جامعة مُحَمَّد خيضر – بسكرة
كلية الحقوق والعلوم السياسية
قسم الحقوق

الجـريمـة المعلـومـاتية و مكـافحتها دوليـا

مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق
تخصص قانون أعمال

إعداد الطالبة:
– ذياب محمد رضا

إشراف الأستاذة:
– معاشي سميرة

الموسم الجامعي: 2016 – 2017

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

مـقدمـــة

مقدمـة

تعتبر القوانين هي مرآة المجتمع ومقياس الحضارة ورقي الدولة، فهي النور الذي يهدي إلى الصواب دون إرهاق وبقدر ما تكون متطورة بقدر ما تحقق الغاية التي وجدت من أجلها.

الجريمة ظاهرة اجتماعية توجد بوجود الإنسان والمجتمع، وتتطور بتطورهما، ولا شك أن المجرمين يحاولون الاستفادة من التقدم التقني وأننا في عصر ثورة المعلومات والتكنولوجيا المتطورة، حيث أنه دخل في قاموس الجرائم نوعا جديدا تطلق عليه الدول (الجريمة المعلوماتية) أصبحت مصطلحا شائعا في الفترة الأخيرة خاصة مع انتشارها وتعدد أشكالها، وإذا كانت مجتمعاتنا العربية لم تتأثر بشكل ملموس بمخاطر هذا النمط المستجد من الإجرام، فإن خطر جرائم الحاسب الآلي الانترنت، المحتمل في البيئة العربية والعالمية، يمكن أن يكون كبيرا باعتبار أن الجاهزية التقنية والتشريعية والأدائية (إستراتيجية حماية المعلومات) لمواجهتها ليست بالمستوى المطلوب، إن لم تكن غائبة تماما، وبالمقابل فقد أمست جرائم الحاسب الآلي والانترنت من أخطر الجرائم التي تقترف في الدول المتقدمة، تحديدا الأمريكية والأوروبية، ولهذا تزايدت خطط مكافحة هذه الجرائم وانصبت الجهود على دراساتها المتعمقة وخلق آليات قانونية للحماية من أخطارها، وبرز في هذا المجال المنظمات الدولية والإقليمية، خاصة المنظمات والهيئات الإقليمية الأوروبي، وإدراكا لقصور القوانين الجنائية بما تتضمنه نصوص التجريم التقليدية، كان لا بد للعديد من الدول وضع القوانين والتشريعات الخاصة، أو العمل على جبهة قوانينها الداخلية لجهة تعديلها من أجل ضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم.

ومازال جميع أساتذة القانون على مستوى العالم عاجزين عن إصدار تشريع يحظر هذا النوع من هذا الجرائم، خاصة وأن أدلة إثبات الجريمة يصعب التوصل إليها، أو الواقع أن الجريمة المعلوماتية تضم أشكالا متعددة، ومتنوعة يصعب حصرها، وهي تزداد كلام توغل العالم في استعمال الحاسب الآلي والانترنت.

أهمية الموضوع:

الجريمة المعلوماتية فهي تدعونا إلى البحث عن كل صغيرة وكبيرة عن عالم الحاسب الآلي والانترنت، وهذا ما يجعل البحث عن كل صغيرة وكبيرة عن عالم الحاسب الآلي والانترنت، وهذا ما يجعل البحث أكثر تشويقا، لأنه موضوع شاسع، وانتشرت الجرائم حول العالم مما أوجبنا التعرض للتحديات التي أخذ بها المجتمع الدولي.

الأهداف:

واخترنا هذا الموضوع لأجل التعرف على:

- التعرف على الجريمة العلوماتية
- النظر في تقسيمات الجريمة المعلوماتية
- التعرف ما إذا كان المجتمع الدولي قد سيطر على هذه الظاهرة ، وماهي السبل لتخطي الصعوبات التي قد تواجهه.

