع السابق، ص78.

المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات الحديثة أو مجرد التفاعل الاجتماعي مع الآخرين.[1]

بالنسبة لمجرموا المعلوماتية يتمتعون بقدرات لا ياستهان بها من الخبرة و المهارة بتقنيات الحاسوب والإنترنت، بل فالبعض من هؤلاء المجرمين هم من المتخصصين في مجال معالجة المعلومات آليا، فتنفيذ الجريمة المعلوماتية يتطلب قدرا من المهارة لدى الفاعل الذي قد اكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبر المكتسبة في مجال تكنولوجيا المعلومات، كما يمكن أن يكون للمجرم ألمعلوماتي تصور كامل لجريمته، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها ويكون ذلك قبل تنفيذ جريمته، حتى لا يفاجأ بأمور غير متوقعة من شأنها أن تؤدي إلى إفشال مخططاته أو الكشف عنها.[2]

5- المجرم المعلوماتي يتمتع بالمعرفة

فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، إذ أن المجرم المعلوماتي باستطاعته أن يكون تصورا كاملا لجريمته، كون المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته[3].

6- المجرم المعلوماتي يتمتع بالسلطة

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

[1]- علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة(دارسة مقارنة)، منشورات زين الحقوقية، لبنان، 2013 ،ص107.
[2]- نهلا عبد القادر المومني، المرجع السابق، ص 77 – 78.
[3]- حاجب هيام، الجريمة المعلوماتية، مذكرة التخرج لنيل اجازة المدرسة العليا للقضاء، الجزائر، 2005_2006، ص9.

التعاملات، وقد تكون هذه السلطة غير حقيقية كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر[1].

الفرع الثاني: تصنيف مرتكبي الجرائم المعلوماتية

لقد تنوعت الاتجاهات الفقهية الباحثة في تصنيف مرتكبي الجرائم المعلوماتية حيث تم تصنيفهم إلى عد فئات، وهذا راجع إلى مقدار الخطورة الإجرامية الكامنة في شخص المجرم ألمعلوماتي، وهذا ما ستعرفه فيما يأتي:

أولا: القراصنة :

يعرف قراصنة المعلومات هم عاد مجرمون من أصحاب الخبر يهدفون إلى دخول أنظمة المعلوماتية غير المسموح بها لهم الدخول إليها وكسر الحواجز الأساسية المحيطة بهذه الأنظمة، ويمكن تصنيف القراصنة إلى صنفين.

1- الهواة العابثون الهاكرز (hackers)

هذا النوع من القراصنة أو كما يطلق عليهم "بالهاكرز" يرون أن اختراق الأنظمة المعلوماتية تحديا لقدراتهم الذاتية، وهذه الطائفة عاد ما تكون من هواة الحاسوب، فيقومون بأعمالهم هذه لمجرد إظهار أنهم قادرون على اقتحام المواقع الأممية أحيانا أو لمجرد ترك بصماتهم التي تثبت وصولهم إلى تلك المواقع أحيانا أخرى، وهم يدعون أنه لا توجد هناك دوافع تخريبية وراء أعمالهم، بل قد يكون الفضول وحب المعرفة والتعمق في عمل الأنظمة المعلوماتية هو دافعهم الأول ومجرموا المعلوماتية هم أشخاص عاديون يشتغلون بمناصب محل ثقة ولديهم الكفاءة الخاصة والمعرفة والمهارة المطلوبة في مجال الحواسيب والشبكات الإلكترونية وعلى سبيل المثال، خرق استشاري تقنية معلومات أحد الأنظمة الأممية للإنترنت البريطانية لمجرد كشف القنوات الأممية بها ولقد نجح في الحصول على أسماء أكثر من (24) ألف شخص وعناوينهم وكلمات السر ومعلومات البطاقات الائتمانية من بينهم خبراء عسكريون وموظفو ن حكوميون وكبار مديري الشركات.[2]

[1]- حاجب هيام، المرجع السابق، ص9.
[2]- نهلا عبد القادر المومني، المرجع السابق، ص 84.

"فالهاكرز" هم متطفلون يتحدون إجراءات أمن النظم و الشبكات لا تتوفر لديهم في الغالب دوافع حاقدة أو تخريبية، وانما ينطلقون من دوافع التحدي و اثبات الذات، تظهر جليا في اعترافات متهم يبلغ من العمر 17 سنة أمام القضاء الألماني حيث نسب إليه دخوله بطريقة غير مشروعة في نظام الفيديو تكس "videotext" الخاص بي "bundaspost" والمعروفة بمصطلح "btx " ودافع المتهم عن نفسه قائل " تملكني إحساس قوي بأن أكون مفيد في كشف عيوب نظام "btx" ولذلك أرسلت في الحال إلى مجموعة عمل"btx " كل العناصر التي اكتشفتها بالصدفة والتي أظهرت تشككها فيما يخص حماية البيانات، لاسيما وأن غالبية ملاحظاتي لم تكن معروفة بعد لدى هؤلاء مما أتاح الأمر إلى تلاشي هذه العيوب، وأضاف كذلك أنه مولع بنظام "btx " و يكرس نفسه له صباحا مساء، لكنه ليس شرير على الاطلاق، كبعض الأشخاص القائمين على نظام "btx" الذين لا يملكون أي كفاءة.[1]

ويجب أن نشير إلى أن أول مرة تم إطلاق على المجرم ألمعلوماتي مصطلح (hackers) كان في الستينيات القرن الماضي، إذ أُطلق على طلبة الجامعات الأمريكية، ممن يتميزون بقدر عالي من الكفاءة التقنية ويتفاخرون بإلمامهم بعلوم الحاسوب، وبقدرتهم على اختراق شبكات الحاسب الآلي وبجهودهم الذاتية، وبدون الاستعانة بأية تعليمات من أية مصادر ومن الأمثلة عن الأفعال التي ارتكبتها طائفة "الهاكرز"، ما قامت به عصابة "414" "الأمريكية" والتي نسبت إليها أكثر من ستين (60) فعًلا وتعديا واخترقا لذاكرات الحاسب الآلي مما نتج عنها أضرارا لحقت بالمنشآت العامة والخاصة.[2]

2- القراصنة المخترقين

يطلق على هذه الطائفة مصطلح "Crackers" يتميز أفرادها بالتخصص العالي في مجال الحاسب الآلي، وتعد هذه الطائفة الأخطر من بين مجرمي المعلوماتية، وتهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم وسخرتهم لارتكاب جرائم الحاسوب، كما يهدف بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي ويتسمون أطراف

[1]- عبد الفتاح حجازي بيومي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، المرجع السابق، ص104.

[2]-جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة)؛ دار الثقافة للنشر والتوزيع، الأردن، 2010 ،ص72.

هذه الطائفة بالتكتم خالفا للطائفة الأولى أيلا يتبادلون المعلومات بشأن أنشطتهم بل يطورون معارفهم الخاصة ويحاولون بقدر الإمكان عدم الكشف عن طرقهم التقنية لارتكاب جرائمهم.[1]

هذه الفئة تعكس اعتداءاتهم و ميولات اجرامية خطيرة تنبئ عن رغبتها في احداث التخريب، يتميز هؤلاء بقدراتهم التقنية الواسعة و خبرتهم في مجال انظمة الحاسوب والشبكات، وهم اكثر خطورة من الصنف الاول[2]، فهم يستخدمون برامج التقنية في محاولات لأختراق الانظمة والاجهزة للحصول على المعلومات السرية[3]، او القيام بعمليات تخريبية معينة كأختراق مزودات الشركات لحذف واضافة المعلومات او لمجرد الاطلاع عليها، او للدخول الى مزودة خدمة الانترنت والتلاعب بمحتويات الصفحة، او الاستيلاء على ارقام البطاقات الائتمانية واستخدامها، وكذلك القيام بمحاولة ازالة او فك الحماية التي تصنعها شركات انتاج البرامج على برامجها لمنع عمليات النسخ غير القانونية.[4]

ثانيا: صغار مجرمي المعلوماتية

هم فئة من صغار السن مولعون بالثورة المعلوماتية بسبب انتشار الحاسبات الآلية[5]، لذلك كان أولئك الشباب يرتكبون الجرائم المعلوماتية عن طريق استخدام الحاسبات الآلية الخاصة بهم أو بمدارسهم[6]، أثارت هذه الفئة جدال فقهيا واسعا بحيث يرى البعض من الفقهاء أنه "لا يبدو من المناسب أن يصنف هؤلاء الشباب في طائفة أو أخرى من الطوائف الإجرامية لان لديهم ببساطة ميلا للمغامر والتحدي والرغبة في الاكتشاف ونادرا ما تكون أهداف أفعالهم المحظور غير شريفة وهم لا

---

[1]- نجا بن مكي، المرجع السابق، ص32-33.

[2]- نهلا عبد القادر المؤمني، المرجع السابق، ص84.

[3]- يعتبر اشهر كراكرز في العالم حتى الان، الامريكي(كيفن ميتينك)، الذي اصبح اسطورة الكراكرز ومثلهم الاعلى، نظرا لموهبته الفذة وقدرته الفائقة في السرقة، وتدمير الاجهزة، والشبكات والمواقع بشكل عام، وقد اصبح اشهر كراكرز بعدما نفذ اكبر عملية سرقة تاريخية الكترونية عرفها العالم، حيث سرق حوالي مئتي الف رقم لبطاقات ائتمان عام 1995، وتم القبض عليه وسجن، الا ان انصاره والجماعات المؤيدة له تقوم بأختراق بعض المواقع الهامة للتأثير على الحكومة الامريكية للافراج عنه، وهذا ما وقع لصحيفة النيويورك تايمز على شبكة الانترنت، انظر الموقع

www.chawkhtabib.info/spip.php.articlc478.

[4]- ايهاب فوزي السقا، الحماية الجنائية والامنية لبطاقات الائتمان، دار الجامعة الجديدة، الاسكندرية، 2007، ص135.

[5]- خالد عياد الحلبي، المرجع السابق، ص35.

[6]- عبد الفتاح بيومي حجازي، النظم القانونية لحماية التجارة الإلكترونية، دار الفكر الجامعي، مصر، 2002، ص104.

يدركون ولا يقدرون مطلقا النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة بالنسبة لنشاط منشأ أو شركة تجارية.[1]

غير ان الفقه الراجح قد اقر بأن هذه الطائفة تصنف ضمن مجرمي المعلوماتية مثل غيرهم من المجرمين، حيث أن أفعالهم المتمثلة في انتهاك الأنظمة واختراق الحواجز الأمنية في مجال إلكتروني تعد أفعال خطير من الناحية العلمية، بل أن أفعالهم لا تقف عند حدود دولة أخرى فهي تتعدى كل الحواجز الجغرافية، وفي الواقع يجب عدم التقليل من خطورة هذه الفئة لانها قد تتعدى مرحلة الهواية والعبث وتدخل مرحلة الاحتراف لهذه الجرائم، كما يوجد مخاوف تتمثل في احتضان منظمات الجريمة لهذه الفئة للاستفادة من مهاراتهم وتطويرها من أجل تحقيق غايتهم الإجرامية.[2]

هؤلاء الشباب قد تكون غايتهم في النهاية مجرد التسلية والملاحظة وليس لديهم كأصل عام دوافع لارتكاب أفعال إجرامية، ولكن لا يجب أن نستخف بها لأن خطر انزلاق هذه الفئة إلى احتراف الأفعال غير المشروعة وارتكاب الجرائم المعلوماتية هو احتمال قائم، وعندئذ يتحول من مجرد هاوي صغير للأفعال غير المشروعة إلى محترف لها، ومثال على الجرائم التي تقترفها هذه الطائفة الإجرامية، ما حدث في الولايات المتحدة الأمريكية أين قام أولاد المدرسة الثانوية في مدينة "مانهاتن" عام1980بختراق شبكة اتصالات البيانات الكندية وتدمير ملفات زبائن الشركة.[3]

يمكن رد الاتجاهات التقديرية لطبيعة هذه الفئة، وسمات افرادها، ومدى خطورتها في نطاق ظاهرة جرائم الحاسوب الى ثلاثة اتجاهات.

– **الاتجاه الاول:** اتجاه لا يرى اصباغ أية صفة جريمة على هذه الفئة، او على الافعال التي تقوم بها، ولا يرى وجوب تصنيفهم ضمن الطوائف الاجرامية لمجرمي المعلوماتية، استنادا الى ان صغار السن لديهم ببساطة ميل للمغامرة والتحدي، والرغبة في الاكتشاف، ونادرا ما تكون اهداف افعالهم المحظورة غير شرعية، واستنادا الى انهم لا يدركون، ولا يقدرون مطلقا النتائج المحتملة التي يمكن ان تؤدي أليها افعالهم غير المشروعة بالنسبة لنشاط منشأة او شركة تجارية.

[1]- نهلا عبد القادر المؤمني، المرجع السابق، ص81-82.
[2]- مرجع نفسه،ص82.
[3]- محمـــود أحمـــد عبابنة، المرجع السابق، ص41.

– **الاتجاه الثاني:** هذا الاتجاه يحتفي بهذه الفئة ويناصرها ويعتبرها ممن يقدم خدمة لأمن المعلومات ووسائل الحماية، ويصفهم بالأخيار واحيانا بالأبطال الشعبيين، هذا الاتجاه في تقديره لهذه الطائفة او الفئة بالمطالبة بمكافئتهم بأعتبارهم لا يسببون ضررا للنظام، ولا يقومون بأعمال احتيالية، وينسب اليهم الفضل في كشف الثغرات الامنية في تقنية المعلومات، ومثل هذا الرأي قال به احد اشهر المدافعين عن الهاكرز الصغار "هيوجوكورن".

– **الاتجاه الثالث:** يرى هذا الاتجاه ان مرتكبي جرائم المعلوماتية من هذه الطائفة، يصنفون ضمن مجرمي الحاسوب كغيرهم دون تمييز استنادا الى ان تحديد الحد الفاصل بين العبث في الحواسيب وبين الجريمة امر عسير من جهة، ودونما اثر على وصف الفعل قانونا من جهة اخرى، استنادا الى ان خطورة افعالهم التي تتميز بأنتهاك الانظمة واختراق الحواسيب، وتجاوز اجراءات الامن، والتي تعد بحق من اكثر جرائم الحاسوب تعقيدا من الوجهة التقنية، عوضا عن مخاطرها المدمرة ويدعم صحة هذا الاتجاه تخوفات التي يثيرها اصحاب الاتجاه الاول ذاتهم، اذ يخشون من الخطر الذي يواجه هذه الطائفة، المتمثل بأحتمال الانزلاق من مجرد هاوي صغير لاقتراف الافعال غير المشروعة الى محترف لأعمال السلب والاحتيال، هذا الى جانب خطر اخر اعظم يتمثل في احتضان منظمات الاجرام ومجرمين غارقين في الاجرام لهؤلاء الشباب، أي استغلالهم من طرف منظمات الجريمة المنظمة.[1]

ثالثا: المجرم الوظيفي (Criminals Career)

فهم الطائفة الأكثر شيوعا بين مجرمي المعلوماتية الذين يهدفون وراء نشاطهم الإجرامي تحقيق الربح المادي بطريقة غير مشروعة، ويعمل المنتمون لهذه الطائفة في أغلب الأحوال بطريقة منظمة حيث ينطبق على أفعالهم وصف الجريمة المنظمة، أو يشترك في هذه الجريمة أكثر من فاعل على الأقل، ويتقرب المجرم ألمعلوماتي المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي، ولا شك أن جرائم الحاسبات الآلية بدأت تجذب بشكل كبير اهتمام الجماعات الإجرامية المنظمة نظرا لارتفاع قيمة الأرباح المادية مع صعوبة الكشف عنها وإثباتها مقارنة مع الجرائم التقليدية، إلا أن نسبة هذا

[1]- عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة دراسة في الظاهرة الاجرامية المعلوماتية، دار الفكر الجامعي، الاسكندرية، 2008، ص89.

النمط ما زالت منخفضة مقارنة مع أنماط أخرى بنسبة (10%) وذلك راجع لما تتطلبه هذه الجريمة من توافر درجة من العلم بتقنية الحاسبات وهو ما لا يتوفر لدى الكثير من هذه الطائفة.[1]

رابعا: المدافع المتطرف ألمعلوماتي

تضم هذه الفئة الجماعات الإرهابية أو المتطرفة، والتي تتكون من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية، ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي، وعادة ما يكون هذا النشاط يرتكز على العنف من أجل لفت الأنظار إلى ما يدعون إليه إن اهتمام الجماعة الإرهابية يتجه إلى نوع جديد من النشاط الإجرامي ألا وهو الجريمة المعلوماتية، فاعتماد المؤسسات المختلفة داخل الدول على أنظمة الحاسبات الآلية في إنجاز أعمالهم والأهمية القصوى للمعلومات التي تحتويها في أغلب الأحوال قد جعل من هذه الأنظمة هدفا جذابا لهذه الجماعات ولا تزال الأسئلة الشهير في هذا الخصوص قيام إحدى الجماعات الإرهابية المعروفة في أوروبا بتدمير ما يزيد عن 60 مركز للحسابات الآلية خلال الثمانينات لتلفت الأنظار إلى أفكار ومعتقداتها.[2]

إذ تعكس اعتداءاتهم و ميولهم الإجرامي والرغبة في الإتلاف والتخزين والتعديل والتخريب باستخدام الفيروسات أو القنابل المنطقية، باعتبارهم من أصحاب التخصصات العالية، ولهم الهيمنة الكاملة على تقنيات الحاسوب والشبكة المعلوماتية ومثال ذلك ما قام به "الكراكرز" الجزائري المدعو(أنجل) المنحدر من مدينة قسنطينة والذي كرس جل وقته لإتلاف موقع (أرض إسرائيل) وهو أشهر وأكبر مواقع الكيان الصهيوني على الشبكة العنكبوتية يشرف عليه مهندس في الإلكترونيك يدعى (يوسي طيب) الذي يعمل بوزارة الدفاع للكيان الصهيوني، يساهم في تطوير الأسلحة في هذا الكيان... وقد طلب (يوسي) من (أنجل) "الكراكرز" الجزائري مرارا التوقف عن الاختراق إلا انه لم يكف عن ذلك.[3]

---

[1]- نائلة عادل محمد فريد قورة، المرجع السابق، ص62.

[2]- نائلة عادل محمد فريد قورة، مرجع نفسه، ص63.

[3]- فلالي رشيد، الشروق تقضي يوم مع أشهر قراصنة الإنترنت في الجزائر، عدد صادر في 22 نوفمبر 2008، مقال متوفر على الموقع:
http://www.echoroukonline.com/ara/?news=29084

خامسا: طائفة مجرمو المعلومات اصحاب الآراء المتطرفة

المتطرفون الفكريون طائفة من الناس نزلت بهم عقولهم الى مستنقع الشطط في التفكير، متطرفون لأفكارهم واراءهم، ومتجاوزون بذلك كل الحدود المعقولة والمقبولة للتحاور والنقاش، ذلك بخصوص قضية او غاية ليس لها علاقة بمصالحهم الشخصية، وهم في سبيل تحقيق ما يعتقدونه، على استعداد لارتكاب انشطة اجرامية مختلفة، وتختلف وراءها اضرار جسيمة سواء على افراد من المجتمع او على قطاعات كاملة منه هادفين من ذلك تحول المجتمع الى الأفضل من جهة نضرهم بدون قيد او شرط، على ذلك يختلف المجرم العادي عن المجرم المعرؤلوماتي المتطرف، فالأول لا يبغي سوأ تحقيق منفعته الشخصية، اما الثاني فيكون مدفوعا ببعض البواعث التي قد تكون ذات طبيعة سياسية او اقتصادية او تتعلق بحقوق الانسان او مرتبطة بشؤون البيئية او الدينية.[1]

هذا التطرف الفكري مجسد اليوم فيما يعرف بصراع الحضارات، حيث اطلق العديد من المتطرفين عديمو الفهم والمتشددون الخلاف الى الوراء بالزج بالدين الى جلسة الصراع، فقد ادعى بعضهم بأفضلية احد الاديان عن الاديان الاخرى من حيث المساهمة بالتقدم الحضاري الذي وصلت اليه البشرية.

ويمكن ان نشير هنا الى منظمة الاولوية الحمراء الايطالية التي استهدفت نظم المعلومات المتعلقة ببعض الهيئات، ومن ذلك اعتدائها على مكتب المرور الرئيسي في ايطاليا – منذ بضع سنوات – مما ادى الى اضرار جسيمة دمرت معظم المعلومات الخاصة باللوحات المعدنية ورخص القيادة بما فيها النسخ الاحتياطية، وظل الايطاليون لمدة عامين متتاليين لم يكن لديهم أي مستند يثبت ملكيتهم لسياراتهم، او لم يكن لديهم رخصة قيادة صحيحة او سليمة.[2]

وكذلك ظهرت في فرنسا منظمة او هيئة ازالة او تدمير الحاسبات او نظم المعلومات لذا فقد ايقنت المنظمات الارهابية ان في استطاعتها وبمجهود بسيط ان تلحق اضرار جسيمة داخل أي مشروع او مؤسسة عن طريق تدمير المركز المعلوماتي، واخيرا نستطيع القول ان افراد هذه الطائفة

[1]- حاتم عبد الرحمن منصور الشحات، الاجرام المعلوماتي، دار النهضة العربية، القاهرة، 2003، ص88.
[2]- سامي الشوا، الغش المعلوماتي ظاهرة اجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، ص245.

من المجرمين لديهم اتجاه اجرامي خطير، وذو نية بالغة السوء، وذلك لأنهم لا يبالون بالأضرار الجسيمة التي اصابت الافراد او المجتمع او بعض قطاعاته.[1]

[1]- جميل عبد الباقي الصغير، الانترنت والقانون الجنائي و الاحكام الموضوعية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2001، ص33.

الفصل الثاني

الفصل الثاني

النماذج الاجرامية المعلوماتية وسبل التصدي للأثار المترتبة عليها

تمهيد

المبحث الاول: النماذج الاجرامية المعلوماتية المؤثرة على التطور الاقتصادي

المطلب الاول: الجرائم الواقعة على المعلومات داخل انظمة المحاكة الالية

الفرع الاول: جريمة السرقة المعلوماتية

الفرع الثاني: جريمة التزوير المعلوماتي

المطلب الثاني: الجرائم الواقعة بواسطة النظام المعلوماتي

الفرع الاول: جريمة الاتلاف المعلوماتي

الفرع الثاني: جريمة النصب (الاحتيال) المعلوماتي

المبحث الثاني: الاثار الاقتصادية للجرائم المعلوماتية واستراتيجيات مواجهتها

المطلب الاول: الاثار الاقتصادية للجرائم المعلوماتية

الفرع الاول: الاثار الناجمة عن الجريمة المعلوماتية و انعكاسها على الاقتصاد

الفرع الثاني: معوقات الجريمة المعلوماتية الماسة بالاقتصاد

الفرع الثالث: التكلفة الاقتصادية للجرائم المعلوماتية

المطلب الثاني: الاتفاقيات الدولية و الاقليمية في مكافحة الجرائم المعلوماتية

الفرع الاول: الاتفاقيات الدولية في مكافحة الجريمة المعلوماتية

الفرع الثاني: الجهود الاقليمية في مكافحة الجريمة المعلوماتية

تمهيد

الجرائم المعلوماتية هي تلك الجرائم التي تتم باستخدام الحاسوب أو تلك الجرائم التي تقع على الحاسوب ذاته كما تتشابه كل من الجريمة المعلوماتية والجريمة التقليدية من حيث المفهوم باعتبار كليهما يهددان المصلحة العامة أو الخاصة المحمية قانون، لكنهما يختلفان من حيث الركن المادي والمعنوي الخاص بكل جريمة .

وعليه سوف نحاول تسليط الضوء على أهم نماذج هذه الجريمة فأخذنا الجرائم المعلوماتية الواقعة على نظام المعلوماتي وهي السرقة المعلوماتية والتزوير المعلوماتي، والجرائم الواقعة بواسطة نظام المعلوماتي وهي جريمتي الاتلاف المعلوماتي والنصب (الاحتيال) المعلوماتي.

سنسلط الضوء على الاثار الاقتصادية للجرائم المعلوماتية واستراتيجيات مواجهتها، ويترتب على الجريمة المعلوماتية الماسة بالاقتصاد عدة اثار يتوجب الوقوف عليها، سوف نتحدث عن اهم الاتفاقيات التي عملت على مكافحة الجريمة المعلوماتية سواء على المستوى الدولي او على المستوى الاقليمي، وعليه قمنا بتقسيم هذا الفصل الى مبحثين تناولنا في المبحث الاول النماذج الاجرامية المعلوماتية المؤثرة على التطور الاقتصادي، وتناولنا في المبحث الثاني الاثار الاقتصادية للجرائم المعلوماتية واستراتيجيات مواجهتها.

المبحث الاول: النماذج الاجرامية المعلوماتية المؤثرة على التطور الاقتصادي

سنحاول تسليط الضوء على أهم نماذج الجريمة المعلوماتية التي لها بعد اقتصادي فأخذنا جريمة السرقة المعلوماتية لما لها أهمية على التطور الاقتصادي، كما اخترنا نموذج آخر يمس بالثقة العامة كجريمة التزوير المعلوماتي و التي أصبحت شائعة بشكل كبير في الوقت الراهن، كما أن دراستنا لنماذج الجريمة المعلوماتية المؤثرة على النمو الاقتصادي لا يمكن أن يكتمل دون التعرف على الاصناف المستحدثة و بالتالي سنحاول معالجة جريمتين مستحدثتين هما جريمة الاتلاف المعلوماتي و كذلك جريمة النصب المعلوماتي.

قمنا بتقسيم هذا المبحث الى مطلبين تناولنا في المطلب الاول الجرائم الواقعة على المعلومات داخل انظمة المحاكة الالية، تناولنا في المطلب الثاني الجرائم الواقعة بواسطة النظام المعلوماتي.

المطلب الاول: الجرائم الواقعة على المعلومات داخل انظمة المحاكة الالية

شمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها، سنحاول التطرق في هذا المبحث لجريمتين هما جريمة السرقة المعلوماتية و جريمة التزوير المعلوماتي.

الفرع الاول: جريمة السرقة المعلوماتية

في مجال شبكة الأنترنت هناك العديد من جرائم الكمبيوتر التي ترتكب كل يوم ويعد الحاسب الآلي أداة فعالة لارتكاب الجريمة ضد أفراد، والاعتداء على أموال الغير التي اتخذت صورة مستحدثة، ولهذا جاء التجريم وفرضت الحماية الجنائية من مخاطر استعمال الأنترنت والبيانات المتبادلة عبرها وهو ما يجرنا إلى دراسة الجرائم المتعلقة بالاعتداء على الأموال المعلوماتية وذلك من خلال تعريف جريمة السرق المعلوماتية و شرح أركان هذه الجريمة، وبيان اهم الجزاءات المقررة لهذه الجريمة.

اولا: تعريف جريمة السرقة المعلوماتية

عرف المشرع العراقي جريمة السرقة في المادة (439) من قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل بأنها ((اختلاس مال منقول مملوك لغير الجاني عمداً، ويعتبر مالاً منقولاً لتطبيق أحكام السرقة...القوى الكهربائية والمائية وكل طاقة أو قوة محرزة أخرى...))[1]، ولقد عرف المشرع الجزائري جريمة السرقة في المادة (350) من قانون العقوبات الجزائري رقم (66-156) لسنة (1966) المعل والمتمم على انها ((كل من اختلس شيئا غير مملوك له يعد سارقا...))[2]، وتقابلها المادة (373) من قانون العقوبات البحريني رقم (15) لسنة 1976، 2وكذلك تقابلها المادة (382) من قانون العقوبات الاماراتي رقم (3) لسنة (1987) المعدل، وتنص المادة (311) من قانون العقوبات المصري في تعريفها للسرقة بأنها ((كل من اختلس منقولا مملوكا لغيره فهو سارق))، كما عرفها المشرع الأردني ((اخذ مال الغير المنقول دون رضاه))[3]، وكذلك عرفها المشرع الفرنسي في قانون العقوبات النافذ 1992 في المادة (1/311)بقوله ((يعد سارقا من اختلس بطريق الغش شيئا مملوكا للغير)).[4] أما بالنسبة لتعريف الفقه للسرقة قد جرى تعريفها أنها:" اختلاس مال منقول مملوك للغير بنية تملكه".[5]

لا تثور المشكلة عندما يتم سرقة المعلومات المخزنة على أدوات التخزين ذات الكيان المادي المحسوس كأسطوانات الحاسب، لأن السرقة هنا تنصرف إلى مال منقول مادي يتم إخراجه من حيازة مالكه أو حائزه الشرعي إلى الغير وهو الأسطوانة بما عليها من معلومات، ولكن يثور الخلاف عندما يتم الاستيلاء على المعلومات المخزنة داخل الجهاز دون وجه حق أو نسخ هذه المعلومات، وهو ما يعبر عنه حاليا بالقرصنة.[6]

---

[1]- الامر رقم (111)، المتضمن قانون العقوبات العراقي، الصادر سنة 1969 المعدل.

[2]- الامر رقم (156/66)، المتضمن قانون العقوبات الجزائري، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 71، الصادر في 08 جوان 1966،المعدل والمتمم.

[3]- الامر رقم (16)، المتضمن قانون العقوبات الاردني، الصادر سنة 1960.

[4]- انسام سمير الطاهر، جريمة السرقة الالكترونية، مجلة جامعة بابل للعلوم الانسانية، قسم القانون، العراق، 2019، المجلد27، العدد5، ص133.

[5]- محمد محمود المكاوي، الجوانب الأخلاقية والمهنية للحماية من الجرائم المعلوماتية، الطبعة الأولى، المكتبة العصرية للنشر والتوزيع مصر، 2010، ص 297.

[6]- محمود احمد عبابنة، المرجع السابق، ص93.

وعلى صعيد الفقه تعرف السرقة المعلوماتية بانها عبارة عن رسالة أيا كانت محتوياتها قابلة للنقل أو الإرسال للغير ، أو هي رمز أو مجموعة رموز تنطوي على معنى معين خاص بالمستخدم.[1]

السرقة المعلوماتية هي عبارة عن أفعال غير مشروعة، يكون الحاسب الآلي محلا لها أو وسيلة لارتكابها، وعليه فإن الحاسب الآلي لا يعدو أن يقوم بأحد الأدوار التالية دور الضحية في السرقة؛ دور المحيط أو البيئة التي ترتكب فيها السرقة؛ دور الوسائل التي ترتكب بواسطتها السرقة؛ ودور التخويف أو الخداع أو غش الضحية.[2]

ثانيا: اركان جريمة السرقة المعلوماتية

لقيام جريمة السرقة المعلوماتية البد من توفر ركنين هما الركن المادي والركن المعنوي لجريمة السرقة المعلوماتية وستتعرض لها كالتالي:

1- الركن المادي

يتمثل الركن المادي في جريمة السرقة المعلوماتية بالدخول غير المشروع على البيانات والمعلومات للآخرين، والقاعدة العامة ان الركن المادي يتكون من عناصر ثلاثة،(سلوك إجرامي ونتيجة جرميه وعلاقة سببية)، ويتمثل السلوك الجاني الإجرامي في جريمة السرقة الالكترونية بالدخول غير المشروع على البيانات والمعلومات للآخرين والقيام بالنسخ والاستيلاء والنقل غير المشروع لها[3]، وبالنسبة (لعنصر النتيجة) يقصد به التغيير الذي يحدث في العالم الخارجي كأثر للفعل الجرمي، والنتيجة لا تعتبر من العناصر الأساسية في كل جريمة وإنما هي لازمة في بعض الجرائم دون الأخرى[4]، إذ تتحقق بمجرد الدخول غير المشروع والقيام بفعل السرقة نلاحظ أن جريمة السرقة المعلوماتية تقع بمجرد وقوع السلوك الإجرامي المتمثل بالنسخ غير المشروع للبيانات والمعلومات ،أما العلاقة السببية في هذه الجريمة هي الصلة التي تربط بين الفعل

[1]- فايز الظفيري، الأحكام العامة للجريمة الإلكترونية، بحث منشور في مجلة العلوم القانونية والاقتصادية، 2002، العدد الثاني، ص488.
[2]- انسام سمير الطاهر، المرجع السابق، ص134.
[3]- مرجع نفسه،ص139.
[4]- معن احمد محمد الحياري، الركن المادي للجريمة، ط1 ،منشورات الحلبي الحقوقية، لبنان، 2010، ص194.

والنتيجة وهي العنصر الثالث من عناصر الركن المادي وتتمثل العلاقة السببية في هذه الجريمة بالرابطة التي تربط فعل السرقة والنتيجة المتحققة أي النسخ أو الاستيلاء أو التجسس أو ما شابه ذلك بحيث إنه لولا فعل الجاني لما ترتبت تلك النتيجة الجرمية.[1]

الركن المادي وفقا للقواعد العامة للسرقة هو الاختلاس اتفق الفقه والقضاء على اعتبار الاختلاس بانه "أخذ مال الغير دون رضاه "، أي لابد أن يتم نزع المال من مالكه بالقوة وهو الاستيلاء على حيازة الشيء بغير رضى مالكه أو حائزه ويتوفر الاختلاس إذا قام الجاني بحركة مادية لينقل الشيء إلى حيازته أيا كانت الطريقة ويشترط أن يكون الاستيلاء بفعل الجاني.[2]

ولإيضاح الركن المادي لجريمة السرقة المعلوماتية سنتناول فيه عناصر فعل الاختلاس في الجريمة المعلوماتية والعنصر المعنوي والذي يتمثل في عدم رضى المجني عليه ونية تملك الجاني.

أ- فعل الاختلاس وعناصره في جريمة السرقة المعلوماتية

لا خلاف بين الفقهاء على أن الاختلاس الذي يقع على المكونات المادية للحاسب الآلي وملحقاته والبرامج والبيانات المدونة على دعامات مادية كالأسطوانات والشرائط وغيرها والتي يتم نقلها أو الاستيلاء عليها وحيازتها دون رضاء مالكها أو حائزها وبغية تملكها تخضع وفقا للمفهوم التقليدي للقواعد العامة للسرقة، فسرقة دعامة مادية (اسطوانة أو أي قرص مضغوط) محمولة بمعلومات في شكل معطيات هو كسرقة كتاب مملوك للغير باعتبار، هو أيضا محمول بمعلومات[3]. والخلاف بين الفقهاء يثور من خلال تطبيق فعل الاختلاس وعناصره على المكونات غير المادية للنظام المعلوماتي وسنوضح ذلك من خلال عنصري الاختلاس

[1]- واثبة داود السعدي، قانون العقوبات، القسم الخاص، بغداد، 1989، ص104.
[2]- عبد الفتاح بيومي حجازي، المرجع السابق، ص408.
[3]- دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري المقارن، رسالة ماجستير، جامعة منتوري قسنطينة، 2013، ص56.

الفقرة الاولى: العنصر الموضوعي (الاستيلاء على المعلوماتية) :

نشأ الخلاف بين الفقهاء حول الاستيلاء على المعلوماتية من خلال رأيين، الأول يرى عدم توافر ركن الاختلاس في حالة الاستيلاء على المعلوماتية، والثاني يرى توافر ركن الاختلاس في حالة الاستيلاء على المعلوماتية، وقد ظهرت أوجه هذا الخلاف من خلال الصور التالية: الأولى الطبيعة المعلوماتية، والثانية المعلوماتية المخزنة بالنظام المعلوماتي، الثالثة المعلوماتية المخزنة على دعامات[1].

الفقرة الثانية: العنصر المعنوي (عدم رضاء المجني عليه ونية تملك الجاني):

يجب أن يتوفر القصد الجنائي العام، و يتمثل في تيقن الجاني أنه يأخذ مال الغير وليس ماله، فالشخص الذي يخرج من المطعم ويحمل معطف غيره معتقدا أنه معطفه لتشابههما لا يتوفر فيه القصد الجنائي العام و عن القصد الجنائي الخاص والذي يتمثل نية تملك الشيء المختلس، فمن يأخذ شيئا من صاحبه بغية استعماله ثم إرجاع له أو الاطلاع عليه فقط فلا يعتبر سارقا، لأنه لم يقصد نقل الملكية له كالذي يأخذ كتبا من زميله لقراءته ثم يرجعه له أو الذي يأخذ سيارة صديقه للنزهة ثم يرجعها فلا يعتبر سارق.[2]

ويتطلب العنصر المعنوي في الاختلاس أن يكون نية لدى الجاني في تملك الشيء المختلس وحيازته الحيازة الكاملة وهو ما أيدته محكمة النقض الفرنسية في قضية "lagbax " الذي كان يعمل موظفا في شركة وقام بتصوير مستندات سرية دون رغبة صاحبها وذلك بنية تملك هذه المستندات لمصلحته الشخصية.[3]

ب- التسليم في المعلوماتية

يعتبر من القواعد العامة أن الاختلاس في جريمة السرقة لا يقع إذا كان المال في حوزة الجاني أو سلم إليه من مالكه، وتتحقق به الحيازة وليس وضع اليد فقط، وفي هذا المقام سنحاول

[1]- انسام سمير الطاهر، المرجع السابق، ص190.

[2] -http://www.4algeria.com

[3]- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، ط2، الدار الجامعية للنشر والتوزيع الإسكندرية، 1992، ص62.

توضيح التسليم الذي ينفي الاختلاس في المعلوماتية، انقسمت الآراء القائلة فيما يتعلق بالتسليم فيما يخص المعلوماتية وأثره بال نسبة لجريمة السرقة، بينما كانت تلك الآراء الفقهية والقضائية تتعلق بالتسليم الصادر من الحاسب الآلي لتوزيع النقود، في حين أننا نود أن نتحدث عن تسليم المعلومات الموجودة داخل الحاسوب لمختلسها ذلك يقتضي من وجهة نظرنا تطبيق القواعد العامة المتعلقة بالتسليم في جريمة السرقة التقليدية.[1]

أما العنصر الشخصي في الحيازة أي عدم....حائز الشيء في الحيازة المعلوماتية والمترتبة عن الاختلاس فتسعى أن مالك المعلومة لم يرضى باختلاس ما يخصه ولم يرضى بنقلها، وان افترض التسليم المسبق للشيء المعلوماتي فقد لا تعني الرضا بالاختلاس فقد كان ذلك يقصد تمكين اليد العارض وهذا لا ينفي ركن الاختلاس و يتعين القول أنه لا مخالفة لمبادئ التفسير التي تحكم نصوص العقابية أو مبدأ المشروعية ذلك لان الثورة المعلوماتية أدت إلى ظهور أنماط جديدة من الجريمة تعجز النصوص العقابية.[2]

2- الركن المعنوي

إن الركن المادي غير كافٍ وحده لتحقيق الجريمة ،أيا كان هذا الركن يؤدي إلى تحقيق نتيجة معينة أو يكتفي بالسلوك المجرد فلابد أن يتواجد إلى جانبه الركن المعنوي، ويتمثل هذا الركن بعنصري العلم والإرادة، فلا يسال الشخص عن أية جريمة مالم تكن هناك علاقة بين ماديات الجريمة ونفسيته، ويشكل هذا ضمانا لتحقق العدالة[3]، وعليه سنبين عناصر الكن المعنوي.

أ- العلم

هو إدراك الأمور على نحو مطابق للواقع، يسبق الإرادة و يتخذ القصد الجنائي عدة صور منها القصد العام و القصد الخاص، فالقصد الجنائي العام: هو الهدف الفوري والمباشر للسلوك

[1]- رابحي عزيزة، الاسرار المعلوماتية وحمايتها الجزائية، اطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة ابي بكر بالقايد، تلمسان، 2018/2017، ص196.

[2]- شول بن شهر، الحماية الجنائية للتجارة إلكترونية، أطروحة دكتوراه في الحقوق، قسم الحقوق كلية الحقوق والعلوم السياسية ،جامعة محمد خيضر، بسكرة،2010 - 2011،ص114.

[3]- محمود نجيب حسني، شرح قانون العقوبات، القسم العام، ط2 ،دار النهضة العربية، القاهرة، 1984، ص201.

الإجرامي وينحصر في حدود تحقيق الغرض من الجريمة أي لا يمتد لما بعدها، القصد الجنائي الخاص: هو ما يتطلب توافره في بعض الجرائم فلا يكفي بمجرد تحقيق الغرض من الجريمة بل هو ابعد من ذلك أي انه يبحث في نوايا المجرم.[1]

ان المجرم المعلوماتي يتوجه من أجل ارتكاب فعل غير مشروع أو غير مسموح عليهم بأركان الجريمة و بالرغم من أن بعض المخترقين يبررون أفعالهم بأنهم مجرد فضوليون و أنهم قد تسللوا صدفة، فلا انتفاء العلم كركن للقصد الجنائي، كان يجب عليهم أن يتراجعوا بمجرد دخولهم و لا يستمروا في الاطلاع على اسرار الافراد والمؤسسات لأن جميع المجرمين و الأشخاص الذين يرتكبون هذه الأفعال يتمتعون بمهارات عقلية و معرفية كبيرة تصل في كثير من الأحيان الى حد العبقرية، فالقصد الجنائي متوافر في جميع الجرائم الالكترونية دون أي استثناء و لكن هذا لا يمنع أن هناك بعض الجرائم المعلوماتية، ليست كيانا مادياً خالصا قوامه السلوك الاجرامي واثاره، فلا يكفي مجرد المادي للفعل او الامتناع المخالف للقانون الى شخص معين ليكون ذلك الشخص مسؤولاً جنائياً او ان تكون هناك ثمة جريمة، وانما يجب ان تكون الى جانب هذه العلاقة المادية علاقة اخرى ذات خصائص نفسية.[2]

ان تجتمع العناصر النفسية للجريمة في ركن يختص بها وهو الركن المعنوي لذا فان الركن المعنوي يقوم على الصلة بين النشاط الذهني والنشاط المادي فأول ما يستلزمه أن يكون النشاط المادي ثمرة ارادة فان لم يكن كذلك فلا يكون مجرماً ولو انه بنى على توجيهها ضرر كما ان توجيه الارادة الى السلوك لا يكفي لإقامة الركن المعنوي بل يجب ان تكون هذه الارادة اجرامية، أي ان تكون تربط الفاعل بالواقعة الاجرامية، والاثم هو اساس الركن المعنوي وبالتالي فهو أساس المسؤولية الجنائية و يأخذ الركن المعنوي للجريمة احدى صورتين هما:- القصد الجنائي والخطأ غير العمدي .وعلى هذا النحو فأن كلاً من القصد الجنائي والخطأ غير العمدي يقوم

[1]- انسام سمير الطاهر، المرجع السابق، ص142.
[2]- يوسف حسن يوسف، الجرائم الدولية للإنترنيت، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2011، ص4.

على اتجاه إرادي منحرف نحو مخالفة القانون، وبعبارة أخرى فأنهما ينطويان على ارادة اثمها القانون بالنظر الى الوجهة التي انصرفت اليها.[1]

ب- الارادة

وهي اتجاه لتحقيق السلوك الاجرامي، ولما كانت الارادة عنصراً لازماً في الخطأ لزومه في العمد، لذا فان انتفائها يعني تخلف الركن المعنوي من أساسه فالفاعل اذا لم يكن مريداً مختاراً لسلوكه كالمكره فان المسؤولية الجنائية تنتفي عنه في جميع اشكالها، اذا كان اتجاه الارادة الى السلوك هو شرط عام ومشترك في سائر صور الركن المعنوي فان تخلف ارادة النتيجة هو من الامور الجوهرية التي تميز الخطأ عن العمد، فالعمد لا يقوم الا اذا اتجهت ارادة الجاني الى النتيجة سواء بطريق مباشر او غير مباشر، اما الخطأ فمن شروطه ان تتخلف الارادة عن النتيجة تماما.[2]

ثالثا: الجزاءات المقررة لجريمة السرقة المعلوماتية

تعددت نقاشات الفقه وقرارات القضاء في طرح الحلول والاستنتاجات حول مدى أمكانية تطبيق النصوص التقليدية الواردة في قانون العقوبات على جريمة السرقة المعلوماتية، وعليه فأننا سنعرض ابتداء ما توصل إليه الفقه والقضاء من تحليل ونتائج، ثم نبين موقف التشريع المقارن في معالجة هذا النوع من الجرائم.[3]

1- موقف الفقه والقضاء من جريمة السرقة المعلوماتية

يتناول الفقه والقضاء سؤالاً يعبر عن حقيقة المشكلة وهو: هل أن سرقة معطيات الحاسوب المتحققة في جريمة السرقة الالكترونية تدخل في نطاق السلوك الإجرامي المكون لجريمة السرقة التقليدية أم لا؟

[1]- أحمد فتحي سرور ، الوسيط في قانون العقوبات، القسم العام ، دار النهضة العربية ، القاهر ،2009، ص346.

[2]- عوض محمد عوض، قانون الإجراءات الجنائية، ج1 ،مؤسسة الثقافة الجامعية، القاهرة، 1989 ،ص258.

[3]- انسام سمير طاهر، المرجع السابق، ص144.

قد يبدو هذا السؤال من قبيل الأمور الغريبة ذلك أنه من المعلوم وحسب المبادئ التقليدية المستقرة أن المعلومة بمفردها تواجه بمنأى عن الدعامة المادية المثبتة عليها، مثل الأفكار والحقوق وهي أشياء غير قابلة ، للسرقة وفقاً للقواعد العامة، لأن الشيء موضوع السرقة يجب أن يكون مادياً ملموساً يسمح بإنتقاله من حيازة مالكه إلى حيازة الجاني عن طريق ركن الاختلاس[1]، ولكن عند عد المال المعلوماتي محلاً لجريمة السرقة يجب التفرقة بين أمرين هما:

– **الأول:** أن المال المعلوماتي المادي فقط هي الآت وأدوات الحاسب وعليها المعلومات، فإذا وقعت جريمة السرقة عليها فأنها تقع على مال مادي ويمكن القول بانطباق جريمة السرقة التقليدية عليه.

– **الثاني:** فهي سرقة المعلومات بذاتها من البرنامج، أي سرقة المحتوى، وهذا الغرض هو الأهم والغالب في هذه السرقة فهل نعدها سرقة أم لا، وبالتالي ينطبق النص المتعلق بالسرقة أم لا؟[2]

ونتيجة لذلك فقد أنقسم الفقه إلى رأيين مؤيد ومعارض حول مدى انطباق النصوص التقليدية على سرقة جريمة السرقة الالكترونية، وعليه سوف نتناول أسانيد كل منهما في رأيه.

الاتجاه الأول: يؤيد أصحاب هذا الاتجاه تطبيق أحكام جريمة السرقة التقليدية على الجرائم الواقعة على المعلومات الموجودة داخل جهاز الكمبيوتر.[3]

الاتجاه الثاني: ويقوم هذا الاتجاه على عدم صلاحية المعلومات لتكون محلاً لجريمة السرقة الالكترونية على الرغم من وجود الفعل الخارجي الملموس الذي يتمثل بفعل النسخ أو القطع غير المصرح به أو غير المشروع ويسير على هذا الاتجاه الفقه الانكليزي الذي يرى أن فكرة قابلية

[1]- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشرع لشبكة الإنترنت، ط2 ،دار النهضة العربية، القاهرة، 2009 ،ص204.

[2]- هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، بحث منشور في مجلة العلوم القانونية والاقتصادية، العدد2، 1993، ص52.

[3]- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، ط2، دار الجامعة الجديدة للنشر، القاهرة، 1997، ص50.

سرقة معلومة معينة تبدو للوهلة الأولى فكرة غير معقولة، لأن السرقة وفقاً للقانون الإنكليزي تفهم على أنها: (أخذ الشيء الملموس من الغير من دون وجه حق وبنية حرمانه منه وإلى الأبد).[1]

2- موقف التشريعات المقارنة من جريمة السرقة المعلوماتية

على صعيد التشريع الفرنسي، نص مشروع قانون العقوبات الجديد على تجريم سرقة المال المعلوماتي متمثلاً في المعلومات والبرامج، وذلك بموجب الفقرة الأولى من المادة /307، وقد أستعمل المشرع الفرنسي لفظاً فنياً ليعبر عن اختلاس المعطيات بشكل دقيق يتناسب مع جدية الموضوع وهو لفظ التقاط (capter) إذ تقرر المادة سابقة الذكر أن (كل من ألتقط بطريق الاختلاس والتحايل برنامج أو معلومة أو أي عنصر من عناصر نظام المعالجة الآلية للبيانات، يعاقب بالحبس مدة ثلاث سنوات وبغرامة مقدارها مليون فرنك).[2]

وعلى الصعيد الفيدرالي في الولايات المتحدة فقد صدر قانون جرائم الكمبيوتر الفيدرالي لسنة 1986، لمواجهة التطور السريع في مجال السرقة المعلوماتية، كما وفرت القوانين الفيدرالية أيضاً حماية للعلامات التجارية وحقوق المؤلف من انتهاك حرمتها، أضافة إلى توسع القضاء في مجال بعض الأفعال وطبق أحكام السرقة على اختلاس المعلومات الحكومية الموجودة على قاعدة خدمات حكومية وانتهت أحكام اخرى إلى تطبيق، أحكام السرقة على نسخ بعض برامج الكمبيوتر، وفي كندا نص قانون العقوبات الكندي في الفقرة الثانية من المادة/301 على معاقبة ((كل من حصل بسوء نية بشكل مباشر أو غير مباشر عن طريق جهاز كهربائي أو ممغنط أو باستخدام جهاز سمعي أو بواسطة جهاز آلي أو غيره، على الخدمات التي يقدمها الحاسب الآلي أو باستخدام هذا الأخير بقصد ارتكاب جريمة))، ويضفي هذا النص الحماية الجنائية على معطيات الحاسوب بوصفها أحدى أهم خدمات الحاسوب، سواء تم الفعل بصورة مباشرة بالتماس مع الحاسوب أو بصورة غير مباشرة عن طريق الاستعانة بأي جهاز يمكن الفاعل من التقاط المعطيات أو أية خدمات أخرى.[3]

[1]- أحمد كيلان عبد الله صكر، الجرائم الناشئة عن إساءة استخدام الحاسوب، رسالة ماجستير، مقدمة إلى كلية القانون، جامعة بغداد، 2002 ،ص59.

[2]- هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، بحث منشور في مجلة العلوم القانونية والأقتصادية، العدد2، 1993، ص70.

[3]- أحمد كيلان عبد الله صكر، المرجع السابق، ص63.

كما صدرت تشريعات عربية تتعلق بتطبيقات استخدام الحاسب الآلي وتجريم الاعتداء على المعلومات، من ذلك مشروع قانون مكافحة جرائم تقنية المعلومات الاتحادي في دولة الأمارات العربية المتحدة، إذ نصت (المادة/10 (من مشروع القانون الإماراتي المذكور على أنه ((كل من توصل عن طريق الشبكة المعلوماتية أو أحدى وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند...يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن ثلاثين ألف درهم أو بإحدى هاتين العقوبتين)).[1]

كما نصت (المادة/4) من قانون مكافحة جرائم المعلوماتية السعودي على أنه ((يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أي من الجرائم المعلوماتية الآتية: الإستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند...)).[2]

الفرع الثاني: جريمة التزوير المعلوماتي

مع الانتشار الواسع الذي عرفه الحاسب الآلي، إذ أصبح يحل محل الأوراق (المحررات أو الوثائق) في جل مجالات تضم المعالجة الآلة للمعلومات ومع تزايد الاعتداءات الواقعة علي المعطيات المخزنة داخل الحاسب الآلي والتي تمس الأفراد في حقوقهم وأموالهم و يمس مراكز الأفراد ، ومع تزايد فرص الأشخاص للعبث والتلاعب في معطيات الحاسب بتبديلها وتغيرها بالشكل الذي يفقد الثقة بالتقنية.[3]

اولا: تعريف الجريمة التزوير المعلوماتي

تعتبر جريمة التزوير المعلوماتي احدى الجرائم الاكثر تعقيدا لاتصالها بالثقة العامة لذلك سوف نتطرق الى تعريف التزوير فقهيا وقانونيا ثم تعريف جريمة التزوير المعلوماتي على النحو الاتي:

[1]- عبد الفتاح بيومي الحجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الكتاب للنشر، الإسكندرية، 2007، ص420.

[2]- عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت في التشريعات العربية، ط1، دار النهضة العربية، القاهرة، بلا سنة طبع، ص249

[3]- أحمد خليفة الملط ، المرجع السابق ، ص425.

1- **التزوير فقهاً:** إن التزوير هو عملية مادية وصورة من صور الكذب التي يقوم بها شخص بغرض تغيير الحقيقة في محرر أو سند عمومي أو سند رسمي بإحدى الطرق المحددة في قانون، وشأنه إلحاق الضرر بالحقوق أو المراكز القانونية لاحد أو بعض أطراف السند أو المحرر محل الادعاء بالتزوير.[1]

2- **لتزوير قانوناً:** عرف قانون العقوبات الأردني رقم (16) لسنة 1966 في المادة (266) بأن التزوير(هو تحريف مفتعل للحقيقة في الوقائع والبينات التي يراد اثباتها بصك او مخطوط يحتج بهما أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي).[2]

وعرف القانون العقوبات العراقي رقم (111) لسنة 1969 في المادة (236) بان التزوير(هو تغيير الحقيقة بقصد الغش في سند أو وثيقة أو أي محرر أخر بإحدى الطرق المادية أو المعنوية التي بينها القانون تغييرا من شأنه إحداث ضرر بالمصلحة العامة أو بشخص من الأشخاص).[3]

3- التزوير المعلوماتي: هو تغيير الحقيقة يرد على مخرجات الحاسوب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطابعة، أو كانت مرسومة عن طريق رسم[4]، كما يعرف بانه تغيير الحقيقة في المحررات المعلوماتية بأي وسيلة وذلك بغية استعماله.[5]

ثانيا: اركان جريمة التزوير المعلوماتي

التزوير المعلوماتي شأنه شأن بقية الجرائم يتكون من ركنين هما الركن المادي والركن المعنوي.

[1]- عبد العزيز سعد، جرائم التزوير وخيانة الأمانة واستعمال المزور، الطبعة الاولى، دار هومة، الجزائر، 2005، ص14.
[2]- انظر للمادة (266)، من قانون العقوبات الاردني، رقم(16)، لسنة 1960.
[3]- انظر للمادة (236)، من قانون العقوبات العراقي، رقم (111)، لسنة 1969.
[4]- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنيت، المرجع السابق ، ص170.
[5]- عمر عبد السلام حسين الجبوري، جريمة التزوير الالكتروني في التشريع الاردني (دراسة مقارنة)، رسالة ماجستير في القانون العام، كلية الحقوق ، جامعة الشرق الاوسط، الاردن، 2017، ص16.

1- الركن المادي لجريمة التزوير المعلوماتي

يتمثل الركن المادي لجريمة التزوير المعلوماتي في تغيير الحقيقة في محرر المعلوماتية والنتيجة المترتبة عن تغير هذه الحقيقة أي الضرر الناتج، إذ يقصد بفعل تغيير الحقيقة بصدد جريمة تزوير المستندات المعالجة آليا كل تغيير للحقيقة أو تحريف لها يرد علي محتوى مستند أصلي حقيقي معالج آليا، بمعني انه لا يتصور وقوع فعل تغيير الحقيقة من خلال طرق التزوير المعنوية والتي كما هو معروف لا تتحقق إلا أثناء تكوين المستند بالنسبة للجريمة محل بحث.[1]

بينما من المتصور وقوع فعل تغيير الحقيقة بالنسبة لهذه الجريمة من خلال طرق التزوير المادية، ولكن شرط أن يكون التزوير لاحقا علي نشأة المستند الأصلي والحقيقي المعالج اليا فلا تتحقق تلك الجريمة من خلال فعل تغيير الحقيقة باستخدام طريقة تزوير مادية أثناء نشأة المستند علي خلاف جريمة التزوير التقليدية، كما لا تتحقق تلك الجريمة من خلال اصطناع لا أساس له أو من مجرد تصوير أو نسخ مستند أصلي موجود.[2]

والتزوير في مجال المعلوماتية يخضع لما يخضع له التزوير في مجال المحررات العادية فبتالي لها نفس أركان وعناصر جريمة التزوير في المحررات، بمعني يلزم لتحققها توافر محرر أو أي دعامة أخرى تحتوي تغييرا عن الفكر و يترتب عنه ضرر للغير.

محل التزوير لا يقتصد علي ما يصدق عليه وصف الكتابة فقط وإنما يمتد ليشمل أيضا أي دعامة أخرى تحتوي علي الفكر وتعبير دعامة أخرى كل الدعامات المستخدمة في مجال الحاسب الآلي والتي يسجل عليها تعبيرا عن الفكر الصحيح لان يرد عليه التزوير بان يكون ليس لمجرد سرد للوقائع أو بيانات،تعبير عن إدارة ولا يصدق هذا علي المستندات المعالجة آليا بل يشمل البرامج أي كان توقعها والمعلومات المسجلة علي أقراص أو شرائط ممغنطة ولو لم يتم معالجتها بعد،أولم يتم إدخالها بعد إلى جهاز الحاسب الآلي،وهكذا يتضح بان التعديل الجديد الذي جاء به التشريع الفرنسي أفضل من الوضع السابق،الذي كان يقتصر فيه التزوير علي

[1]- امال دكومي، الجريمة المعلوماتية واثارها على النمو الاقتصادي، مذكرة ماستر في القانون الجنائي للأعمال، جامعة العربي بن مهدي، كلية الحقوق والعلوم السياسية قسم الحقوق، ام البواقي، 2015/2014، ص42.

[2]- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، ط3، الدار الجامعية للنشر و التوزيع، الاسكندرية، 1999، ص151.

المستندات المعالجة آليا فقط ،ويتعين الصعوبات للتمييز بين ذلك المستندات وغيرها مما لا يخضع لتلك المعالجة.[1]

بالنسبة للضرر في جريمة التزوير فهو عنصر جوهري ويرجع البعض أن الضرر في جريمة التزوير هو مضمون لمصطلح اللامشروعية، ويكفي احتمال الضرر ولقيام جريمة التزوير، وكذلك لا يتطلب القانون وقوع الضرر فعلا، وإنما يكتفي لكونه محتمل الوقوع، وهو لا يكون له محل لا باستعمال المحرر المزور، جاعلا من هذا الاستعمال جريمة قائمة بذاتها وتكون العبرة في تقدير احتمال الضرر إنما نكون بالوقت الذي وقع فيه تغيير الحقيقة في المحرر، فإذا كان الضرر محتملا في هذا الوقت قامت الجريمة ولا يعفى الجاني من العقاب أنيطرأ بعد ذلك سبب ينفي كل احتمال للضرر كإعدام المحرر، ومسالة الضرر فهي تتعلق بالوقائع، ولذلك يفصل فيها قاضي الموضوع حسبما يراه من ظروف كل دعوى.[2]

2- الركن المعنوي لجريمة التزوير المعلوماتي

جريمة التزوير المعلوماتي هي من الجرائم العمدية لقيام هذه الجريمة البد من توفر القصد الجنائي العام و القصد الجنائي الخاص.

بالنسبة للتزوير المعلوماتي فان الركن المعنوي لهذه الجريمة المعلوماتية هو ذات المدلول في جريمة تزوير المحررات و هو ما يتخذ صورة القصد الجنائي العام بعنصرية العلم و الإدارة إضافة إلى ذلك القصد الخاص فيجب أن يتصرف علم الجاني إلى انه يغير الحقيقة في مستند معلوماتي بإحدى الطرق المحددة في القانون وان تتجه إرادته إلى فعل تغيير الحقيقة.[3]

وكذلك يجب أن يعلم الجاني أنه يغير الحقيقة في محرر بإحدى الطرق التي نص عليها ذا كان لا يعلم ذلك انتفى القصد الجنائي لديه حتى لو كان جهله ارجعاً إلى إهماله في التأكد من ذلك وهذا العلم مفترض فلا يدفع مسئوليته عن ذلك بجهله، +كما ينبغي أن يعلم الجاني أن فعله

[1]- جميل عبد الباقي الصغير، الانترنيت و القانون الجنائي، ط 1، دار النهضة العربية، القاهرة، 2000،ص155.

[2]- ايهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، دار الجامعة الجديدة للنشر، الاسكندرية، 2008، ص56-57.

[3]- حسام محمد نبيل الشنراقي، جرائم الاعتداء على التوزيع الالكتروني، ط1، دار الكتب القانونية، مصر، 2013، ص277.

يسبب ضررا فعلياً أو محتملا للغير فإذا انتفى ذلك انتفى القصد ايضاً، ولا يكفي توفر الامرين السابقين بل يلزم بالإضافة إلى ذلك أن تتجه نية الجاني إلى استعمال المحرر فيما زور من أجله حتى ولو لم يستعمله ولا فائدة من نفي الجاني لهذه التهمة بدفع أنه لم يحصل على فائدة من جراء عمله.[1]

ثالثا: الجزاءات المقررة لجريمة التزوير المعلوماتية

لم تكن الحماية الجنائية للجرائم المعلوماتية قبل أربعة عقود على الحالة التي هي عليها الان، فلم يرى المشرعون في بادئ الامر حاجة تدعوا إلى تميز جرائم المعطيات بصفة عامة وجريمة التزوير المعلوماتي بصفة خاصة عن غيرها من الجرائم، فاحتفظوا بالنصوص التقليدية، وتعددت عندها محاولات الفقه و القضاء لتطويع تلك النصوص لتشمل هذه الجرائم لكن الواقع كشف عن عم جدوى هذا الحل مما استدعى المشرعين لوضع نصوص خاصة لتلك الجرائم كل واحدة على حدى.

1- موقف التشريعات الأوربية و الأمريكية في مكافحة التزوير المعلوماتي

لقد أدى التطور التقني إلى ظهور جرائم جديدة لم يتناولها القانون الجنائي التقليدي، مما أجمع معه مشرعي القانون الوضعي في الدول المتقدمة على جسامة الجريمة المعلوماتية و التهديدات التي يمكن أن تنشأ عن استخدام الحاسب و شبكة الأنترنت، وطبقا لمبدأ الشرعية الذي يقضي بأن "لا جريمة ولا عقوبة إلا بنص قانوني " ولمواجهة الخطر المحدق و الخسائر الفادحة التي تسببها جرائم الاعلام الالي، لأجل هذا سنت العديد من الدول المتقدمة قوانين جنائية خاصة أو عدلت قوانين العقوبات لديها بما يكفل مواجهة جرائم الاعلام الالي الواقعة عمى معطيات الحاسوب من بيانات و برامج.[2]

[1]- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، الطبعة الاولى، مكتبة الآلات الكاتبة، أسيوط، 1995، ص258.

[2]- يوسف مناصرة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، رسالة ماجستير، جامعة الجزائر، كلية الحقوق، 2009/2008، ص89-90.

أ- موقف التشريع الفرنسي

اهتمت فرنسا بتطوير قوانينها الجنائية للتوافق مع المستجدات الاجرامية، فكانت أول المحاولات من طرف وزيرها للعدل وذلك سنة 1985 عندما تقدم بمشروع قانون عقوبات جديد أضاف بموجبه بابا رابعا للكتاب الثالث منه بعنوان "الجرائم في المادة المعلوماتية " يتكوف من ثمانية مواد من 1/307 إلى 8/307 تناولت بالتجريم الموضوعات التالية:

- التقاط البرامج أو المعطيات أو أي عنصر آخر من النظام المعلوماتي.

- استخدام أو نقل أو انتاج برامج أو معطيات أو أي عنصر من عناصر النظام بدون موافقة من لهم الحق.

- تخريب أو تعييب كل جزء من نظام المعالجة الالية للمعلومات أو عرقلة أدائه لوظيفته.

- الحصول أو السماح بالحصول على فائدة غير مشروعة عن طريق الاستخدام الغير مشروع لنظام المعالجة الالية للبيانات.[1]

لكن هذا المشروع لم يجد سبيله للتطبيق، أما المحاولة التي كتب لها النجاح فقد كانت في الخامس أغسطس عام 1986 عندما تقدم باقتراح مشروع قانون الغش المعلوماتي، هذا الاقتراح حاول تعديل وتطويع بعض النصوص القائمة في قانون العقوبات والتي تناولت جرائم تقليدية كالسرقة و خيانة الامانة و التزوير و الاتلاف والاخفاء، وذلك لتشمل العدوان على المعلوماتية وحدث أن تعددت مناقشات هذا المشروع في البرلمان الفرنسي، وطال أمدها حتى استغرقت عام ونصف وأسفرت في النهاية عن قانون اختلف تماما عن ذلك الذي قدم أول مرة، بل تشابه إلى حد كبير مع المشروع الاول الذي تقدم به وزير العدل الفرنسي عام 1985.[2]

أما المحطة الثانية من محطات التجريم المعلوماتي فكانت عام 1994 عندما تم تعديل قانون العقوبات الفرنسي، وقد استخدم هذا التعديل مصطلح " الغش " في الجرائم السابقة

[1]- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الالي، ط3، المرجع السابق، ص39.
[2]- أحمد طه، الجرائم الناشئة عند استخدام الحاسب الالي دراسة مقارنة، دار النهضة العربية، القاهرة، 2000 ،ص261.

واستغنى عف مصطلح " دون مراعاة حقوق الغير " كما أن هذا التعديل مس المادة 1/441،[1] فطور من جريمة التزوير المعلوماتي، لتصبح جريمة تزوير المستندات المعلوماتية واستعملها بعد ما كانت جريمة تزوير المستندات المعالجة آليا فحسب، وبالتالي أصبح نص المادة 1/441 يستوعب حالات التزوير العادي في المحررات إلى جانب تزوير الوثيقة المعلوماتية، وذلك بتجريم التزوير الواقع عمى وثيقة معلوماتية مطبوعة على سند أو دعامة.[2]

ومن خلال ما سبق يتضح لنا مدى استيعاب القانون الفرنسي لجريمة التزوير المعلوماتي حيث قام المشرع الفرنسي بتعديل النص الخاص بجريمة التزوير فأصبحت تشمل التزوير في المحررات والمستندات المعلوماتية كوف أن هذه الجريمة ال تدخل في نطاق جرائم الاعتداء على نظام المعالجة الالية للمعطيات لاختلاف المصلحة المحمية.

ب- موقف التشريع الكندي

تعتبر كندا من بين الدول الكبرى التي يستعمل مواطنيها و مؤسساتها الحاسوب و الانترنت مما جعل المشرع الكندي يعدل قانون العقوبات عام 1985 فعاقب استنادا إلى التعديل كل من أوقف أو اعترض بطريق الغش أو بدون وجه حق أو تسبب في إعاقة أو عرقلة أي من وظائف الحاسوب، كما عاقب على الحصول بالغش على خدمات الحاسوب وعلى استخدام أو التسبب في استخدام الحاسوب لارتكاب أي من الافعال المذكورة، وعاقب في ذات التعديل على إتلاف المعطيات وحدد الافعال المنطوية تحت هذا الوصف و عدل القانون تعريف الوثيقة التقليدية المعتبر في جريمة التزوير لتشمل أية مادة يتم التسجيل عليها من قبل انسان أو حاسوب لغاية تجاوز مشكلة مفهوم المحرر المادي و تطلبه كمحل لجريمة التزوير.[3].

[1]- لمادة 1/441 من قانون العقوبات الفرنسي "يعد تزويرا كل تغيير تدليسي للحقيقة ، يكون من طبيعته أن يسبب ضررا، ويتم بأي وسيلة مهما كانت، في محرر أو أي سند للتعبير عن الرأي والذي يكون موضوعه أو الذي من الممكن أن يكون له أثر في انشاء دليل على حق أو فعل تكون له نتائج قانونية ، بيدف الاعتراف".

[2]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، المرجع السابق، ص 204.

[3]- يوسف مناصرة، المرجع السابق، ص104.

ويتضح من خلال هذا القانون مدى مواكبة التشريع الكندي للجرائم المعلوماتية و مكافحته للتزوير المعلوماتي حيث جاء شاملا للجرائم الواقعة على نظام المعالجة الالية للمعطيات كما أنه نص على جريمة التزوير المعلوماتي.

2- موقف الدول العربية في مكافحة التزوير المعلوماتي

إن ما كان سائدا عند القوانين العرب هو أن هناك فراغ قانوني على الصعيد العربي يحول دون مجابهة جرائم المساس بأنظمة المعالجة الالية للمعطيات، لكن هذا التصور صار اليوم غير ذي جدوى، ولتأكيد ذلك سوف نحاول إيراد بعض نماذج القوانين العربية الخاصة بمكافحة و محاربة جرائم المساس بأنظمة المعالجة الالية للمعطيات مثل قانون الامارات العربية المتحدة أي القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات، والقانون المغربي لسنة 2003.[1]

أ- موقف التشريع الاماراتي

تعد دولة الامارات العربية المتحدة أول دولة خليجية أصدرت قانونا مختصا في مكافحة جرائم المعلومات من الناحية التشريعية حيث أصدرت عام 2002 قانون التوقيع الالكتروني والتجارة، وقد قضى هذا القانون بمنع مزودوا خدمات الانترنت من كشف أية معلومات يحصلون عليها في أثناء تزويد الخدمة[2]، ادراكا لاهمية مكافحة جرائم تقنية المعلومات و حرصا منه لتغطية الفجوة التشريعية في مجال الانترنت و المعلوماتية أصدر المشرع الاماراتي القانون الاتحادي الاماراتي رقم 2 لسنة 2006 لمكافحة جرائم تقنية المعلومات، ويعتبر هذا القانون أحدث و أشمل التشريعات العربية في هذا المجال.

هذا وقد نص القانون الاتحادي 2 لدولة الامارات العربية المتحدة على جريمة التزوير المعلوماتي في مادته الرابعة والتي تنص على ما يلي: " يعاقب بالسجن المؤقت كل من زور

[1]- ياسين بوعروة، جريمة التزوير المعلوماتي، مذكرة ماستر في القانون الجنائي للاعمال، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة العربي بن مهدي، ام البواقي، 2014/2013، ص50.
[2]- يوسف مناصرة، المرجع السابق، ص120.

مستندا من مستندات الحكومة الاتحادية او المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحمية معترفاً بو قانونًا في نظام معلوماتي.

وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير فيما عدا ذلك من المستندات إذا كان من شأن ذلك إحداث ضرر.

ويعاقب بالعقوبة المقررة لجريمة التزوير حسب الاحوال من استعمل المستند المزور مع علمه بتزويره[1]."

ومن خلال هذا يتضح لنا مدى مسايرة القانون الاماراتي لتقنية المعلومات من خلال هذا القانون الذي جاء لمكافحة و مواجهة والحد من الجرائم المعلوماتية، كما أن هذا القانون جاء شاملا لجميع الجرائم بما فيها جريمة التزوير المعلوماتي وبالتالي يمكن القول أن هذا القانون سد الثغرة التشريعية في مجال المعلوماتية في القانون الاماراتي.

ب- موقف التشريع المغربي

اتخذت الجريمة المعلوماتية في المملكة المغربية خلال العقود الاخيرة صورا متعددة مما دفع المشرع المغربي إلى سن قانون لسد الفراغ التشريعي في مجال مكافحة الجرائم المعلوماتية، و جاء القانون 07/03 لشأن اتمام مجموعة القانون الجنائي فيما يتعلق بالأخلال بسير نظم المعالجة الالية للمعطيات و يحتوي القانون على تسعة فصول من الفصل 3-607 إلى الفصل 11-607 من مجموعة القانون الجنائي المغربي.[2]

و لمواجهة ظاهرة التزوير المعلوماتي جرم المشرع المغربي فعل تزوير أو تزييف الوثائق المعلوماتية إذا أدى ذلك إلى احداث ضرر للغير، بحيث أن الفصل 7-607 نص على ما يلي :

[1]- انظر للمادة (4)، من قانون الاتحادي رقم 2 لمكافحة جرائم تقنية المعلومات لدولة الامارات العربية المتحدة ، لسنة 2006.

[2]- ياسين بوعروة، المرجع السابق، ص52.

"دون الاخلال بالمقتضيات الجنائية الاشد، يعاقب بالحبس من سنتين إلى خمس سنوات و بغرامة مالية من 10000إلى 1000000 درهم كل من زور أو زيف وثائق المعلوماتية أيا كان شكلها إذا كان من شأن التزوير أو التزييف إلحاق ضرر بالغير.

دون الاخلال بالمقتضيات الجنائية الأشد، تطبق نفس العقوبة على كل من استعمل وظائف المعلوماتية المشار إليها في الفقرة السابقة وهو يعلم أنها مزورة أو مزيفة".[1]

لقد استغل المشرع المغربي فرصة اصدار تشريع معلوماتي، ووضع نصا قانونيا يجرم فيه التزوير المعلوماتي، لأنه قبل صدور هذا القانون لم يكن بالإمكان في المغرب الحديث عن تزوير الا في ظل كتابة تقليدية، أما الان فإن القضاء المغربي يممك آلية قانونية يمكن بموجبها متابعة الجاني الذي زور وثائق معلوماتية.[2]

المطلب الثاني: الجرائم الواقعة بواسطة النظام المعلوماتي

الجرائم الواقعة بواسطة النظام المعلوماتي كثيرة و عديدة و سوف نسلط الضوء على جريمتين، جريمة الاتلاف المعلوماتي و جريمة النصب المعلوماتي باعتبار هاتين الجريمتين الاكثر شيوعا في الفترة الاخيرة في المجتمع إضافة إلى تعدد طرقها و وسائلها.

الفرع الاول: جريمة الاتلاف المعلوماتي

تتضمن نضم المعالجة الالية للمعلومات عناصر مادية يمكن أن تكون ملكا للغير كوسائل إدخال واخراج التي يمكن أن تتعرض للإتلاف إي إزالة عن طريق الغش لوثيقة أو سند أو أموال منقولة، كما يقع على و أشياء مادية أخرى معلوماتية، الشاشة الفارة و يمكن أن تكون هده الاخيرة ملكا للغير و في هذه الحالة يرى معظم الفقه انه يمكن تطبيق النصوص التقليدية للإتلاف باعتباره ملا مملوك للغير، أما في حالة ما إذا وقع على المكونات المعنوية للحساب الالي و التي يقصد بها العناصر التي تتكون منها نظام الحاسب الالي كالمعلومات وبيانات و

[1]- انظر للمادة (7-607)، من القانون رقم 07/03 المتمم لمجموعة القانون الجنائي المغربي فيما يتعمق بالأخلال بسير نظم المعالجة الالية للمعطيات.
[2]- محمد جوهر، خصوصية زجر الاجرام المعلوماتي، المجلة المغربية للقانون والاقتصاد والتسيير، العدد52، المغرب، 2006.

هنا يثار التساؤل هل يمكن تطبيق النصوص التقليدية لجريمة الاتلاف المعلوماتي مما يدفعنا إلى دراسة تعريف هذه الجريمة و بيان الركن المادي و المعنوي و العقوبات المقررة لجريمة الاتلاف المعلوماتي.

اولا: تعريف جريمة الاتلاف المعلوماتي

لقد تعددت التعاريف بخصوص اتلاف المعطيات المعلوماتية وعليه سنتطرق الى التعريف اللغوي و التعريف الفقهي.

1- التعريف اللغوي:

"كلمة الاتلاف منشقة من كلمة التلف، التي تعني الهلاك وذهبت نفس تلفا أي هدرا".[1]

2- التعريف الفقهي:

يعرف الاتلاف بوجه عام انه:" اخراج الشيء من ان يكون منتفعا به منفعة مطلوبة منه عادة[2]، اما الاتلاف المعلوماتي فيقصد به:" كل فعل الغاية من القيام به تدمير المعطيات والتدمير كليا وذلك بجعلها غير صالحة للاستعمال او تدميرا جزئيا ذلك من قيمة ادائها".[3]

كما يعرف على انه:" الافناء لمادة الشيء او قيام بإحداث تغييرات عليها، بحيث تصبح غير صالحة للاستعمال في الغرض الذي انشا لها وبالتالي تضيع القيمة المادية لهذا الشيء على المالك.[4]

وعليه فان الاتلاف المعلوماتي لا يتحقق فقط في التأثير على مادة الشيء، بل يتحقق كذلك في حالة الانتقاص من قيمته، العبرة هو ان يمس فعل الاتلاف بالقيمة المادية للشيء،

[1]- مصطفى يوسف كافي، جرائم الفساد غسيل الاموال السياحة الارهاب الالكتروني المعلوماتية،ط1، مكتبة المجتمع العربي، عمان، 2014، ص175.
[2]- مرجع نفسه، ص175.
[3]- عايد رجا الخلايلة، المسؤولية التقصيرية الالكترونية المسؤولية الناشئة عن اساءة استخدام اجهزة الحاسوب والانترنت دراسة مقارنة، ط1، دار الثقافة، عمان، 2009، ص109.
[4]- عبد الفتاح بيومي حجازي، الحكومة الالكترونية ونظامها، الكتاب الثاني، دار الفكر الجامعي، الاسكندرية، 2004، ص329.

ليس التعرض لمادته، لان الفعل الذي يفقد الشيء من قيمته المالية وينقص منها فيتحقق بذلك الاعتداء الذي جرمه القانون.

ثانيا: اركان جريمة الاتلاف المعلوماتي

ان جريمة اتلاف المعطيات المعلوماتية لا يتحقق الا بتوافر الاركان العامة لأية جريمة وهي (الركن المادي والركن المعنوي) وبالتالي لا يمكن تطبيق نصوص جزائية على جريمة الاتلاف التقني الا بتوافر شروط التي تقوم علها اركان الجريمة.

1- الركن المادي لجريمة الاتلاف المعلوماتي

يقوم الركن المادي في جريمة اتلاف المعلومات على عنصرين اساسيين هما فعل الاتلاف و وقوع الضرر.

أ- السلوك الاجرامي

ان فعل الاتلاف في المجال المعلوماتي يمكن ان يمتد الى المكونات المادية (الشاشة و لوحة المفاتيح...الخ) او يكون على المكونات المعنوية للنظام المعلوماتي (المعطيات و البرامج والمعلومات)، وفي كلتا الحالتين يتمثل السلوك الاجرامي الذي يقوم به الجاني في تخريب الاموال سواء كانت مادية او معنوية غير صالحة للاستخدام سواء كان الاتلاف تاما جزئيا.[1]

يتمثل سلوك الجاني في اتلاف المكونات المادية للنظام المعلوماتي (لوحة المفاتيح و الشاشة و حدات الادخال...) بتخريبه او تعطيله او جعله غير صالح للاستعمال.[2]

يقصد بالتخريب هو: "توقف الشيء تماما عن أن يؤدي منفعته حتى ولو لم تفنى مادته سواء كان هذا التوقف كليا او جزئيا ويكون الشيء غير صالح للاستعمال بجعله لا يقوم بوظيفته المرصود لها على النحو الاكمل".[3]

[1]- امين طعباش، الحماية الجنائية للمعاملات الالكترونية، ط1، مكتبة الوفاء القانونية، الاسكندرية، 2005، ص76.

[2]- هدى حامد قشقوش، جرائم الحاسوب الالي في التشريع المقارن، ط1، دار النهضة العربية، القاهرة، 1992، ص564.

[3]- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الالي، المرجع السابق، ص111.

اما التعطيل فيقصد به: "توقف الشيء عن القيام بوظيفته لفترة مؤقتة" ومن الامثلة الواقعة الاعتداء المادي على النظام المعلوماتي وهو ما قامت به مجموعة من المجرمين تطلق على نفسها منظمة تدمير الحاسبات او نظم المعلومات حيث تسببت هذه الجماعة للشركات الفرنسية التي تقوم بصناعة اجهزة الانظمة المعلوماتية خسائر مالية كبيرة نتيجة افعال التعدي والاتلاف.[1]

اما بالنسبة لسلوك الجاني في اتلاف المكونات المعنوية (المعطيات و المعلومات و البرامج) للنظام المعلوماتي فيتمثل في ثلاث عناصر وهي (المحو و التعديل الغير مشروع للمعطيات و الادخال الغير مشروع للمعطيات) بحيث يكون هذا الاتلاف معيبا لكل او لجزء من النظام المعلوماتي.[2]

ب- وقوع الضرر

ان جريمة اتلاف المعطيات المعلوماتية من جرائم الضرر لا الخطر، الضرر هو اثر الفعل الذي قام به الجاني فلا جريمة اتلاف بدون ضرر حتى مع تحقق السلوك الاجرامي، فأغلبية التشريعات اشترطت لقيام جريمة اتلاف المعطيات المعلوماتية وقوع نتيجة معينة، فالضرر يختلف باختلاف طبيعة المال محل الاتلاف و بحسب ماهية المال فقد يكون على شكل انقاص لكل او لجزء مكونات الشيء الاساسي حيث يؤثر في المال كوحدة وبالتالي يودي الى تعطيله، وقد يكون على شكل ابطال اداء المال (الكيان المادي و المعنوي) لوظيفته وحرمان صاحبه من الاستفادة من ماله، ومنه نلاحظ ان حجم الضرر وطبيعته ومدى شموله للمال يؤدي الى انعدامه او كونه يعطل المال جزئيا (كيان مادي و معنوي) لا ينظر اليه بقدر ما ينظر الى تحققه بأية نسبة كانت.[3]

[1]- امين طعباش، المرجع السابق، ص77.
[2]- مرجع نفسه، ص78.
[3]- اسامة احمد المناعسة و جلال محمد الزعبي، المرجع السابق، ص121-122.

2- الركن المعنوي لجريمة الاتلاف المعلوماتي

ان اتلاف المعطيات تعتبر من الجرائم العمدية المقترنة وجوبا بالقصد الجنائي مع ضرورة توافر القصد الجنائي الخاص، وعليه فان الركن المعنوي لجريمة اتلاف المعطيات المعلوماتية يقوم على القصد الاجرامي العام، مع ضرورة توافر القصد الاجرامي الخاص.

أ- القصد الاجرامي العام

لاجل توافر القصد الجنائي لابد من توافر عنصران هما العلم و الارادة و يجب ان ينصرف كلاهما الى كافة العناصر التي يتألف منها الركن المادي للجريمة، فلا بد ان يعلم الجاني ان المعطيات و البرامج التي تقع على فعله المادي غير مملوكة له وانما مملوكة لغيره و ان تتجه ارادته الى اتلاف و تخريب المعطيات و البرامج[1]، وهو ما نصت عليه اتفاقية بودابست في المادة الرابعة منها.

ب- القصد الاجرامي الخاص

لا يكفي عنصري العلم والارادة لتقوم جريمة اتلاف المعطيات المعلوماتية بل وجب ان تتوافر على القصد الجنائي الخاص (النية الاجرامية لدى الجاني) لتقوم هاته الجريمة ليس هذا القصد الخاص، عليه وجب ان تتجه ارادة الفاعل لتخريب وافساد او تغيير في حالة المعطيات و المعلومات و البرامج الموجودة في النظام المعلوماتي[2]، وهو ما نصت عليه اتفاقية بودابست من خلال المواد(4-5).

ثالثا: الجزاءات المقررة لجريمة الاتلاف المعلوماتية

نظرا للمكونات المنطقية لأنظمة الحاسب الآلي وما تشمله من برامج ومعلومات وبيانات من قيمة اقتصادية، سارعت الدول إلى فرض حمايتها لتلك المكونات و جرّمت كل ما من شأنه

[1]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الالي في التشريع الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية، 2007، ص186-187.

[2]- حسام محمد نبيل الشراقي، الجرائم المعلوماتية دراسة مقارنة على جرائم الاعتداء التوقيع الالكتروني، دار الكتب القانونية، مصر، 2013، ص328.

الإضرار بها خاصة إذا تم عبر شبكة الإنترنت وعلى الرغم من ذلك فالموقف لم يكن واحداً في جميع الدول.

1- موقف التشريعات الغربية من جريمة اتلاف المعلومات

أولى المشرّع الغربي المكونات المنطقية لأنظمة الحاسب الآلي وما تشمله من برامج ومعلومات وبيانات اهتماما خاصة نظرا لما لها من قيمة اقتصادية كبيرة خاصة في عصر عرف بكونه عصر المعلوماتية ، وتمثل هذا الاهتمام الغربي في استحداث نصوص خاصة تجرّم كل ما من شأنه الإضرار بتلك المكونات.[1]

أ- موقف التشريع الأمريكي

لم يتضمن التشريع الفيدرالي لجرائم الحاسب الآلي الصادر عام 1984م على ما شأنه تجريم إتلاف المعلومات والبرامج بصورة عامة، إنما أقتصر التجريم فقط على الإتلاف الذي يترتب عليه إعاقة أنظمة الحاسبات الآلية عن العمل حيث جرّمت الفقرة الثانية من المادة"1030- a "من التشريع الفيدرالي الأمريكي إتلاف المعلومات الذي يترتب عليه إعاقة الحكومة عن استعمال أنظمة الحاسبات الآلية.

الا أنه ونتيجة لكثرة الانتقادات التي وجهت إلى هذا التشريع تم تعديله بحيث أصبحت الفقرة الثالثة من المادة "1030-a "تتناول فقط الدخول غير المصرح به إلى حاسب آلي تستعمله الحكومة متى أعاق الدخول هذا الاستعمال، وأضيفت فقرة خامسة إلى ذات المادة جرّمت الإتلاف العمدي غير المصرح به لمعلومات يحتويها حاسب آلي تابع لحكومة الولايات المتحدة وإدارتها أو حاسب آلي غير تابع للحكومة إلا أنه يتم استخدامه من قبلها أو لصالحها، أو إعاقة هذا الحاسب عن إدارة المهام المختلفة التي تباشرها الحكومة بواسطته، والهدف من إضافة الفقرة السابقة هو حماية المعلومات وأنظمة الحاسبات الآلية من أعمال الإتلاف التي ترتكب بواسطة أشخاص غير مصرح لهم بالدخول إلى النظام، ومن أهم ما أتت به المادة "1030 -a" بعد تعديلها تجريم الإتلاف المعلوماتي فالبند الأول من الفقرة الخامسة ينص على "تعديل المعلومات و البرامج و الشفرات و الأوامر داخل أنظمة الحاسبات الآلية مما يترتب عليه

[1] -https://www.startimes.com/?t=16193884.

أضرار تلحق بحاسب آلي يتمتع بالحماية متى ما كان إحداث الضرر قد تم عمدا" والفعل الإجرامي هنا يعد جناية.[1]

ب- موقف التشريع الفرنسي

تعتبر فرنسا من أوائل الدول الغربية التي سارعت إلى إصدار تشريعات خاصة بحماية النظم المعلوماتية والتصدي لبعض صور الجرائم المستحدثة ، والتي قد تقع بسبب التقدم في استخدام الحاسب الآلي وكذلك شبكة الإنترنت أو بعض الشبكات المحلية كما هو الحال في شبكة المانتيل الفرنسية.

ويعد القانون رقم 17-78 الصادر في السادس من يناير1978م بشأن الحريات والمعلومات هو اللبنة الأساسية لتنظيم وحماية النظم المعلوماتية في فرنسا حيث عالج المشرّع من خلاله مسألة تخزين البيانات في الحاسب الآلي وبيان لأنواعها المختلفة ومدة التخزين ، كذلك الجهة المختصة بالرقابة والإشراف على أعمال ذلك القانون.[2]

بعد ذلك وعلى أثر التطور الكبير في ثورة المعلومات وفي الحاسبات الآلية وشبكة الإنترنت تقدم النائب Jacques Godjrain في الخامس من أغسطس باقتراح مشروع قانون خاص بالغش المعلوماتى والذي تم إقراره في 1987/12/22م ليصبح قانونا نافذا اعتبارا من الخامس من يناير1988م وحمل رقم 19-88 بشأن الغش المعلوماتى و في وقت لاحق أدمجت نصوص هذا القانون في قانون العقوبات الفرنسي الجديد (المواد 323-1 إلى 323-7) تحت عنوان " الاعتداءات على نظام المعالجة الآلية للمعطيات".[3]

ومن أهم ما جاء به هذا القانون فيما يتعلق بالإتلاف المعلوماتي نص المادة 323-1 والخاصة بجريمة الدخول غير المشروع على أنظمة الحاسب الآلي، حيث اعتبر الإتلاف الواقع على المعطيات الموجودة داخل النظام ظرفا مشددا لجريمة الدخول غير المشروع متى ما كان الإتلاف بسبب هذه الجريمة الأخيرة. وهناك أيضا المادة 323-3 التي جرّمت إدخال البيانات

[1] -https://www.startimes.com/?t=16193884.

[2]- مرجع نفسه.

[3] -https://www.startimes.com/?t=16193884

بطريقة غير مشروعة في نظام معالجة البيانات أو إلغاء أو تعديل البيانات التي يحتوى عليها النظام بطريقة غير مشروعة[1].

2- موقف التشريعات العربية

اهتمام المشرع العربي بجريمة الإتلاف المعلوماتي لم يكن بذات المستوى الموجود لدى المشرع الغربي، فأغلب الدول العربية لم تحرك ساكنا لمواجهة هذا النوع المستحدث من الجرائم وإنما اعتمدت على النصوص القائمة المنصوص عليها في مدوناتها العقابية، ومع ذلك قامت بعض الدول العربية باستحداث نصوصاً خاصة بهذه الجرائم.

أ- موقف جمهورية مصر العربية

لمشرع المصري جرّم الإتلاف ولكن بالمفهوم التقليدي له، فالمادة 361من قانون العقوبات تنص على " كل من خرب أو أتلف عمدا أموالا ثابتة أو منقولة لا يمتلكها أو جعلها غير صالحة للاستعمال أو عطلها بأية طريقة يعاقب بالحبس مدة لا تزيد على ستة أشهر وبغرامة لا تتجاوز ثلاثمائة جنيه أو بإحدى هاتين العقوبتين ... ".

أما بالنسبة للإتلاف المعلوماتي الواقع على المكونات المنطقية للحاسب الآلي فلا يوجد نص خاص كذاك الموجود في التشريع الأمريكي والفرنسي أو في أو التشريع العماني ، باستثناء بعض النصوص الواردة في القانون رقم 143 لسنة 1994م بشأن الأحوال المدنية والتي يقتصر تطبيقها بصريح النص على شبكة الحاسبات الخاصة بمصلحة الأحوال المدنية فقط، بالتالي ومع وجود الاختلاف الفقهي حول مدى صلاحية النصوص التقليدية لمواجهة الإتلاف المعلوماتي فإنه يكون من الملائم جدا استحداث نصوصاً جديدة تتلاءم مع التطور التقني في تكنولوجيا المعلومات وشبكات الاتصال.[2]

[1]- مرجع نفسه.
[2]- مرجع نفسه.

ب- موقف التشريع الجزائري

لقد اقر المشرع الجزائري المسؤولية الجزائية للشخص الطبيعي و الشخص المعنوي في معظم الجرائم وهو ما اقره في الجرائم المعلوماتي و بالتحديد في جريمة اتلاف المعطيات المعلوماتية، ولقد نصت المادة 394مكررر 1 من قانون العقوبات الجزائري على معاقبة الشخص المتلف للمعطيات والمعلومات، لقد نصت المادة 394مكرر 4 من قانون العقوبات الجزائري على العقوبات التي تطبق على الشخص المعنوي.

الفرع الثاني: جريمة النصب (الاحتيال) المعلوماتي

يعد النصب المعلوماتي من اكثر الجرائم المعلوماتية التي ترتكب على نطاق واسع في مختلف الدول وتسبب خسائر اقتصادية فادحة، الامر الذي شكل قلقا لدى المعنيين بالأمر، حيث نجد ان هذه الجريمة تزعزع كيان الافراد بالوسائل التقنية الحديثة لنقل الاموال، وعليه سوف نبين تعريف جريمة النصب المعلوماتي و بيان اركانها و الجزاءات المقررة لهذه الجريمة.[1]

اولا: تعريف جريمة النصب المعلوماتي

عرف بعض الفقهاء النصب المعلوماتي بأنه: "التلاعب العمدي بمعلومات وبيانات تمثل قيماً مادية يختزنها نظام الحاسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة، أو أية وسيلة أخرى من شأنها التأثير على الحاسب الآلي، حتى يقوم بعملياته بناء على هذه البيانات أو الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع و إلحاق الضرر بالغي".[2]

ويعرف كذلك بانه التلاعب العمدي بمعلومات وبيانات تمثل قيمة مادية يختزنها نظام الحاسوب الالي او الادخال غير المصرح به لمعلومات و بيانات صحيحة، او التلاعب في

[1]- نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2، دار الثقافة للنشر و التوزيع، الاردن، 2010 ، ص186.
[2]- عبد الجبوري و سامر سلمان، جريمة الاحتيال الالكتروني، رسالة ماجستير مقدمة الى كلية الحقوق ، جامعة البحرين،2014، ص6.

الاوامر و التعليمات التي تحكم عملية البرمجة او اية وسيلة اخرى من شانها التأثير على الحاسب الالي حتى يقوم بعملياته بناءا على هذه البيانات او الاحتيال المعلوماتي.[1]

كما عرفته احدى الدراسات التي اجريت في الولايات المتحدة الامريكية انه "فعل او مجموعة من الافعال غير المشروعة و المتعمدة التي ترتكب بهدف الخداع او التعريف للحصول على شيء ذو قيمة، يكون نظام الحاسوب لازما لارتكابها".[2]

ومن خلال التعريفات السابقة يتضح أنا لفعل المرتكب غير المشروع قد يكون باستخدام طرق احتيالية أو تغيير حقيقة لبيانات أو اختلاسها أو تخريب البيانات أو دخول غير مشروع إلى موقع خاص، قد يوجه هذا الفعل غير المشروع ضد نظام حاسوبي آخر كتخريب بياناته أو قد يتعلق بنفس النظام الحاسوبي، كتقديم خدمة وهمية مثلاً.

ثانيا: اركان جريمة النصب المعلوماتي

يتطلب وقوع جريمة النصب عبر شبكة المعلومات توافر أركانها، فلابد من أن تتبلور الجريمة ماديا وتتخذ شكلاً معيناً وهو الركن المادي للجريمة المتمثل في سلوك الجاني لإحدى وسائل الاحتيال المنصوص عليها في القانون، إلاّ أن هذا الركن لا يكفي إسناد المسؤولية إلى شخص معين بل يجب أن يتحقق الركن المعنوي المتمثل بالقصد الجنائي والذي يرتكز على توفر الإرادة الآثمة لدى الجاني حين ارتكابه للجريمة وعلمه بأن فعله أو امتناعه يشكل ضرراً أو خطراً على الغير يعاقب عليه القانون.

1- الركن المادي لجريمة النصب المعلوماتي

يتطلب النصب ركًنا مادياً قوامه الاستيلاء بالاحتيال على مال الغير، يتألف هذا الركن من فعل النصب وهو استعمال وسيلة من وسائل النصب، نتيجة معاقب عليها هي الاستيلاء على مال منقول للغير، علاقة سببية بين السلوك والنتيجة.

[1]- معتوق عبد اللطيف، الاطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، رسالة ماجستير في العلوم القانونية، جامعة العقيد الحاج لخضر، باتنة، كلية الحقوق و العلوم السياسية، 2012-2011، ص42.

[2]- حمزة بن عقون، السلوك الاجرامي للمجرم المعلوماتي، رسالة ماجستير في العلوم القانونية، جامعة العقيد الحاج لخضر، باتنة، كلية الحقوق و العلوم السياسية، 2011- 2012 ،ص63.

ويأخذ الركن المادي الخاص بجريمة الاحتيال عبر شبكة المعلومات الدولية، أشكالاً عدة منها البريد الإلكتروني الذي تم إرساله أو الأداة الإلكترونية التي يتم الاستعانة بها في ارتكاب جريمة الاحتيال المعلوماتية، أو الأدوات التي تم تصميمها، أو تم الاستعانة بها من خلال الاتصال أو الإيقاع بالضحية كما يلزم توفر الأداة التي تم إرسال الرسالة من خلالها والتي تتمثل في هذه الحالة الجهاز الحاسوبي لإتمام عملية الاحتيال، أو الوصول إلى قواعد بيانات غير مسموح بالاطلاع عليها، أو استخدامه للوصول إلى معلومات موجودة على جهاز حاسوبي أخر، وكلها أمور كفيلة بأن ت ثبت توفر الركن المادي للجريمة.[1]

أ- السلوك الاجرامي (فعل النصب)

تقوم جريمة النصب على خداع المجني عليه و ذلك عن طريق صور عدة بالنسبة لطرق النصب، المتمثلة في استعمال طرق احتيالية **و** اتخاذ اسم كاذب أو صفة غير صحيحة و اتخاذ الاكاذيب نطاق معين يؤدي إلى التصرف في مال أو منقول ليس ملكا للجاني.

ب- النتيجة (تسليم المال المعلوماتي)

يعد تسليم المال النتيجة الجريمة، فإن تم ذلك تحققت الجريمة تامة، أما في حالة إذا تخلف هذا العنصر وقفت الجريمة عند حد الشروع، و التسليم هو سلوك يصدر عن المجني عليه يتضمن قيامه بتصرف مالي من شأن هذا التصرف نقل مال موضوع الجريمة إلى الجاني أو إلى أي شخص آخر يعنيه، كل ذلك بناءا على إرادة مشوبة بالغلط، نتيجة لما استخدمه الجاني من وسائل احتيالية، من هنا يشترط أن يأتي سلوك المجني عليه في تسليم المال بناءا على إرادة مشوبة بالغلط وقت التسليم، أي إرادة معينة و يجب أن يكون السلوك الناقل للمال غير صحيح قانونا ولا قيمة و لا أثر له.[2]

أما في مجال المعلومات فإن الحاسب الالي يقوم بفعل التسليم بالمفهوم المادي للكلمة كما أن التسليم يجب ألا ينظر إليه في الشكل المادي فقط، انما هو كذلك عمل

[1]- سمير إبراهيم جميل الغزاوي، المسؤولية الجنائية الناشئة عن استخدام الانترنيت، رسالة ماجستير مقدمة الى كلية القانون، جامعة بغداد، 2005، ص98.

[2]- محمد عودة الجبور، الجرائم الواقعة على الاموال، ط1 ،دار النفائس، الاردن، 2011، ص214.

قانوني في عنصره الجوهري يتمثل في إرادة المجني عليه المعيبة بالخداع و ليست المناولة المادية سوى مظهره المادي أو أثره.[1]

ج- العلاقة السببية بين الاحتيال و النتيجة

لا يكفي لقيام جريمة النصب ان يرتكب الجاني فعل الاحتيال وحدوث واقعة التسليم التي تعني سلب المال، انما يلزم ان يكون التسليم وقع بطريقة من طرق النصب المستخدمة من الجاني، أي ان العلاقة السببية تنص على ان النصب هو السبب الفعلي و الدافع على التسليم، ان يكون التسليم لاحقا على فعل الاحتيال و نتيجة لانخداع المجني عليه، ان يكون مبني على الضرر.[2]

2- الركن المعنوي لجرمة النصب المعلوماتي

النصب جريمة عمدية، يعني انه يجب توافر العلم والارادة بخصوص النشاط والنتيجة.

أ- القصد العام

القصد العام في جرائم النصب المعلوماتي يرى الفقهاء ان الجرائم المعلوماتية تنطبق سواء بالنسبة للجرائم الناشئة عن طريق علم الجاني بأن قيامه بتلاعب المعلوماتي بالبيانات الموجودة بالنظام أو المعطيات التي يقوم بإدخالها بأنه يقوم بعمل غير مشروع و يستخدم الطرق الاحتيالية، إذا اتخذ اسم كاذب من أجل تحويل الاموال من حساب إلى آخر أو حالة قيام باستخراج فواتير بحساب غير حقيقي، أن تتجه إرادته إلى خداع النظام من أجل سلب مال الغير و الجرائم الناشئة عن استخدام بطاقات الائتمان حيث يصرف علم الجاني أنه و بالرغم من علمه بعدم سماح الرصيد في حسابه إلا أن إرادته تتجه إلى وجود ائتمان، بقصد الحصول على أموال من البنك.[3]

---

[1]- حسام محمد نبيل الشنراقي، جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، مصر، 2013، ص205.

[2]- احمد خليفة الملط، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، الاسكندرية، 2006، ص 346.

[3]- خديجة دحمان صبايحية، جرائم السرقة والاحتيال عبر الانترنيت، دراسة مقارنة بين الفقه الجزائري، رسالة الماجستير في العلوم الاسلامية، تخصص شريعة وقانون الشريعة العلوم الاسلامية، جامعة الجزائر،2013/2012، ص72.

ب- القصد الخاص

القصد الخاص في جريمة النصب المعلوماتي يكون متوفر حالة استخدام الجاني للنظام المعلوماتي لسلب مال الغير أن يستخرج من النظام فواتير باسمه أو باسم شركائه بمبالغ غير مستحقة ثم يقوم بتقاسمها بينهم هو و شركائه[1]، كما يتوفر القصد الخاص في النصب المعلوماتي وقت ما قام الجاني باستخدام البطاقة و هو يعلم أن رصيده ال يكفي و بطاقته منتهية أو موقوفة و يستخدمها و يعد فعل الجاني مناورة هدفها الاستيلاء على جزء من مال البنك، لأن الجاني يعلم أنه لا يحق له استخدام هذه البطاقة و رغم ذلك يوجه إرادته لاستخدامها لسلب مال المجني عليه.[2]

ثالثا: الجزاءات المقررة لجريمة النصب المعلوماتي

تختلف جرائم الحاسوب عن الجرائم الاخرى فيما يتعلق بالتحقيق وجمع الادلة، منها النصب المعلوماتي فهي تختلف عن جريمة النصب في صورتها التقليدية، فالجرائم التي ترتكب بواسطة الحاسوب تنشا في الخفاء، ينصب الاعتداء فيها على معطيات الحاسوب المخزنة و المعلومات المنقولة عبر نظم شبكات المعلومات[3]، سوف نبين عقوبات جريمة النصب الالكتروني وفق النظام السعودي و القانون الأردني و القانون الجزائري.

1- عقوبة جريمة النصب الالكتروني وفق النظام السعودي

ففي نظام مكافحة جرائم المعلوماتية السعودي تتمثل عقوبات جرائم الاستيلاء على مالٍ منقولٍ، أو الاستيلاء على سند أو توقيعه وذلك عن طريق الاحتيال، أو اتخاذ اسمٍ كاذب، أو انتحال صفة غير صحيحة المنصوص عليها في المادة الرابعة من نظام مكافحة جرائم المعلوماتية بالسجن والغرامة، أو بواحدة من هاتين العقوبتين، وذلك وفقاً لما يلي:

[1]- خديجة دحمان صبايحية، المرجع السابق، ص72.
[2]- أمين طعباش، الحماية الجنائية المعاملات الالكترونية، ط1، الوفاء القانونية، الاسكندرية، 2015، ص176.
[3]- خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنيت ، ط1 ، دار الثقافة للنشر و التوزيع، الاردن، 2011، ص 147-148.

السجن وقد حددت المادة الحد الأعلى للسجن في الجرائم السابقة، وذلك بما لا يتجاوز ثلاث سنوات ولم تضع حداً أدنى، باستثناء ما سيأتي من الظروف المشددة للعقوبة، والتي تجعل الحد الأدنى للسجن نصف المدة، وبالتالي لا تقل مدة السجن في تلك الحالات عن سنة وستة أشهر، في النظام السعودي فقد اشتمال المادة (4)و (5)كما وضحنا على عقوبات محددة بحد أقصى وفقاً للجرائم المنصوص عليها في طيات النظام، وبالنسبة لجريمة الاحتيال فقد حدد لها النظام السعودي حسب ما ورد في المادة الرابعة منه بألا تزيد مدة حبس الجاني على ثلاث سنوات وبغرامة لا تزيد عن مليوني ريال أو بإحدى هاتين العقوبتين.[1]

2- عقوبة جريمة النصب الالكتروني وفق النظام الاردني

قانون الجرائم الإلكترونية الأردني منح المنظم الأردني للقاضي سلطات تقديرية واسعة في إقرار ما يصل إليه باجتهاده، وإصدار الأحكام بالعقوبات المناسبة بحق الجاني وفقاً لما يراه، ويظهر ذلك جلياً في عدم تحديد العقوبة من قبل المشرع في بعض المواد ومنها المادة (3)التي تنص على انه (يعاقب كل من دخل قصداً إلى الشبكة المعلوماتية أو نظام معلومات باي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (100)مائة دينار ولا تزيد على (200)مائتي دينار أو بكلتا هاتين العقوبتين...)، وفق المادة (3) "يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين" ، كما أجاز المشرع إمكانية الجمع بين عقوبتي السجن والغرامة بقوله "أو بهما معاً" في إشارة منه لتشديد العقوبة حال ارتكاب الفعل في حالات خاصة، وفي مواضع أخرى يجدد مقدارها وفق ما ورد في المادة الثانية عشرة.[2]

3- عقوبة جريمة النصب الالكتروني وفق النظام الجزائري

بالنسبة لقانون العقوبات الجزائري لم يرد نص قانوني يعاقب على جريمة النصب المعلوماتي، لكنه اورد نص المادة (372) من قانون العقوبات تنص على جريمة النصب التقليدية كما يلي:

[1]- وائل محمد نصيرات و غادة عبد الرحمن الطريفي، جريمة الاحتيال عبر شبكة المعلمات الدولية دفاتر السياسة والقانون، السعودية، 2018، ص109.
[2]- مرجع نفسه، ص109.

يعاقب بالحبس من سنة على الاقل الى خمس سنوات على الاكثر وبغرامة من 20.000 الى 100.000 دينار جزائري و تنص المادة (17) على الشروع.[1]

[1]- انظر لمادة (372)، من قانون العقوبات الجزائري، رقم 156/66، المعدل و المتمم.

المبحث الثاني: الاثار الاقتصادية للجرائم المعلوماتية واستراتيجيات مواجهتها

قمنا بتقسيم هذا المبحث الى مطلبين تناولنا في المطلب الاول الاثار الاقتصادية للجرائم المعلوماتية و تناولنا في المطلب الثاني مكافحة الجرائم المعلوماتية على المستوى الدولي.

المطلب الاول: الاثار الاقتصادية للجرائم المعلوماتية

للجريمة المعلوماتية الماسة بالاقتصاد عدة اثار يتوجب الوقوف عليها، ناهيك عن ضرورة الوقوف على معوقات اثبات الجريمة المعلوماتية الماسة بالاقتصاد الرقمي وهذا ما سنتطرق اليه في هذا المطلب.

الفرع الاول: الاثار الناجمة عن الجريمة المعلوماتية وانعكاسها على الاقتصاد

تتمثل اهم الاثار الناجمة عن الجريمة الماسة بالاقتصاد في ما يلي:

اولا- المساس بالاستقرار المالي و الاقتصادي

ان الاستقرار المالي و الاقتصادي يعد مطلبا هاما في أي دولة لضمان الاستقرار، تعد الجرائم الاقتصادية في البيئة الرقمية من اهم عوامل عدم الاستقرار، فان تعلق الامر بالمجرم الاقتصادي الذي يستعمل البيئة الرقمية لتبيض الاموال و توظيفها في المشاريع، فانه لا يتوانى في تصفية المشاريع بمجرد تحقيق اهدافه، مما يمس باستقرار الاقتصاد.[1]

ثانيا- الخسائر المالية المنجرة على الجريمة المعلوماتية

لا شك ان التحول الذي عرفه الاقتصاد من اقتصاد تقليدي الى اقتصاد رقمي و تحول المعاملات التجارية و المالية الى طبيعة الكترونية، هو ما زاد من خطورة الجريمة المعلوماتية

[1]- مجدوب نوال و اخرين، الجرائم المعلوماتية واثارها على التنمية الاقتصادية، ط1، المركز الديمقراطي العربي، ج2، برلين، 2020، ص52.

ونجم عنه خسائر كبيرة يتكبدا العالم[1]، بذلك يمكن القول ان رقمية التعاملات الجارية التي يقوم بها اشخاص طبيعيون و شركات التسويق نجم عنها ارتفاع معدل الاجرام المعلوماتي و نتيجة ذلك استنزاف الاقتصاد، اذ تبين من خلال الاحصائيات ان الاقتصاد العالمي يتضرر من جراء الجريمة المعلوماتية سنويا أي ما يعادل تريليون دولار سنويا.[2]

والاشكال ليس فقط في ارتفاع حجم الخسائر المالية، بل ان الامر اخطر من ذلك، اذ ان تزايد الاقبال على المعلوماتية جعل حجم الخسائر غير ثابت، فقد اصبحت الخسائر الناجمة عن الجريمة المعلوماتية ضريبة لا مفر منها.[3]

ثالثا- احداث العجز في ميزان المدفوعات

تؤدي الجريمة المعلوماتية ذات الطابع الاقتصادي الى احداث عجز في المدفوعات و لاسيما في حالة الاستعمال الرقمي بهدف التهرب من دفع الضرائب، كما تساهم الجرائم المعلوماتية في زيادة الانفاق العام بهدف مواجهتها.[4]

رابعا- الاضرار بالنشاط المصرفي

تؤدي الجريمة المعلوماتية الى افساد نشاط البنوك عن طريق التعامل بالعملات الرقمية المزورة، و بطاقات الائتمان المزورة، ناهيك عن كون الجريمة المعلوماتية تسبب انهيار في سوق القيم المنقولة، في حالة استثمار الاموال الاجرامية المحصلة عن طريق البيئة الرقمية في سوق القيم المنقولة، من خلال شراء اوراق مالية من عائدات اجرامية مما يحدث خلل في توازن سوق القيم المنقولة مما يؤدي الى انهيار سوق القيم المنقولة.[5]

[1]- صراح كريمة و دقيش جمال، الابعاد التسويقية، مجلة الدراسة التسويقية، مجلد رقم 02، عدد01، 2018، ص44.
[2]- مجدوب نوال و اخرين، المرجع السابق، ص53.
[3]- صراح كريمة و دقيش جمال، المرجع السابق، ص46.
[4]- مجدوب نوال واخرين، المرجع السابق، ص53.
[5]- مرجع نفسه، ص53.

خامسا- انخفاض معدل الاستثمار و الادخار

غالبا ما يقوم الاقتصادي الذي حصل على اموال عن طرق البيئة الرقمية بإخراج الاموال التي جمعها من اقليم الدولة التي تم استنزاف اقتصادها الى اقليم دولة اخرى، ذلك بهدف اخفاء الشبهة و هو ما يؤدي الى انخفاض معدل الاستثمار بسبب نقص التمويل، ناهيك عن انخفاض معدل الاستثمار الذي يعد مؤشرا على سلامة اقتصاد الدولة.[1]

كما ساهمت المعلوماتية في خلق سرعة كبيرة لحركة رؤوس الاموال، سهلت الربط بين الاسواق العالمية في اطار نظام تبادلي، حفزت المعلوماتية الشركات العابرة للحدود، مما زاد في حجم التفاعل بين المتعاملين الاقتصاديين و ساهمت في تفشي التهريب.[2]

سادسا- ارتفاع معدل التضخم

ان الجريمة المعلوماتية قد تكون مؤشر لحدوث تضخم او زيادة معدله في حالة كان موجود من قبل، يتحقق ذلك في تلك الحالة التي تطرح اموال غير مشروعة محصلة عن طريق البيئة الرقمية بغض النظر عن نوع الجريمة قصد توظيفها و استثمارها مما يؤدي الى الزيادة في اسعار السلع و الخدمات و النتيجة ارتفاع قيمتها.[3]

الفرع الثاني: معوقات الجريمة المعلوماتية الماسة بالاقتصاد

هناك عدة معوقات تحول دون اثبات الجريمة المعلوماتية الماسة بالاقتصاد الرقمي التي يمكن اختصارها في ما يلي:

اولا: عدم وجود اثار مادية للجريمة

ان خصوصية الجريمة المعلوماتية الماسة بالاقتصاد جعلتها تنفرد بذاتية مقارنة بباقي الجرائم، الامر الذي جعل عملية الكشف عنها من طرف السلطات جد صعبة و لاسيما مع

[1]- بسام احمد الزلمي و عبود السراج، دور النقود الالكترونية في عمليات غسل الاموال، مقال منشور مجلة العلوم الاقتصادية و القانونية، جامعة دمشق، المجلد رقم 36، العدد 01، 2010، ص03.
[2]- مجدوب نوال و اخرين، المرجع السابق، ص54.
[3]- مرجع نفسه، ص53.

افتقارها للدليل الرقمي[1]، يبقى اغلبها مجهول، يضيف ذلك ان مرتكب الجريمة يبذل قصارى جهده لعدم ترك أي اثر مادي، ناهيك عن عدم تمكن الكل من التحكم في المعلوماتية، لا شك ان جهل المعلوماتية ساعد المجرم الاقتصادي في ارتكاب الجريمة.[2]

ثانيا: اتسام الجريمة المعلوماتية الماسة بالاقتصاد بكونها جريمة عابرة للحدود

لقد تحدثنه عن هذه الخاصية سابقا حيث تناولنا بان الجريمة المعلوماتية تتصف بانها من الجرائم العابرة للحدود، حيث ان العولمة والمعلوماتية جعلت العالم قرية واحدة، اذ و رغم إيجابيات العولمة الا ان المجرمون استغلوا هذه الاخيرة من اجل تسهيل ارتكاب الجريمة، اين تعدى الاجرام حدود الدولة الواحدة، صار بإمكان المجرم اختراق حساب او موقع او حساب بنك معين دولة معينة، له تحويل المبالغ و المعاملات الى دولة ثالثة، دون ان يتحرك من مكانه وهو ما يسمى بالأجرام عن بعد، بدون استعمال العنف بل و هو مستلق بسريره، اذ صار بغير حاجة لكسر الاقفال ولا اخفاء البصمات او تحويل العائدات الاجرامية، بل يكفيه خط انترنت و حاسوب حتى يجول و يصول بكافة انحاء العالم مرتكبا جرائمه الاقتصادية من تزوير بطاقات الائتمان و الاحتيال السيبراني.[3]

ثالثا: المعوقات القضائية

تتجلى المعوقات القضائية التي تحول دون امكانية الكشف عن الجريمة الاقتصادية المرتكبة في البيئة الرقمية في ما يلي:

– نقص المعوقات لدى جهات البحث والتحري و التحقيق بالجريمة المعلوماتية، أي نقص الخبرة لدى رجال الضبط القضائي و الامن عموما، اجهزة العدالة الجنائية ممثلة في الوسط الاتهامي و التحقيق، لاشك ان من شان ذلك الحيلولة دون الكشف عن الجريمة المعلوماتية المرتكبة في البيئة الرقمية .

[1]- فيصل فهد، انتهاك الخصوصية، مقال منشور بمجلة الامن و الحياة، الصادر عن اكاديمية نايف للعلوم الامنية، العدد 378، السعودية، 2013، ص03.
[2]- بن بادرة عبد الحليم، اجراءات البحث والتحري عن الجريمة المعلوماتية – الخصوصية والاشكالات، مجلة الحقوق والعلوم السياسية، العدد 23، الجزائر، 2015، ص150.
[3]- مجدوب نوال و اخرين، المرجع السابق، ص55.

– ومن بين المعوقات القضائية ايضا ما يعرف بتنازع الاختصاص القضائي بين العالمية والاقليمية، ولا سيما و ان السلوك المادي للجريمة الاقتصادية قد يكون بإقليم دولة، و النتيجة الاجرامية بإقليم دولة اخرى.[1]

رابعا: المعوقات المرتبطة بإثبات الجريمة في حد ذاتها

من بين معوقات الاثبات و المرتبطة بالجريمة في حد ذاتها هي كالاتي:

– اتخاذ الجناة لتدابير امنية، اين يسعى المجرم الاقتصادي لإخفاء الدليل المعلوماتي و تمويهه في شكل عطل او خطا في نظام التشغيل، مع ازالة اثار الجريمة عن طريق التلاعب بالبيانات الرقمية أي المكتوبة برموز رقمية، لا يمكن فهمها لا من طرف الحاسوب، مع قيامه بتشفير البيانات مما يجعل امر فكها امر مستحيل، من ثم يصعب على جهات التحري الوصول اليها، ناهيك عن الانتحال الرقمي اين ينتحل المجرم المعلوماتي صفة اخرى غير صفته.

– الطبيعة غير المادية للأدلة الالكترونية التي ارتكب بها الجريمة الاقتصادية، اذ عادة ما يكون الدليل بالجريمة التقليدية مرئي اما سلاح ابيض، او مادة سامة، او محررات مزورة، غير انه وعندما يتعلق الامر بالجريمة المعلوماتية فان اداة الجريمة هي غير مادية و يصعب الكشف عنها من منطلق ان قوامها معنوي مرتبط بالمعالجة الالية للبيانات، مع امكانية تدمير الدليل الرقمي في ثوان في عملية التفتيش و دون قصد.

– ضخامة حجم المعلومات و البيانات المتعين فحصها، اذ قامت جهات التحقيق فيه فان مسرح الجريمة غير واضح المعالم، في ظل العالم الافتراضي مما يجعل المعينة صعبة و لاسيما مع اصطدامه بفكرة المشروعية و حق الفرد بالخصوصية[2]، هو امر شاق نظرا لنقص الامكانيات المادية و البشرية، مما يؤدي لخطا بالتحقيق و تكرار العملية، اذ يمكن للجاني و بسهولة و

[1]- بن بادرة عبد الحليم، المرجع السابق، ص151.
[2]- زوزو هدى، التسريب كأسلوب من اساليب التحري في قانون الاجراءات الجزائية الجزائري دفاتر السياسة و القانون، جامعة قاصدي مرباح ورقلة، العدد11، الجزائر، 2014، ص122.

سرعة القيام بتدمير الدليل الرقمي دون أي اثر، كل ذلك ينعكس سلبا على الاقتصاد الوطني، فتكاليف التحقيق و التحري في حد ذاتها تستنزف الاقتصاد.[1]

الفرع الثالث: التكلفة الاقتصادية للجرائم المعلوماتية

لا تزال "ثقافة الأمن الإلكتروني" ضعيفة أو غائبة لدى الأفراد وعديد من الشركات في عالمنا المعاصر، على الرغم من الخسائر الضخمة، التي بات الاقتصاد الدولي يتعرض لها أخيرا نتيجة جرائم الإنترنت الاقتصادية، التي ترى بعض التقارير والدراسات أنها استفحلت للحد، الذي جعل منها "وباء" عالميا[2]، لذلك سف نتناول التكلفة الاقتصادية التي تتكبدها الدول بفعل الجرائم المعلوماتية، ثم سنتناول التكلفة الاقتصادية التي تتكبدها الشركات بفعل الجرائم المعلوماتي.

اولا: التكلفة الاقتصادية التي تتكبدها الدول بفعل الجرائم المعلوماتية

تكلف الجرائم الالكترونية الاقتصاد العالمي 445 مليار دولار سنويا و تتراوح بين385 مليار دولار كحد ادنى و 575 دولار كحد اعلى[3]، قال المدير العام ورئيس مجلس إدارة صندوق النقد العربي عبد الرحمن بن عبدالله الحميدي إن التكلفة الإجمالية للتهديدات و الجرائم المعلوماتية على مستوى العالم تتجاوز6 تريليونات دولار في عام 2021 مسجلة ارتفاعا من نحو ثلاثة تريليونات دولار في عام 2015، وأوضح الحميدي في كلمة خلال المؤتمر السنوي الثالث لأمن المعلومات في القطاع المالي الذي افتتحت أعماله بالدوحة أن تكلفة تلك الجرائم رغم تفاوت تقديراتها حسب المصدر، تشير إلى أن الصناعة المالية والمصرفية تواجه تحديات غير مسبوقة تتمثل في جانب منها بالنمو المتسارع في استخدامات التقنيات المالية الحديثة، وأكد على أهمية بذل المزيد من الجهود لبناء إطار مؤسسي، يشمل آليات ووسائل فعّالة لإدارة المخاطر للمراقبة والمتابعة والتنسيق وتبادل المعلومات حول التهديدات المعلوماتية.[4]

[1]- مجدوب نوال و اخرين، المرجع السابق، ص56.
[2] -https://www.aleqt.com/2020/02/22/article_1767431.html.
[3] -Véronique Arène avec IDG NS, publié le 10 Juin 2014.
[4] -https://www.google.dz/url?sa=t&source=web&rct=j&url=https://www.alaraby.co.uk/6-.

اما بالنسبة لأكثر الدول عرضة للجرائم الالكترونية حسب تقرير أعدته RSA العالمية لأمن المعلومات، فإن الربع الرابع من سنة 2017 سجل أكبر فترة تمت فيها هجمات التصيد الالكتروني بحوالي 29347 هجمة أما الربع الاول لسنة 2018 يشهد هو الاخر حوالي 24581 هجمة الكترونية، فعدد الهجمات الالكترونية تحافظ عمى استقرار نسبي لها مما يدل على استمرا الظاهرة بشكل مكثف حتى سنة 2018، حسب نفس التقرير للربع الاول والثاني من سنة 2018 فإن الدول الاكثر استهدافا لهجمات صيد المعلومات هي الولايات المتحدة الامريكية وكندا، أما الدول الاكثر استضافة للهجمات هي الولايات المتحدة، كما شهدت بولندا واسبانيا زيادة في هجمات التصيد في الربع الثاني من 2018، مما دفعهما للوصول إلى أكثر خمس بلدان استهدافا، فرنساه الوافدة الجديدة لقائمة أفضل 10 بلدن استهدافا، فالربع الثاني لسنة 2018 شهد تغييرات مثيرة للاهتمام يشمل وافدون جدد لقائمة البلدان المستضيفة كبولندا واستراليا وماليزيا، كما سجمت روسيا انخفاض طفيف في عدد الهجمات التي استضافتها، أيضا سجلنا سقوط كل من الصين ولوكسمبورغ من القائمة للربع الثاني مما يدل على انخفاض محسوس للهجمات التي تعرض لها هذا الربع.[1]

[1] -rsa,"rsa quarterly fraud report"volume1,q1 2018,date of view:30/9/2018,p5,online:https://www.nu.co.za/images/docs/rsa-fraud-report-p1-2018.pdf.

جدول للدول المستهدفة والمستضيفة للهجمات المعلوماتية للربع الاول والثاني 2018

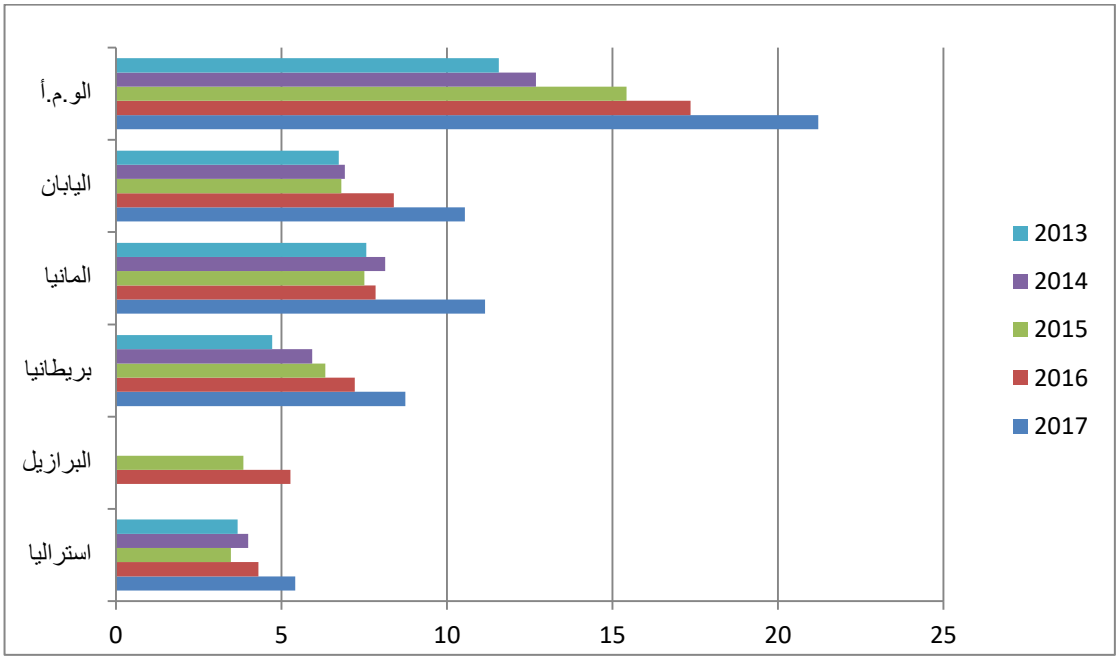
الدول المستضيفة للهجمات الالكترونية (الربع الاول 2018)		الدول المستهدفة من قبل الهجمات الالكترونية (الربع الاول 2018)		الدول المستضيفة للهجمات الالكترونية (الربع الثاني 2018)		الدول المستهدفة من قبل الهجمات الالكترونية (الربع الثاني 2018)	
1	الو.م.أ	1	كندا	1	الو.م.أ	1	كندا
2	روسيا	2	الو.م.أ	2	الهند	2	الو.م.أ
3	الهند	3	الهند	3	كندا	3	هولندا
4	استراليا	4	البرازيل	4	روسيا	4	الهند
5	كندا	5	هولندا	5	المانيا	5	اسبانيا
6	فرنسا	6	كولومبيا	6	هولندا	6	البرازيل
7	لوكسمبورغ	7	اسبانيا	7	استراليا	7	كولومبيا
8	المانيا	8	المكسيك	8	ماليزيا	8	فرنسا
9	الصين	9	المانيا	9	ايطاليا	9	البيرو
10	ايطاليا	10	جنوب افريقيا	10	فرنسا	10	المكسيك

rsa quarterly fraud report"volume1,q1 2018,date of view:30/9/2018,p5,online:https://www.nu.co.za/images/docs/rsa-fraud-report-p1-2018.pdf.

ثانيا: التكلفة الاقتصادية التي تتكبدها الشركات بفعل الجرائم المعلوماتية

أن اهم أثرين للجرائم المعلوماتية على الشركات هما الخسائر المالية الفادحة التي تلحق بهذه الشركات من جراء مثل هذه الجرائم، كذلك الخسائر التي تتكبدها الشركات لاقتناء وسائل الحماية والامن ضد الهجمات والجرائم المعلوماتية وخير دليل على ذلك الاحصائيات والارقام التي تبين حجم هذه الخسائر.[1]

شكل رقم (01): تطور حجم خسائر الجرائم المعلوماتية لستة دول خلال خمسة سنوات (مليون دولار امريكي)



Ponemo Institute, "2017 Cost of Cyber Crime Study", Date of view, 30/09/2018, online: https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrimeUS-FINAL.pdf

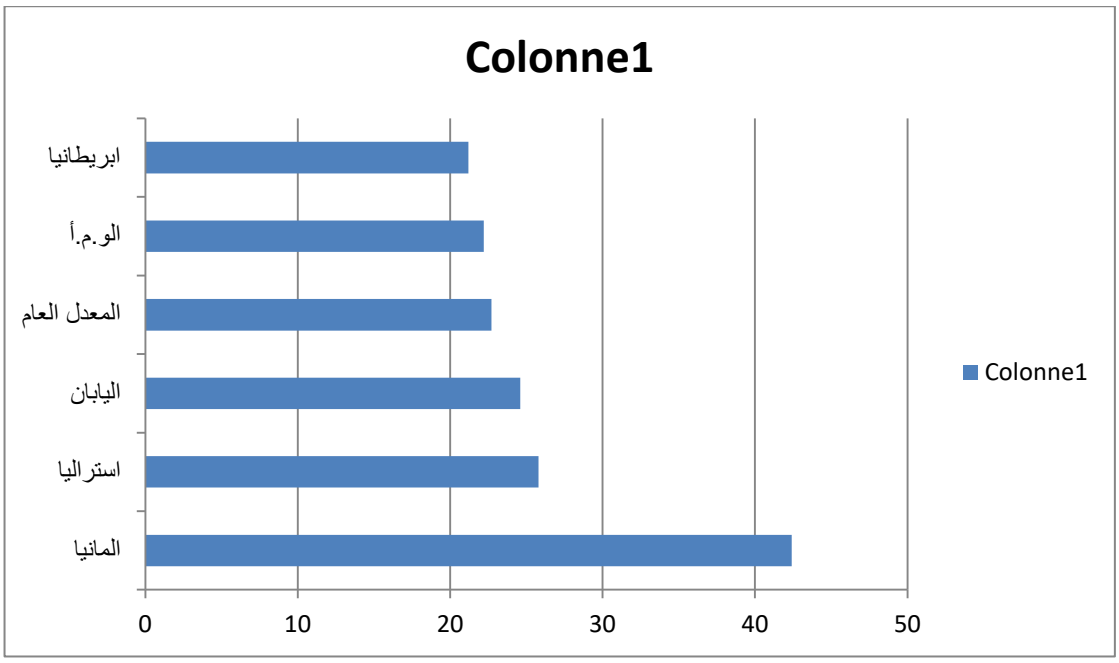
عند مراقبة اتجاهات التكلفة مع مرور الوقت لحوالي 237 شركة منفصلة، نلاحظ أن أعلى تكلفة على مدار الخمس سنوات تسجل دائما بالولايات المتحدة الامريكية وأدناها بأستراليا، على العموم تم تسجيل زيادة مستمرة في تكاليف الجريمة مع مرور الوقت فالولايات المتحدة الامريكية تطورت تكاليفها من11.56 مليون دولار سنة 2013 إلى 21.22 مليون دولار سنة 2017

[1]- وهيبة عبد الرحيم واخرين، الجرائم الالكترونية من خلال مؤشرات عالمية واثارها على المؤسسات، مجلة دراسات-issn:1112-4652- جامعة الاغواط، الجزائر، المجلد16، العدد01، 2019، ص42.

أي بزيادة تقدر حوالي 9.66 مليون دولار، في حين الزيادة في تكاليف وخسائر الجريمة بأستراليا مقارنة بين سنتي 2013 و2017 تقدر فقط بحوالي 1.74 مليون دولار فقط.

وحسب الشكل الموالي فإن أعلى نسبة ارتفاع لتكاليف الجريمة المعلوماتية سجل بين سنتي 2016و2017 في ألمانيا بحوالي 24.2%، تليها استراليا بحوالي 25.8% ثم اليابان 24.6%، وأدناها سجلت في بريطانيا 21.2%. [1]

شكل رقم (02): نسبة الزيادة في تكلفة الجريمة المعلوماتية لمدة سنة واحدة على الشركات (2016-2017).



Ponemo Institute, "2017 Cost of Cyber Crime Study", Date of view, 30/09/2018, online: https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrimeUS-FINAL.pdf

وحسب نفس التقرير فإن الشركات التي تتبنى أجهزة أمنية مشددة ومبتكرة ضد الجريمة الالكترونية يبلغ متوسط تكلفة الجريمة 7.9 مليون دولار بينما الشركات التي تتبنى أجهزة أمنية منخفضة فإن متوسط التكلفة يرتفع عندها إلى 11.1 مليون دولار.

[1] - Ponemo Institute, "2017 Cost of Cyber Crime Study", Date of view, 30/09/2018, online: https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrimeUS-FINAL.pdf.

أما في تقريرها لعام 2017 أصبح قطاع الخدمات المالية الاكثر تكلفة بسبب الجرائم الالكترونية أين كلف القطاع 18.28 مليون دولار من الخسائر جراء الجرائم الالكترونية، لانه الاكثر استهدافا بالاضافة لقطاع المرافق والطاقة الذي تكبد خسائر قدرها 17.2 مليون دولار، هذا مقارنة بالقطاعات الاخرى كالشركات في علوم الحياة وقطاع النقل والاتصالات، وأقل قطاع تكبد خسائر بسبب الجرائم الالكترونية هو قطاع التعليم وقطاع حسن الضيافة (صناعة تعتمد على تعليم الشعوب كرم وحسن الضيافة لتشجيع السياحة) والشكل الموالي يبين تكلفة الجريمة الالكترونية حسب القطاعات لسنة 2017.[1]

لمطلب الثاني: الاتفاقيات الدولية والاقليمية في مكافحة الجرائم المعلوماتية

لقد تنوعت الاتفاقيات على نوعها في تحديد الجريمة المعلوماتية، وتحديد سبل مكافحتها، في هذا الشق من الدراسة سنصب الاهتمام على مجموعة من الاتفاقيات الدولية والاقليمية التي قيل بها في هذا الصدد.

الفرع الاول: الاتفاقيات الدولية في مجال مكافحة الجريمة المعلوماتية

سنحاول في هذا الجزء من البحث الى التعرف الى اهم الاتفاقيات الدولية التي جاءت في مكافحة الجريمة المعلوماتية.

اولا: اتفاقية برن لمكافحة الجريمة المعلوماتية

تعد اتفاقية برن التي تم التوقيع عليها في عام 1971 في سويسرا[2]، حجر الاساس في مجال الحماية الدولية لحق المؤلف، قد وقعت على هذه الاتفاقية 120 دولة، وتعد المادة التاسعة من هذه الاتفاقية هي الاساس لأنها تنص على منح اصحاب حقوق المؤلف حق استئثاري، في التصريح بعمل نسخ من هذه المصنفات بأي طريقة وبأي شكل كان.[3]

---

[1] -Ponemon Institute,"2017 cost of cyber crime study", p14, op.cit.

[2]- المرسوم الرئاسي رقم 79-341 المؤرخ في 13-09-1997 المتضمن انضمام الجزائر مع التحفظ الى اتفاقية برن المؤرخة في 09-09-1869، المتممة في باريس 04-05-1909، المعدلة في 28-09-1997، ج ر عدد 01، المؤرخة في 14-09-1997.

[3]- بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، اطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر 01، 2018، ص14.

قد عرفت هذه الاتفاقية عدة تعديلات، حيث جاءت اتفاقية باريس مكملة لها في ماي 1896، المعدلة في برلين 13 سبتمبر 1908، المكملة ببرن في 20 مارس 1914، المعدلة بروما في جوان 1928، وبروكسل سنة 1948، وستوكهولم في جولية 1967، وباريس في جولية 1971، حيث تشكل الدول الاطراف في هذه الاتفاقية اتحادا لحماية حقوق المؤلف على مصنفاتهم الادبية والفنية.[1]

فضلا عن ذلك تمنح اتفاقية برن صاحب الحق المؤلف الحق في ان يرخص او يمنع أي ترجمة او اقتباس او بث اذاعي او توصيل الى الجمهور لمصنفه، وكذلك تلزم الاتفاقية بتوقيع جزاءات سواء كان المؤلف المتعدى عليه وطنيا او اجنبيا.[2]

يرجع الاهتمام بحق المؤلف الى انه الوسيلة القانونية الرئيسية لحماية حقوق المؤلف، فحق المؤلف من اهم الحقوق التي تكفلها النظم القانونية على اختلافها للمبدعين والمؤلفين حماية لإبداعاتهم الفكرية، ان لم يكن اهمها على الاطلاق، يوفر هذا الحق بشروط معينة لمؤلفي مصنفات معينة في الآداب والعلوم والفنون، أيا كان نوع هذه المصنفات، او اهميتها، او طريقة التعبير عنها او الغرض من تصنيفها حماية قانونية لا بأس بها لمدة زمنية معينة.[3]

ان اتفاقية برن كأي اتفاقية دولية تقوم على مجموعة من المبادئ الاساسية، التي تحدد نطاق الحماية الواجبة واسلوب تطبيقها، هذه المبادئ لا تتغير مع التعديلات او البروتوكولات التي قد يتم ادخالها على الاتفاقية ويتم حصرها في مبدأين هامين هما:

مبدأ المعاملة الوطنية الذي يقصد به تمتع جميع المصنفات الخاضعة لحماية الاتفاقية في اقليم أي دولة عضو في الاتفاقية، بنفس الحماية التي تتمتع بها المصنفات الوطنية لهذه الاخيرة لدى دولة اخرى طرف في اتفاقية برن.

---

[1]- محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة أيليزا للبحوث والدراسات، العدد2، المركز الجامعي ايليزا، الجزائر، 2017، ص36.

[2]- منير محمد الجنبيهي و ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الالي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، 2005، ص 201.

[3]- سعيداني سلامة، تطور التشريعات والاتفاقيات الدولية في مجال الجرائم المعلوماتية (وقائع ومقاربات)، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، العدد 10، المجلد 01، 2018، ص201.

كما نجد كذلك مبدأ الحد الادنى من الحماية الذي حاول من خلاله واضعو اتفاقية برن توحيد مستوى الحماية التي تتمتع بها المصنفات، من خلال وضع حد ادنى لحمايتها، لأجل ضمان ان لا يقل مستوى الحماية في أي دولة متعاقدة، ذلك لأجل مواجهة التفاوت التشريعي بين مستويات الحماية في الانظمة القانونية المختلفة.[1]

ثانيا: اتفاقية تريبس لمكافحة الجريمة المعلوماتية

لقد حظيت حقوق الملكية الفكرية لحماية خاصة، على المستوى الدولي نظرا للكم الهائل من الاتفاقيات والمعاهدات المبرمة بشأنها، لقد ازداد مجال الاهتمام دوليا بهذه الحقوق خاصة بعد انشاء منظمة التجارة العالمية، في 15 افريل 1994، ووجود اتفاقية سميت باتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية، والمعروفة اختصارا باتفاقية تريبس، هي تمثل بلا شك من اهم الاتفاقيات الدولية على الاطلاق، نظرا لما استحدثته من احكام موضوعية جاءت مغايرة ومختلفة عما جاءت به باقي الاتفاقيات الدولية، التي سبقتها في هذا الموضوع، خاصة ما يتعلق بموضوع الملكية الفكرية.[2]

وجاءت الاتفاقية متكونة من دباجة وثلاث وسبعين مادة، جاءت موزعة على سبعة اجزاء، قد جاءت بأحكام تفصيلية هدفها الاساسي هو تحرير التجارة العالمية.[3]

وان اهم ما تضمنته اتفاقية تريبس هي مجموعة الاجراءات الهامة والفعالة، لردع الاعتداءات على حقوق الملكية الفكرية[4]، كما انها ومن جهة اخرى تفرض على الدول اتخاذ العديد من التدابير الهامة لمعالجة الوضع، ومن تلك التدابير على سبيل المثال لا الحصر، اعطاء الحق للسلطات في اصدار الاوامر، بشأن حملات مفاجئة لضبط ادلة ارتكاب الجريمة،

[1]- رشا علي الدين، النظام القانوني لحماية البرمجيات، دار الجامعة الجديدة، الاسكندرية، 2007، ص241.
[2]- عامر محمود الكسواني، الملكية الفكرية، ط1، دار وائل للنشر، الاردن، 2011، ص14.
[3]- عبد الرحيم عنتر عبد الرحمان، حقوق الملكية الفكرية واثارها الاقتصادية، ط1، دار الفكر الجامعي، مصر، 2007، ص120.
[4]- حواس فتيحة، حماية المصنفات الرقمية واسماء النطاقات على شبكة الانترنت، اطروحة دكتوراه، جامعة الجزائر 01، 2016، ص127.

التي عادة ما تكون سهلة التخلص منها، لو لم تكن هناك سرعة في محاولة ضبطها وذلك للتحفظ على ادوات ارتكاب الجريمة، ذلك فضلا عن فرض عقوبات جنائية رادعة.[1]

ولفعالية هذه الاجراءات اشترطت الاتفاقية على الدول الاعضاء لحماية حقوق الملكية، المنصوص عليها في هذه الاتفاقية، بهدف تسهيل اتخاذ تدابير فعالة ضد أي تعدي على حقوق الملكية الفكرية، التي تناولتها الاتفاقية، يجب اتخاذ اجراءات سريعة لمنع التعديات والانتهاكات الحالة في المادة 41 من الاتفاقية.

هذا ونصت المادة التاسعة من الاتفاقية على انه على الدول الاعضاء فيها الالتزام بأحكام المواد من 01 الى 21 من معاهدة برن لسنة 1971، مع مراعاة ان الحماية تسري على المنتوج وليس الافكار فقط، كما نصت على الحماية الزمنية لهذه المصنفات وحددتها بمدى حياة المؤلف بالإضافة الى مدة خمسين عاما بعد وفاته.[2]

قد اخذت اتفاقية تريبس بنفس المبادئ التي قامت عليها اتفاقية برن لسنة 1971، وهما مبدأ المعاملة الوطنية ومبدأ الحد الادنى من الحماية، مع اضافة مبدأين هما مبدأ الدولة الاولى للرعاية، الذي مفاده ان كل دولة عضو في الاتفاقية، اذا ما قامت بمنح أي ميزة تفضيلية معينة، يتعين عليها منح جميع الدول الاعضاء الاخرى نفس الميزة، ومبدأ المعاملة التفضيلية للدولة النامية، وهذا مراعاة لظروف هذه الاخيرة، حيث تراعي المرونة في تنفيذ احكامها على الصعيد الداخلي للدول النامية الاعضاء من اتفاقية تريبس، وتمكين هذه الدول من انشاء قاعدة تكنولوجية متطورة، تخدم مصالحها الاقتصادية.[3]

ثالثا: معاهدة الويبو لمكافحة الجرائم المعلوماتية

تم التوقيع على اتفاقية الويبو المنشأة للمنظمة العالمية للملكية الفكرية الويبو، في استوكهولم في 14 جولية 1967 ودخلت حيز التنفيذ سنة 1970 وعدلت سنة 1979، الويبو عبارة عن منظمة دولية حكومية اصبحت في عداد الوكالات المتخصصة التابعة لمنظومة الامم

[1]- سعيداني سلامة، المرجع السابق، ص201.
[2]- بدري فيصل، المرجع السابق، ص22.
[3]- مجدوب نوال واخرين، المرجع السابق، ص364-365.

المتحدة سنة 1974، قد بلغ عدد الدول الاعضاء في هذه المنظمة عام 1999 الى 177 دولة، وترتكز نشاطات واختصاصات هذه المنظمة، في دعم حماية الملكية الفكرية بفروعها، الملكية الادبية في جميع انحاء العالم بفضل تعاون الدول مع بعضها البعض في هذا المجال.[1]

وقد انقسمت معاهدة الويبو الى ثلاث معاهدات هي، معاهدة الويبو بشأن حق المؤلف، معاهدة الويبو بشأن الاداء والتسجيل الصوتي، معاهدة الويبو بشأن الحماية الدولية لحق المؤلف والحقوق المجاورة، تم التوقيع عليها في 20 ديسمبر 1996.[2]

الفرع الثاني: الجهود الاقليمية في مكافحة الجريمة المعلوماتية

تتجلى الجهود الاقليمية في مكافحة الجريمة المعلوماتية، في مجموعة المساعي التي بذلها المجلس الاوروبي، الذي برز دوره كعنصر فعال في مكافحة هذه الجريمة، لما فيه من ضمان في المحافظة على المعطيات الفردية، وكل ما يتعلق بالحياة الخاصة، يرجع السبب في ذلك في ان جميع الدول المنضمة الى المجلس الاوروبي هي دول متطورة علميا وتقنيا، الامر الذي دفعها في بذل جهد في مجال مكافحة الجريمة المعلوماتية.[3]

بالإضافة الى الجهود التي تبذلها جامعة الدول العربية، من خلال اعتمادها عبر امانة مجلس وزراء العدل العرب، لما سمي بقانون الامارات العربي الاسترشادي، لمكافحة جرائم تقنية المعلومات وما في حكمها، نسبة الى مقدم هذا المقترح، الممثل في دولة الامارات العربية المتحدة.[4]

[1]- محمود عبابنة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر والتوزيع، الاردن، 2009، ص160.
[2]- بدري فيصل، المرجع السابق، ص21.
[3]- سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، جامعة باتنة، 2013، ص27.
[4]- بدري فيصل، المرجع السابق، ص27.

اولا: معاهدة بودابيست لمكافحة الجرائم المعلوماتية والاتصالات

شهدت العاصمة المجرية بودابيست في اواخر عام 2001 ميلاد اولى معاهدات الدولية التي تكافح جرائم الانترنت، وتبلور التعاون والتضامن الدولي في محاربتها، ومحاولة الحد منها خاصة بعد ان وصلت تلك الجرائم الى حد خطير اصبح يهدد الاشخاص والممتلكات.[1]

ولقد تم صياغة هذه المعاهدة من جانب عدد كبير من الخبراء القانونيين، في مجلس اوروبا، وبمساعدة دول اخرى لا سيما الولايات المتحدة الامريكية، وبعد مشاورات عديدة بين الحكومات واجهزة الشرطة وقطاع الكمبيوتر على مستوى العالم، وهو الامر الذي ادى في النهاية الى التوقيع عليها من قبل ثلاثين دولة بتاريخ 23 نوفمبر 2001 في العاصمة المجرية بودابيست، ذلك لمواجهة الاستخدام غير المشروع للحسابات، وشبكات المعلومات فيما يعرف بالأجرام الالكتروني او الاجرام المعلوماتي او الجرائم المعلوماتية.[2]

حيث تم التوقيع عليها من طرف ثلاثون دولة في العاصمة المجرية بودابيست نذكر منها دول الاعضاء في الاتحاد الاوروبي، كندا، اليابان، جنوب افريقيا، امريكا، و جاءت هذه الاتفاقية لتعالج اشكالية دول الجريمة المعلوماتية، وتجاوزها للحدود الدولية، بما يساعد الدول على مكافحة هذه الجريمة وتعقب مرتكبيها، والمساعدة على الاستدلال عليهم وضبطهم، كما تحدد افضل الطرق الواجب اتباعها في التحقيق، في جرائم الانترنت التي تعهد الدول الموقعة بالتعاون الوثيق من اجل مكافحتها.[3]

وقد اشتملت الاتفاقية الاوروبية لجرائم الحاسوب الالي والانترنت المسماة باتفاقية بودابيست الموقعة في 23-11-2001 على خمسة عناوين علي كالاتي:

1- الجرائم التي تمس سرية وامن وسلامة وتوفير بيانات الحاسوب، ومنظوماته وهي تضم الدخول غير المشروع، والاغراض غير المشروعة، وتدخل في البيانات، والتدخل غير المشروع في المنظومة، واساءة استخدام الاجهزة.

[1]- منير محمد الجنبيهي و ممدوح محمد الجنبيهي، المرجع السابق، ص96.
[2]- محمد علي العريان، الجرائم المعلوماتية، دار الجامع الجديدة، الاسكندرية، 2011، ص25.
[3]- محمد سعيد الزناتي، المرجع السابق، ص37.

2- الجرائم المتصلة بالحاسوب الالي، تضم جريمة التزوير المتعلقة بالحاسوب، وجريمة التدليس المتعلقة بالحاسوب.

3- الجرائم المتصلة بالمواد الاباحية للأطفال، الانتاج او النشر غير المشروع للمواد الاباحية، وصور الاطفال الفاضحة.

4- الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المرتبطة بها طبع والنشر.

5- اما العنوان الاخير فخصص للمسؤولية و الجزاءات، وهو يشتمل على بنود اضافية بشأن الشروع والاشتراك، وايضا الجزاءات او التدابير، ذلك طبقا للاتفاقيات او المعايير الدولية الحديثة بالنسبة لمسؤولية الاشخاص المعنوية.[1]

وقد ركزت اتفاقية بودابيست على ثلاث عناصر اساسية:

أ- يتمثل في اهمية التدابير التشريعية الموضوعية أي نصوص التجريم الموضوعية.

ب- يتمثل في اهمية التدابير التشريعية الاجرائية المتلائمة مع طبيعة الجرائم المعلوماتية أي النصوص الاجرائية.

ج- يتمثل في اهمية التدابير التعاون الدولي والاقليمي، في مجال مكافحة الجرائم.[2]

لقد قام واضعوا الاتفاقية بتحديد الاطار العام لهذه الجرائم، والمتمثل في الدخول غير المشروع او الاعتراض غير المشروع او الاعتداء على سلامة البيانات او النظام المعلوماتي، كذلك اساءة استخدام اجهزة الحاسبات او التزوير المعلوماتي او الغش المعلوماتي، وقد اوجبت اتفاقية بودابيست بعض الشروط حتى تأخذ الأفعال المنصوص عليها فيها وصف الجريمة، سنرددها كالاتي:

- ان ترتكب الجرائم المنصوص عليها في صلب الاتفاقية دون وجه حق.

[1]- محمد السعيد زناتي، المرجع السابق، ص37.
[2]- بدري فيصل، المرجع السابق، ص29.

– ان ترتكب الجرائم المنصوص عليها في الاتفاقية بطريقة عمدية، من اجل اقرار المسؤولية الجنائية.[1]

ثانيا: القانون العربي النموذجي الاسترشادي لمكافحة الجريمة المعلوماتية

يعد القانون العربي النموذجي لمكافحة جرائم الكمبيوتر، خطوة فعالة في مجال مكافحة الجريمة المعلوماتية، ومسلك منطقي وضروري لا بد من اتخاذه، لأن المجتمعات العربية ليست بمنأى عن هذه الجريمة الجديدة، كما ان ارتباط الدول ببعضها البعض في شتى مجالات الحياة بفضل التطور المعلوماتي الذي وصل اليه العالم اليوم يفرض ضرورة التعامل المثلي، في مواجهة الجريمة بصفة عامة والجريمة المعلوماتية بصفة خاصة، نظرا لخصوصيتها وميزاتها التي من اهمها كونها جريمة متعدية الحدود.[2]

وقد اعتمد مجلس وزراء العدل العرب، قانون الامارات العربي لمكافحة جرائم تقنية المعلومات وما في حكمها لسنة 2004، في دورته التاسع عشرة، والذي جاء متكون من 27 مادة.[3]

واعقبه بعد ذلك مجلس وزراء الداخلية العرب في الدورة الحادية والعشرون، ثم بعد ذلك طلب من الامانة العامة التابعة لجامعة الدول العربية تعميمه، على وزارات الداخلية للدول العربية الاعضاء للاستفادة منه، بالرغم من وجاهة القانون الا ان معظم الدول العربية، لم تواكبه بتشريعات داخلية تفعل القانون.[4]

من الجرائم المعلوماتية التي نص عليها القانون العربي النموذجي، نجد جريمة غسيل الاموال عبر الوسائط الالكترونية، التي نصت عليها المادة التاسعة عشر منه[5]، وجريمة التزوير

[1]-محمد علي العريان، المرجع السابق، ص26.
[2]- بدري فيصل، المرجع السابق، ص33.
[3]- قرار مجلس وزراء العدل العرب في الدورة التاسعة عشر، الرقم495- د19- 2003/10/8.
[4]- نوفل علي عبد الله الصفو، جريمة انشاء موقع او نشر معلومات مخلة بالأداب العامة بوسائل تقنية المعلومات (دراسة مقارنة)، المجلة المصرية للدراسات القانونية الاقتصادية، عدد3، 2005، ص37.
[5]- بدري فيصل، المرجع السابق، ص35.

المعلوماتي التي نصت عليها المادة الرابعة من القانون النموذجي[1]، وجريمة اختراق النظم المعلوماتية التي نصت عليها المادة الثالثة منه[2]، وجريمة السرقة المعلوماتية التي نصت عليها المادة الرابعة عشر على سرقة المعلومات بتجريم كل من عملية نسخ ونشر المصنفات الفكرية او الادبية، او الابحاث العلمية او ما في حكمها، اذا ما ارتكبت دون وجه حق، بعقوبة الحبس التي يترك تقديرها وفقا لقانون كل دولة دون الاخلال بالنصوص الخاصة بالملكية الفكرية لكل بلد.[3]

ثالثا: الاتفاقية العربية لمكافحة جرائم تقينة المعلومات

جاءت هذه الاتفاقية في اطار تعزيز التعاون بين الدول العربية، في مجال مكافحة جرائم تقنية المعلومات التي تهدد امنها ومصالحها، وسلامة مجتمعاتها، يث عقدت هذه الاتفاقية بمدينة القاهرة بجمهورية مصر العربية بتاريخ 21 ديسمبر 2010، في اطار انعقاد مجلسي وزاء الداخلية والعدل العرب المشترك بمقر جامعة الدول العربية بالقاهرة، حررت هذه الاتفاقية في 43 مادة ضمن خمس فصول.[4]

[1]- نص المادة الرابعة من القانون النموذجي العربي: "كل من زور المستندات المعالجة اليا او البيانات المخزنة في ذاكرة الحاسوب او على شريط او اسطوانة مضغوطة او غيرها من الوسائط يعاقب وتترك العقوبة وفقا لتقدير الدولة".

[2]- تنص المادة الثالثة من القانون النموذجي العربي: "كل من توصل لطريقة التحايل لأختراق نظم المعالجة الالية للبيانات يعاقب بالحبس و الغرامة وتترك العقوبة لتقدير الدولة".

[3]- بدري فيصل، المرجع السابق، ص38.

[4]- محمد السعيد الزناتي، المرجع السابق، ص38.

الخاتمة

الخاتمة

وفي الختام تعد المعلومات سمة حديثة من قبل الدول والافراد وبات استخدام الانظمة المعلوماتية المقياس الذي يحدد مدى تطور الشعوب وتقدمها، حيث خلف عصر المعلوماتية آثار إيجابية إلى جانب السلبية نجمت عن استغلال بعض الافراد والجهات للتقنيات المعلومات في غير الغرض الذي جاءت من أجله لذلك من المتوقع أن الجريمة المعلوماتية ستستمر وتطغى على ساحة الاجرام بقدر كبير وستطور مع مرور الوقت إلى ما هو أخطر وأعقد انه يتطلب تدخلا تشريعيا سريعا من أجل وضع حماية قانونية متكاملة وسد جميع الثغرات والتي ينبغي أن تطور لمواكبة نظم المعلومات.

لقد أصبح الوضع أكثر تعقيدا، حيث صاحب تلك الثورة أداة رئيسية هي الحاسب الالي المربوط بالشبكة العنكبوتية العالمية، مما سهل اختراق المعلومات، استخدامها وإفشائها الى الاطراف المنافسة بغرض الاضرار بهم.

ومن ثم انتقل الوضع من كونه محليا الى كل أحناء العالم ليمس أغلب الميادين لا سيما عالم الاقتصاد، وتفاقم الى درجة أثقلت كاهل الفكر القانوني والاقتصادي، مما أدى بتكاتف الجهود الدولية في محاولة بلورة ورسم قانون دولي يحمل في طياته أدوات كانت نتيجة دراسات نخبة من العلماء والخرباء، عسى الوصول الى معلم يضبط تلك الاستخدامات اللامحدودة التي أضحت هاجس المجتمع المعلوماتي الذي كلف اضرارا متفاوتة، و تحقيق ذلك التوازن ومحو تلك التناقضات هو غاية طمح إليها أغلب مفكري الاقتصاد خاصة كون أن وسطهم كان الضحية الاكبر، ومن خالل دراستنا هذه نتوصل إلى هذه النتائج نحصلها فيما يلي:

* لم يتوصل او يتم الاتفاق على تعريف جامعا مانعا للجريمة المعلوماتية.

* أفرز التطور العلمي ظهور أنماط مستحدثة من المجرمين المعلوماتيين لم يكونوا موجودين من قبل.

* ارتبط ظهور أنماط مستحدثة من مرتكبي الجرائم بعد الاقتصار على ذات الدوافع في ارتكاب الجرائم التقليدية حيث ظهرت دوافع أيضا تتسم بالحداثة والغرابة حيث شملت إلى جانب تحقيق المكسب المادي والانتقام شملت أيضا التفوق العلمي والتسلية كدوافع جديدة ارتكاب الجرائم.

* بالنسبة للتزوير المعلوماتي والسرقة المعلوماتية فانه لا تكفي إسقاط النصوص التقليدية على مثل هذه الجرائم المستحدثة.

* تبين ان هناك نوعين من التصنيف للجرائم المعلوماتية، التصنيف التشريعي بالإضافة الى التصنيف الفقهي.

* هناك الكثير من النماذج الاجرامية المعلوماتية سواء التي ترتكب داخل انظمة المحاكة الالية، او ترتكب بواسطة النظام المعلوماتي.

* كما لاحظنه زيادة التكلفة الاقتصادية للجريمة المعلوماتية مع مرور الزمن نظرا للتطور وامكانية حصول الجميع على وسائل التواصل التي تمكنه من الاختراق والدخول بصورة غير مشروعة.

* مهما تعددت صور الجريمة المعلوماتية فان كل تلك الجرائم تستهدف الاقتصاد، وتحول دون تحقق التطور والتنمية الاقتصادية، سواء بطريقة مباشرة عن طريق ارتكاب الجريمة الاقتصادية الرقمية، او بطريقة غير مباشرة من خلال ما تتكبده الدول والشركات الاقتصادية من خسائر.

* كما ان الدول عملت على مكافحة الجريمة المعلوماتية سواء عن طريق الاتفاقيات الدولية والاقليمية للحد من الجريمة المعلوماتية.

* نلاحظ تكاتف الجهود الدولية في محاولة بلورة ورسم قانون دولي يحمل في طياته أدوات كانت نتيجة دراسات نخبة من العلماء والخبرباء، لعلى وعسى الوصول الى معلم يضبط تلك الاستخدامات اللامحدودة التي أصبحت هاجس المجتمع المعلوماتي الذي كلف اضرارا متفاوتة، و تحقيق ذلك التوازن ومحو تلك التناقضات هو غاية طمع إليها أغلب مفكري الاقتصاد خاصة كون أن وسطهم كان الضحية الاكبر.

كلما زادت العولمة الاقتصادية والتكنولوجيا تطورا زادت مواجهة الانشطة الاجرامية تعقيدا، ذلك أن المجتمع الدولي لا يزال مبنيا على وجود دول ذات سيادة تتبنى مفاهيم وقواعد عدة واسنادا إلى النتائج السابقة توصلنا إلى صياغة مجموعة من توصيات نريدها على الشكل التالي:

* ضرورة الاعتماد على تقنيات متطورة وحديثة من أجل الكشف عن هوية مرتكبي الجريمة والاستدلال عليه في أسرع وقت ممكن.

* يجب أن يتلاءم تعريف الجريمة المعلوماتية مع فكرة عالمية المعلومات والاتصالات، بحيث يكون متفقا عليه على المستوى العالمي خاصة مراعاة التطور التكنولوجي الحاصل يوما عن يوم، ويجب توضيح الدور الذي يقوم به الحاسب الآلي في ارتكاب الجريمة.

* مساعدة شركات التقنية والانترنت في اتخاذ اجراءات أمنية مناسبة سواء من حيث سلامة المنشآت أو ما يختص بقواعد حماية الاجهزة، والبرامج.

* البدء من عقد دورات مكثفة لعاملي مجال أنظمة المعالجة الالية للمعطيات وتطبيقات الحاسوب، والجرائم المرتبطة بها.

* ضرورة نشر الوعي بين مستخدمي الانترنت وكيفية تفادي التعدي على بياناتهم الشخصية، وتعريفهم حجم الخطورة التي ترصدهم في حالة عدم اتخاذ احتياطات اللازمة.

* على المؤسسات التي تعمل في محيط معرض للجرائم المعلوماتية كالبلدان المتقدمة، اقتناء برامج حماية متطورة منذ بداية تأسيسها حتى تحافظ على سمعتها.

* لابد على المؤسسات التفكير في احتمالية تعرضها للجرائم المعلوماتية، وعدم الثقة بانها بعيدة كل البعد عن ذلك فهي جريمة عابرة للقارات وتحدث دون اشعار مسبق.

* البدء من ضرورة إصدار تشريع لمكافحة الاجرام المعلوماتي وصوره، المختلفة وان يتضمن هذا التشريع النصوص الموضوعية، بالإضافة إلى النصوص الاجرائية مناسبة لتحقيق الجريمة المعلوماتية وأسباب ارتكابها.

* ضرورة إيجاد قاعدة تعاون دولي فيما يتعلق بالجريمة المعلوماتية للتوفيق بين التشريعات الخاصة بهذه الجرائم.

* وانطلاقا من كل ما سبق يمكن القول انه ان الاوان ليكون التجريم و العقاب ذو حركة و مرونة تتماشى والابعاد المستقبلية، باعتبار ان الجريمة المعلوماتية في تطور سريع، ناهيك عن ضرورة تظافر الجهود الرسمية للحد من مضار الجريمة المعلوماتية.

قائمة المصادر

والمراجع

اولا: قائمة المصادر

1- الاتفاقيات

1/ اتفاقية برن، لحماية حقوق المؤلف على مصنفاتهم الادبية والفنية، المؤرخة في 09-09-1869، المتممة في باريس 04-05-1909، المعدلة في 28-09-1997.

2/ اتفاقية بودابست، لمكافحة الجرائم المعلوماتية المنبثقة عن اجتماع المجلس الاوربي ببودابست، بتاريخ 21 /نوفمبر/2001، المجر تحت رقم 185.

3/ لاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المنبثقة عن اجتماع مجلس الوزراء الداخلية والعدل العرب بصفة مشتركة، بمقر الأمانة العامة لجامعة الدول العربية، بالقاهرة، مصر، بتاريخ 2010/12/21.

2- القوانين

1/ الامر رقم (16)، المتضمن قانون العقوبات الاردني، الصادر سنة 1960.

2/ الامر رقم (156/66)، المتضمن قانون العقوبات الجزائري، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 71، الصادر في 08 جوان 1966،المعدل والمتمم.

3/ الامر رقم (111)، المتضمن قانون العقوبات العراقي، الصادر سنة 1969 المعدل.

4/ قانون الاردني رقم 85 ، لسنة 2001 ، الجريدة الرسمية للمملكة الأردنية الهاشمية رقم 4524 ، الصادر بتاريخ 2001/12/31م.

5/ قانون إمارة دبي رقم 02، لسنة 2002، متعلق بالمعاملات والتجارة الإلكترونية، صادر بتاريخ 12/ فبراير/ 2002.

6/ المرسوم السعودي رقم م/17، المؤرخ في 1428/3/7هجري، المتضمن نظام مكافحة جرائم المعلوماتية، الصادر بتاريخ 1428/3/8هجري.

7/ القانون الجزائري رقم 09/04 ، المؤرخ في 05/شعبان/2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات إعلام واتصال ومكافحتها، الجريد الرسمية العدد 47 ، الصادر في 16/شعبان/ 2009.

8/ القرار الفلسطيني رقم 10، المتضمن قانون الجرائم الالكترونية الفلسطيني، الصادر بتاريخ 2018/04/17م.

ثانيا: قائمة المراجع

1-الكتب بالغة العربية

- احمد خليفة الملط، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، الاسكندرية، 2006.
- احمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، مصر، 2007.
- أحمد طه، الجرائم الناشئة عند استخدام الحاسب الالي دراسة مقارنة، دار النهضة العربية، القاهرة، 2000.
- أحمد فتحي سرور ، الوسيط في قانون العقوبات، القسم العام ، دار النهضة العربية ، القاهر ،2009.
- سامة احمد المناعسة و جلال محمد الزعبي، جرائم تقنية نظم المعلومات الالكترونية، ط2، دار الثقافة للنشر وتوزيع، عمان، 2014.

- أسامة احمد المناعسة، جرائم الحاسوب الآلي، دار وائل لنشر والتوزيع، عمان، 2001.
- أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية لمكافحة جرائم الكمبيوتر والانترنيت، مكتبة الوفاء القانونية، مصر، 2011.
- أمين طعباش، الحماية الجنائية المعاملات الالكترونية، ط1، الوفاء القانونية، الاسكندرية، 2015.
- أيمن عبد الحفيظ، الاتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية، ط 1، دار النهضة العربية للطبع والنشر والتوزيع، د.ب.ن، 2005.
- ايهاب فوزي السقا، الحماية الجنائية والامنية لبطاقات الائتمان، دار الجامعة الجديدة، الاسكندرية، 2007.
- ايهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، دار الجامعة الجديدة للنشر، الاسكندرية، 2008.
- جعفر حسن جاسم الطائي ، جرائم تكنولوجيا المعلومات ، دار البلدية ، عمان ، 2010.
- جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة)؛ دار الثقافة للنشر والتوزيع، الأُردن، 2010.
- جميل عبد الباقي الصغير، الانترنت والقانون الجنائي و الاحكام الموضوعية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة، 2001.
- جميل عبد الباقي الصغير، الانترنيت و القانون الجنائي، ط 1، دار النهضة العربية، القاهرة، 2000.
- حاتم عبد الرحمن منصور الشحات، الاجرام المعلوماتي، دار النهضة العربية، القاهرة، 2003.
- حسام محمد نبيل الشراقي، الجرائم المعلوماتية دراسة مقارنة على جرائم الاعتداء التوقيع الالكتروني، دار الكتب القانونية، مصر، 2013.
- حسام محمد نبيل الشنراقي، جرائم الاعتداء على التوزيع الالكتروني، ط1، دار الكتب القانونية، مصر، 2013.

- حسام محمد نبيل الشنراقي، جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، مصر، 2013.
- خالد داودي، الجريمة المعلوماتية، دار الإعصار العلمي للنشر وتوزيع ،ط 1، عمان، 2017 .
- خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنيت ، ط1 ، دار الثقافة للنشر و التوزيع، الاردن، 2011.
- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب و الانترنت، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان، 2011.
- رشا علي الدين، النظام القانوني لحماية البرمجيات، دار الجامعة الجديدة، الاسكندرية، 2007.
- طارق إبراهيم الدسوقى عطية، الامن المعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الاسكندرية، مصر، 2009.
- عامر محمود الكسواني، الملكية الفكرية، ط1، دار وائل للنشر، الاردن، 2011، ص14.
- عايد رجا الخلايلة، المسؤولية التقصيرية الالكترونية المسؤولية الناشئة عن اساءة استخدام اجهزة الحاسوب والانترنت دراسة مقارنة، ط1، دار الثقافة، عمان، 2009.
- عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات، ط1، دار المستقبل للنشر و التوزيع ، عمان، 2009.
- عبد الرحيم عنتر عبد الرحمان، حقوق الملكية الفكرية واثارها الاقتصادية، ط1، دار الفكر الجامعي، مصر، 2007.
- عبد العزيز سعد، جرائم التزوير وخيانة الأمانة واستعمال المزور، الطبعة الاولى، دار هومة، الجزائر، 2005.
- عبد الفتاح بيومي الحجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الكتاب للنشر، الإسكندرية، 2007.

- عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة دراسة في الظاهرة الاجرامية المعلوماتية، دار الفكر الجامعي، الاسكندرية، 2008.
- عبد الفتاح بيومي حجازي، الحكومة الالكترونية ونظامها، الكتاب الثاني، دار الفكر الجامعي، الاسكندرية، 2004.
- عبد الفتاح بيومي حجازي، النظم القانونية لحماية التجارة الإلكترونية، دار الفكر الجامعي، مصر، 2002.
- عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت في التشريعات العربية، ط1، دار النهضة العربية، القاهرة، بلا سنة طبع.
- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي، مصر، 2006.
- عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في الجريمة و المجرم ألمعلوماتي، دار الفكر الجامعي، مصر، 2000.
- عبد الفتاح مراد ، دور الكمبيوتر في مجال إرتكاب الجرائم الإلكترونية شرح جرائم الكمبيوتر والأنترنت، دار الكتب والوثائق المصرية، مصر، د.س.ن.
- عبد الله عبد الكريم عبد الله ، جرائم المعلوماتية والانترنت الجرائم الالكترونية، منشورات الحلبي الحقوقية، طبعة 1، بيروت ، 2007.
- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، ط1، الدار الجامعية للنشر والتوزيع الإسكندرية، 1992.
- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، ط3، الدار الجامعية للنشر و التوزيع، الاسكندرية، 1999.
- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، ط2، دار الجامعة الجديدة للنشر، القاهرة، 1997.
- علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة(دارسة مقارنة)، منشورات زين الحقوقية، لبنان، 2013.

- عمر محمد أبو بكر بن يونس ، الجرائم الناشئة عن إستخدام الأنترنت، دار النهظة العربية ، 2004.
- عوض محمد عوض، قانون الإجراءات الجنائية، ج1 ،مؤسسة الثقافة الجامعية، القاهرة، 1989.
- كامل فريد السالك، الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية، حلب، 2000.
- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الالي في التشريع الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية، 2007.
- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية، مصر، 1998.
- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، القاهرة، دار النهضة العربية، 1994.
- محمد عبد الله أبو بكر، موسوعة جرائم المعلومات (جرائم الكمبيوتر والانترنت)، المكتب العربي الحديث، الإسكندرية، 2011.
- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشرع لشبكة الإنترنت، ط2 ،دار النهضة العربية، القاهرة، 2009.
- محمد علي العريان، الجرائم المعلوماتية، دار الجامع الجديدة، الاسكندرية، 2011.
- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديد للنشر، كلية الحقوق جامعة الإسكندرية، الإسكندرية، 2004.
- محمد عودة الجبور، الجرائم الواقفة على الاموال، ط1 ،دار النفائس، الاردن، 2011.
- محمد محمود المكاوي، الجوانب الأخلاقية والمهنية للحماية من الجرائم المعلوماتية، ط1، المكتبة العصرية للنشر والتوزيع مصر، 2010.
- محمود احمد عبابنة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر وتوزيع، عمان، 2009.

- محمود عبابنة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر والتوزيع، الاردن، 2009.
- محمود نجيب حسني، شرح قانون العقوبات، القسم العام، ط2، دار النهضة العربية، القاهرة، 1984.
- مصطفى يوسف كافي، جرائم الفساد غسيل الاموال السياحة الارهاب الالكتروني المعلوماتية،ط1، مكتبة المجتمع العربي، عمان، 2014.
- معن احمد محمد الحياري، الركن المادي للجريمة، ط1 ،منشورات الحلبي الحقوقية، لبنان، 2010.
- منير محمد الجنبيهي و ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الالي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، 2005.
- مين طعباش، الحماية الجنائية للمعاملات الالكترونية، ط1، مكتبة الوفاء القانونية، الاسكندرية، 2005.
- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، د.ط، بيروت، منشورات الحلبي الحقوقية، 2005.
- نبيلة هبة هروال ، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع إستدلالات (دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية، 2013.
- نسرين عبد الحميد نبيه، الجريمة المعلوماتية و المجرم ألمعلوماتي، منشأة المعارف، جلال حزي و شركائه، الإسكندرية، 2008.
- نهلا عبد القادر المومني ، الجرائم المعلوماتية ، ط1 ، دار الثقافة للنشر و التوزيع ، عمان ، 2008.
- نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2، دار الثقافة للنشر و التوزيع، الاردن، 2010.
- هدى حامد قشقوش، جرائم الحاسوب الالي في التشريع المقارن، ط1، دار النهضة العربية، القاهرة، 1992.
- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، الطبعة الاولى، مكتبة الآلات الكاتبة، أسيوط، 1995.

- هلالي عبد الله احمد، اتفاقية بودابست لمكافحة الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2007.
- واثبة داود السعدي، قانون العقوبات، القسم الخاص، بغداد، 1989.
- وائل محمد نصيرات و غادة عبد الرحمن الطريفي، جريمة الاحتيال عبر شبكة المعلمات الدولية دفاتر السياسة والقانون، السعودية، 2018.
- يوسف حسن يوسف، الجرائم الدولية للإنترنيت، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2011.
- يونس عرب، دليل امن المعلومات و الخصوصية (جرائم الكمبيوتر و الانترنت)، إتحاد المصارف، الجزء الأول، الأردن، 2002.

2- الاطروحات والمذكرات العلمية

أ- اطروحات الدكتوراه

- بدري فيصل، مكافجة الجريمة المعلوماتية في القانون الدولي والداخلي، اطروحة دكتوراه في القانون العام، كلية الحقوق، جامعة الجزائر 01، 2018.
- حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه في علوم الحقوق، كلية الحقوق والعلوم السياسية ، جامعة باتنة، 2016.
- حواس فتيحة، حماية المصنفات الرقمية واسماء النطاقات على شبكة الانترنت، اطروحة دكتوراه، جامعة الجزائر 01، 2016.
- رابحي عزيزة، الاسرار المعلوماتية وحمايتها الجزائية، اطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة ابي بكر بالقايد، تلمسان، 2018/2017.
- شول بن شهر، الحماية الجنائية للتجارة إلكترونية، أطروحة دكتوراه في الحقوق، قسم الحقوق كلية الحقوق والعلوم السياسية ،جامعة محمد خيضر، بسكرة،2010 – 2011.

ب- مذكرات الماجستير والماستر

- أحمد كيلان عبد الله صكر، الجرائم الناشئة عن إساءة استخدام الحاسوب، رسالة ماجستير، مقدمة إلى كلية القانون، جامعة بغداد، 2002.
- امال دكومي، الجريمة المعلوماتية واثارها على النمو الاقتصادي، مذكرة ماستر في القانون الجنائي للأعمال، جامعة العربي بن مهدي، كلية الحقوق والعلوم السياسية قسم الحقوق، ام البواقي، 2015/2014.
- جزار منصورية، الجريمة المعلوماتية، مذكرة ماستر في الحقوق، تخصص علم الإجرام والعلوم الجنائية، جامعة عبد الحميد بن باديس، 2016-2017.
- حاجب هيام، الجريمة المعلوماتية، مذكرة التخرج لنيل اجازة المدرسة العليا للقضاء، الجزائر، 2005_2006.
- حمزة بن عقون، السلوك الاجرامي للمجرم المعلوماتي، رسالة ماجستير في العلوم القانونية، جامعة العقيد الحاج لخضر، باتنة، كلية الحقوق و العلوم السياسية، 2011- 2012.
- حمزة بن عقون، السلوك الإجرامي للمجرم ألمعلوماتي، رسالة ماجستير في العلوم القانونية، تخصص علم الإجرام و العقاب، جامعة باتنة، 2012/2011، ص14، نقلا عن يونس عرب، دليل أمن المعلومات والخصوصية.
- خديجة دحمان صبايحية، جرائم السرقة والاحتيال عبر الانترنيت، دراسة مقارنة بين الفقه الجزائري، رسالة الماجستير في العلوم الاسلامية، تخصص شريعة وقانون الشريعة العلوم الاسلامية، جامعة الجزائر،2013/2012.
- دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري المقارن، رسالة ماجستير، جامعة منتوري قسنطينة، 2013.
- سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، جامعة باتنة، 2013.

- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير في العلوم القانونية، جامعة الحاج لخضر، باتنة، 2012-2013.
- سمير إبراهيم جميل الغزاوي، المسؤولية الجنائية الناشئة عن استخدام الانترنيت، رسالة ماجستير مقدمة الى كلية القانون، جامعة بغداد، 2005.
- صغير يوسف، الجريمة المرتكبة عبر الأنترنت، رسالة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2013 ،ص09 ،نقلا عن كحلوش علي، جرائم الحاسوب وأساليب مواجهتها مجلة صادرة عن مديرية الأمن الوطني، العدد84 ،2007.
- عبد الجبوري و سامر سلمان، جريمة الاحتيال الالكتروني، رسالة ماجستير مقدمة الى كلية الحقوق ، جامعة البحرين،2014.
- عبد اللطيف معتوق، إطار القانوني لمكافحة الجرائم المعلومات في التشريع الجزائري، رسالة ماجستير في العلوم القانونية، جامعة العقيد لخضر، باتنة، 2011-2012.
- عبد الله بن حسين آل حجراف القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية، رسالة ماجستير في قسم العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض.
- عمر عبد السلام حسين الجبوري، جريمة التزوير الالكتروني في التشريع الاردني (دراسة مقارنة)، رسالة ماجستير في القانون العام، كلية الحقوق ، جامعة الشرق الاوسط، الاردن، 2017.
- فتحية رصاع ، الحماية الجنائية للمعلومات على شبكة الإنترنت ، رسالة ماجستير في القانون العام ، كلية الحقوق والعلوم السياسية ، جامعة أبي بكر بلقايد ، تلمسان ، 2001/ 2012.
- لعاقل فريال، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة ماستر في القانون العام، جامعة أكلي محند اولحاج – البويرة، 2014/2015.

- معتوق عبد اللطيف، الاطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، رسالة ماجستير في العلوم القانونية، جامعة العقيد الحاج لخضر، باتنة، كلية الحقوق و العلوم السياسية، 2011-2012.
- نجا بن مكي، السياسة الجنائية لمكافحة الجرائم المعلوماتية، رسالة ماجستير في القانون الدولي، معهد العلوم القانونية والإدارية، قطب خنشلة، 2009/2008.
- ياسين بوعروة، جريمة التزوير المعلوماتي، مذكرة ماستر في القانون الجنائي للاعمال، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة العربي بن مهدي، ام البواقي، 2014/2013.ذ
- يوسف مناصرة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، رسالة ماجستير، جامعة الجزائر، كلية الحقوق، 2009/2008.

3- المقالات

- بسام احمد الزلمي و عبود السراج، دور النقود الالكترونية في عمليات غسل الاموال، مقال منشور مجلة العلوم الاقتصادية و القانونية، جامعة دمشق، المجلد رقم 36، العدد 01، 2010.
- بن بادرة عبد الحليم، اجراءات البحث والتحري عن الجريمة المعلوماتية – الخصوصية والاشكالات، مجلة الحقوق والعلوم السياسية، العدد 23، الجزائر، 2015.
- زوزو هدى، التسريب كأسلوب من اساليب التحري في قانون الاجراءات الجزائية الجزائري دفاتر السياسة و القانون، جامعة قاصدي مرباح ورقلة، العدد11، الجزائر، 2014.
- سعيداني سلامة، تطور التشريعات والاتفاقيات الدولية في مجال الجرائم المعلوماتية (وقائع ومقاربات)، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، العدد 10، المجلد 01، 2018.
- صراح كريمة و دقيش جمال، الابعاد التسويقية، مجلة الدراسة التسويقية، مجلد رقم 02، عدد01، 2018.

- فايز الظفيري، الأحكام العامة للجريمة الإلكترونية، بحث منشور في مجلة العلوم القانونية والاقتصادية، العدد الثاني، 2002.

فلالي رشيد، الشروق تقضي يوم مع أشهر قراصنة الإنترنت في الجزائر، عدد صادر في 22 نوفمبر 2008، مقال متوفر على الموقع: http://www.echoroukonline.com/ara/?news=29084

- فيصل فهد، انتهاك الخصوصية، مقال منشور بمجلة الامن و الحياة، الصادر عن اكاديمية نايف للعلوم الامنية، العدد 378، السعودية، 2013.
- محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة أيليزا للبحوث والدراسات، العدد2، المركز الجامعي ايليزا، الجزائر، 2017.
- محمد جوهر، خصوصية زجر الاجرام المعلوماتي، المجلة المغربية للقانون والاقتصاد والتسيير، العدد52، المغرب، 2006.
- نوفل علي عبد الله الصفو، جريمة انشاء موقع او نشر معلومات مخلة بالأداب العامة بوسائل تقنية المعلومات (دراسة مقارنة)، المجلة المصرية للدراسات القانونية الاقتصادية، عدد3، 2005.
- هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، بحث منشور في مجلة العلوم القانونية والاقتصادية، العدد2، 1993.
- هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، بحث منشور في مجلة العلوم القانونية والأقتصادية، العدد2، 1993.
- وهيبة عبد الرحيم واخرين، الجرائم الالكترونية من خلال مؤشرات عالمية واثارها على المؤسسات، مجلة دراسات-issn:1112-4652- جامعة الاغواط، الجزائر، المجلد16، العدد01، 2019.

4- الملتقيات

- دورثي إي دينغ، قراصنة أنظمة الكمبيوتر إعداد، ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر،واشنطن، ترجمة : آمنة علي يوسف، ديسمبر 1998.
- عرب يونس، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، 2002.
- محمد سامي الشوا، الغش المعلوماتي ظاهرة اجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة.

5- المواقع الالكترونية

- www.oecd.orgموقع منظمة التعاون الاقتصادي والتنمية.
- https://www.aljazeera.net/news/politics/2020/12/23.
- Https://universitylifestyle.net/7/4/2021.
- https://platform.almanha.com/files/2/115333.
- www.minishawi.com.
- www.chawkhtabib.info/spip.php.articlc478.
- http://www.4algeria.com.
- https://www.startimes.com/?t=16193884.
- https://www.aleqt.com/2020/02/22/article_1767431.html.
- https://www.google.dz/url?sa=t&source=web&rct=j&url=https://www.alaraby.co.uk/6-.

6- الكتب باللغة الاجنبية

- Michael (J) Privacy and Human Rights: An international and comparative study wide special reference to developments in information technology. Dartmouth (1994).p.12.

- Loi n°88-19 du 05 janvier 1988 relative à la fraude informatique, JORF du 06 janvier 1988 (LOI Godfrain).
- Vivant et autres: Informatique et droit pénal. Les biens informatiques objets de fraude Lamy informatique.1991.n°3445.p1511.
- Roden (adrian), computer crime and the law, C.L.J ..,1991,vol.15,p.399.
- Parker (Donn B) Figding computer crime A neur Framework for protecting information 1998/P 11.
- Véronique Arène avec IDG NS, publié le 10 Juin 2014
- . rsa quarterly fraud report"volume1,q1 2018,date of view:30/9/2018,p5,online:https://www.nu.co.za/images/docs/rsa-fraud-report-p1-2018.pdf.
- Ponemo Institute, "2017 Cost of Cyber Crime Study", Date of view, 30/09/2018online: https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrimeUS-FINAL.pdf.

فهرس

الموضوعات

فهرس الموضوعات

فهرس الموضوعات	
العنوان	**الصفحة**
مقدمة	**02**
الفصل الاول: ماهية الجريمة المعلوماتية	
تمهيد	**07**
المبحث الاول: مفهوم الجريمة المعلوماتية	**08**
المطلب الاول: تعريف الجريمة المعلوماتية	**08**
الفرع الاول: موقف الهيئات الدولية والتشريعيات الوطنية من تعريف الجريمة المعلوماتية	**08**
اولا: تعريف الهيئات الدولية للجريمة المعلوماتية	**09**
ثانيا: تعريف التشريعات الوطنية للجريمة المعلوماتية	**11**
الفرع الثاني: التعريف الفقهي للجريمة المعلوماتية	**13**
اولا: التعرف الضيق للجريمة المعلوماتية	**13**
ثانيا: التعريف الواسع للجريمة المعلوماتية	**16**
الفرع الثالث: تطور الجريمة المعلوماتية	**18**
المطلب الثاني: خصائص ودوافع الجريمة المعلوماتية	**20**
الفرع الاول: خصائص الجريمة المعلوماتية	**20**
اولا: الجرائم المعلوماتية ترتكب بواسطة الانترنت	**20**
ثانيا: الجريمة المعلوماتية عابرة للحدود الوطنية	**20**
ثالثا: صعوبات اكتشاف الجريمة المعلوماتية	**21**
رابعا: الجريمة المعلوماتية جريمة ناعمة	**22**
الفرع الثاني: دوافع ارتكاب الجريمة المعلوماتية	**23**
اولا: الدوافع المادية لارتكاب الجريمة المعلوماتية	**23**

فهرس الموضوعات

ثانيا: دافع الانتقام لارتكاب الجريمة المعلوماتية	**24**
ثالثا: الدوافع الذهنية لارتكاب الجريمة المعلوماتية	**25**
رابعا: دافع الفقر لارتكاب الجريمة المعلوماتية	**25**
خامسا: الدوافع السياسية لارتكاب الجريمة المعلوماتية	**25**
سادسا: دوافع التهديد لارتكاب الجريمة المعلوماتية	**26**
المبحث الثاني: تصنيف الجرائم المعلوماتية وتحديد مرتكبيها	**27**
المطلب الاول: تصنيف الجريمة المعلوماتية	**27**
الفرع الاول: التصنيف التشريعي للجرائم المعلوماتية	**27**
اولا: تصنيف الجريمة المعلوماتية وفقا لاتفاقية (بودابست) في 2001	**27**
ثانيا: تصنيف الجريمة المعلوماتية وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات	**28**
الفرع الثاني: التصنيف الفقهي للجرائم المعلوماتية	**29**
اولا: تصنيف الجرائم المعلوماتية بحسب ما اذا كان النظام وسيلة او محل	**29**
ثانيا: تصنيف الجرائم المعلوماتية بحسب جرائم الكمبيوتر والانترنت	**34**
المطلب الثاني: مرتكبو الجريمة المعلوماتية	**35**
الفرع الاول: مفهوم المجرم المعلوماتي	**35**
اولا: تعريف المجرم المعلوماتي	**36**
ثانيا: خصائص المجرم المعلوماتي	**37**
الفرع الثاني: تصنيف مرتكبي الجرائم المعلوماتية	**40**
اولا: القراصنة	**40**
ثانيا: صغار مجرمي المعلوماتية	**42**
ثالثا: المجرم الوظيفي	**44**
رابعا: المدافع المتطرف المعلوماتي	**45**

فهرس الموضوعات

خامسا: طائفة مجرمو المعلوماتية اصحاب الآراء المتطرفة	**46**
الفصل الثاني: النماذج الاجرامية المعلوماتية وسبل التصدي للأثار المترتبة عليها	
تمهيد	**50**
المبحث الاول: النماذج الاجرامية المعلوماتية المؤثرة على التطور الاقتصادي	**51**
المطلب الاول: الجرائم الواقعة على المعلومات داخل انظمة المحاكة الالية	**51**
الفرع الاول: جريمة السرقة المعلوماتية	**51**
اولا: تعريف جريمة السرقة المعلوماتية	**52**
ثانيا: اركان جريمة السرقة المعلوماتية	**53**
ثالثا: الجزاءات المقررة لجريمة السرقة المعلوماتية	**58**
الفرع الثاني: جريمة التزوير المعلوماتي	**61**
اولا: تعريف جريمة التزوير المعلوماتي	**61**
ثانيا: اركان جريمة التزوير المعلوماتي	**62**
ثالثا: الجزاءات المقررة لجريمة التزوير المعلوماتي	**65**
المطلب الثاني: الجرائم الواقعة بواسطة النظام المعلوماتي	**70**
الفرع الاول: جريمة الاتلاف المعلوماتي	**70**
اولا: تعريف جريمة التلاف المعلوماتي	**71**
ثانيا: اركان جريمة الاتلاف المعلوماتي	**72**
ثالثا: الجزاءات المقررة لجريمة الاتلاف المعلوماتي	**74**
الفرع الثاني: جريمة النصب (الاحتيال) المعلوماتي	**78**
اولا: تعريف جريمة النصب المعلوماتي	**78**
ثانيا: اركان جريمة النصب المعلوماتي	**79**

فهرس الموضوعات

ثالثا: الجزاءات المقررة لجريمة النصب المعلوماتي	**82**
المبحث الثاني: الاثار الاقتصادية للجرائم المعلوماتية و استراتيجيات مواجهتها	**85**
المطلب الاول: الاثار الاقتصادية للجرائم المعلوماتية	**85**
الفرع الاول: الاثار الناجمة عن الجريمة المعلوماتية و انعكاساتها على الاقتصاد	**85**
اولا: المساس بالاستقرار المالي والاقتصادي	**85**
ثانيا: الخسائر المالية المنجرة على الجريمة المعلوماتية	**85**
ثالثا: احداث العجز في ميزانية المدفوعات	**86**
رابعا: الاضرار بالنشاط المصرفي	**86**
خامسا: انخفاض معدل الاستثمار و الادخار	**87**
سادسا: ارتفاع معدل التضخم	**87**
الفرع الثاني: معوقات الجريمة المعلوماتية الماسة بالاقتصاد	**87**
اولا: عدم وجود اثار مادية للجريمة	**87**
ثانيا: اتسام الجريمة المعلوماتية الماسة بكونها جريمة عابرة للحدود	**88**
ثالثا: المعوقات القضائية	**88**
رابعا: المعوقات المرتبطة بإثبات الجريمة في حد ذاتها	**89**
الفرع الثالث: التكلفة الاقتصادية للجرائم المعلوماتية	**90**
اولا: التكلفة الاقتصادية التي تتكبدها الدول بفعل الجرائم المعلوماتية	**90**
ثانيا: التكلفة الاقتصادية التي تتكبدها الشركات بفعل الجرائم المعلوماتية	**93**
المطلب الثاني: الاتفاقيات الدولية والاقليمية في مكافحة الجرائم المعلوماتية	**95**
الفرع الاول: الاتفاقيات الدولية في مجال مكافحة الجريمة المعلوماتية	**95**
اولا: اتفاقية (برن) لمكافحة الجريمة المعلوماتية	**95**
ثانيا: اتفاقية (تريبس) لمكافحة الجريمة المعلوماتية	**97**

فهرس الموضوعات

ثالثا: معاهدة (الويبو) لمكافحة الجرائم المعلوماتية	**98**
الفرع الثاني: الجهود الاقليمية في مكافحة الجريمة المعلوماتية	**99**
اولا: معاهدة (بودابست) لمكافحة الجرائم المعلوماتية والاتصالات	**99**
ثانيا: القانون العربي النموذجي الاسترشادي لمكافحة الجريمة المعلوماتية	**102**
ثالثا: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات	**103**
الخاتمة	**105**
قائمة المصادر والمراجع	**110**
فهرس الموضوعات	

مـلخص مذكرة الماستر

إن النمو المستمر للثروة المعلوماتية الذي يعيشه عصرنا و يشهده حاضرنا حيث أصبحنا نواجه العديد من الأخطار و المشاكل التي تنشا بشكل تلقائي مع أي تطور حضاري و تقني، فدخول الإنترنت في عالمنا و تمكن الصغير و الكبير و الجاهل و المتعلم من استخدامه، دون أي قيود أو رقابة أدى إلى زيادة هذه الأخطار لا سيما على التطور الاقتصادي.

باعتبار أن الجريمة المعلوماتية تتميز بمجموعة من الخصائص ولعل الخاصية الاساسية فيها بانها جريمة عابرة للحدود و هذا ما يستدل عليه بان العالم أصبح قرية صغيرة، وترتكب الجريمة المعلوماتية بواسطة شخص يسما المجرم المعلوماتي وهذا الشخص له القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الالكتروني الرقمي، حيث يكون لهذا المجرم مجموعة من الدوافع التي تدفعه الى ارتكاب هذه الجريمة.

ولعل اهم نماذج الجريمة المعلوماتية المؤثرة على الاقتصاد حسب تقسيم الجرائم الواقعة داخل انظمة المحاكة الالية كجريمة السرق المعلوماتية و جريمة التزوير المعلوماتي، ومنها الذي يقع بواسطة النظام المعلوماتي كجريمة التلاف المعلوماتي و جريمة النصب المعلوماتي.

ونظرا لتأثير الجريمة المعلوماتية على الاقتصاد نتجه عنها مجموعة من المعوقات والاضرار الاقتصادية التي تكبدتها الدول والمؤسسات الاقتصادية نتيجة الخسائر الفادحة بفعل الاختراقات، مما دفع الدول الى العمل على التصدي ومكافحة هذه الظاهرة الاجرامية من خلال الاتفاقيات الدولية والاقليمية التي عملت على تنظيم هذه الجريمة، وكذلك عملت الشركات على ايجاد برامج من اجل حماية نفسها من أي اختراق تتعرض له.

الكلمات المفتاحية:

1/الجريمة المعلوماتية **2/**المجرم المعلوماتي **3/**تصنيف الجرائم المعلوماتية **4/**نماذج الجرائم المعلوماتية **5/** الاثار الاقتصادية للجريمة المعلوماتية **6/**مكافحة الجريمة المعلوماتية

Abstract of The master thesis

The continuous growth of the information wealth that our age is experiencing and witnessed by our present, where we are facing many dangers and problems that arise automatically with any civil and technical development, the entry of the Internet into our world and enabling the young, the old, the ignorant and the educated to use it, without any restrictions or Control led to an increase in these risks, especially on economic development.

Considering that the information crime is characterized by a set of characteristics, and perhaps the main characteristic of it is that it is a cross-border crime, and this is evidenced by the fact that the world has become a small village, and the information crime is committed by a person called the information criminal and this person has the ability to convert his language into a digital language, store and retrieve it using an electronic computer Digital, where this criminal has a set of motives that push him to commit this crime.

Perhaps the most important models of information crime affecting the economy according to the division of crimes within automated simulation systems, such as the crime of information theft and the crime of information forgery, including those that occur by the information system such as the crime of information damage and the crime of information fraud.

In view of the impact of information crime on the economy, a set of obstacles and economic damages have been incurred by countries and economic institutions as a result of heavy losses due to the breaches, which prompted countries to work to confront and combat this criminal phenomenon through international and regional agreements that worked to regulate this crime, as well as companies To find programs in order to protect itself from any penetration it is exposed to

keywords:

1/ information crime **2/** cyber criminal **3/** Classification of cyber crime **4/** Information crime models **5/** The economic effects of information crime **6/** Fighting cybercrime