الإشكالية: كيف ساهم المجتمع الدولي في مكافحة الجرائم المعلوماتية؟

نتبع في الدراسة المنهج الوصفي التحليلي، و هذا لطبيعتها التي تستوجب أن نقوم بطرح الأفكار المتواجدة على مستوى القوانين و الإتفاقيات و تحليلها ، و يستوجب هذا أولا لوصف الجريمة، لأجل التوصل للإجابة حول الاشكالية و لهذا قسمنا الموضوع على النحو الأتي:

الفصل الأول: ماهية الجريمة المعلوماتية

المبحث الأول : المفاهيم المتعلقة بالجريمة المعلوماتية

المطلب الأول: مفهوم الجريمة المعلوماتية

الفرع الأول: تعريف الجريمة المعلوماتية

الفرع الثاني: خصائص الجريمة المعلوماتية

المطلب الثاني: مميزات الجريمة المعلوماتية

الفرع الأول: الطبيعة القانونية للجريمة المعلوماتية

الفرع الثاني: أشخاص الجريمة المعلوماتية

المبحث الثاني: تصنيف الجرائم المعلوماتية

المطلب الأول: تصنيف جرائم الحاسب الآلي

الفرع الأول: جريمة النصب والاحتيال المعلوماتي

الفرع الثاني: اختراق جهاز الحاسب الآلي واتلاف المعلومات

الفرع الثالث: تخريب البرامج المعلوماتية بالفيروسات

المطلب الثاني: جرائم الأنترنت

الفرع الأول: المواقع المخلة بالآداب العامة و الهجوم على المواقع

الفرع الثاني: الجرائم المنظمة والإرهاب الإلكتروني

الفرع الثالث: جرائم القرصنة والتجسس

المطلب الثالث: كيفية ضبط جرائم الحاسب الآلي والأنترنت

الفصل الثاني:مواقف التشريعات و الجهود الدولية لمكافحة الجريمة المعلوماتية

الـفـصـــل
الأول

الفصل الأول: ماهية الجريمة المعلوماتية

تعتبر الجريمة المعلوماتية حديثة نسبيا قياسا بغيرها من الجرائم التقليدية في العالم بشكل اجمع و في العالم العربي على وجه خصوص و ربما يرجع السبب في ذلك إلى أن اغلب الدول العربية حديثة العهد بتقنيات الحاسب الآلي كما أن الكثير من الدول لم تدشن خدمة الانترنت لمواطنيها إلا منذ سنوات قليلة فقط ولكن مع تزايد استخدام الحاسب الآلي في السبعينات بدء اعتبار تلك السلوكات ظاهرة إجرامية وليست مجرد سلوكات غير أخلاقية .

في فترة الثمانينات ظهر مفهوم جديد للجريمة المعلوماتية ارتبط أساسا بعمليات اقتحام نظم الحاسب عن بعد كأنشطة نشر و زرع الفيروسات المعلوماتية التي تقوم بتدمير البرامج و الملفات بواسطة مقتحمي النظم hackers" لكن دوافع ارتكاب تلك السلوكيات بداية محصورة في رغبة المحترفين في تجاوز إجراءات امن المعلومات و إظهار تفوقهم التقني لذا انحصر مرتكبوا تلك الجرائم في الأولاد القصر النوابغ الراغبين في التحدي و المغامرة لكن فيما بعد أصبحوا مجرمين حقيقيين مما أدى إلى إعادة النظر في سمات مرتكبي الجريمة المعلوماتية بعد ظهور ما يسمى بالمجرم الالكتروني الذي تدفعه نوايا إجرامية خطيرة تستهدف الاستيلاء على أموال الغير و التجسس قصد الاستيلاء على المعطيات السرية ، ثم شهد حقل الجرائم المعلوماتية تطورا هائلا في التسعينات بعد أن تغير و مفهومها بفعل ما أحدثته شبكة الإنترنت من تسهيل عملية الدخول إلى الأنظمة و اقتحام شبكات المعطيات مما أدى إلى ظهور أشكال جديدة للإجرام كأنشطة إنكار الخدمة التي تقوم بتعطيل نظام تقني و منعه من القيام بعمله المعتاد و كثيرا ما مورست مثل هذه الأنشطة على مواقع الإنترنت المتخصصة بتسويق منتجات معينة هامة و التي يؤدي انقطاعها عن الخدمة بساعات معينة إلى خسائر مالية تقدر بالملايين الدولارات .

أما في التسعينات شهدت الجرائم المعلوماتية تطورا هائلا بفعل ما أحدثته شبكة الانترنت من تسهيل لعمليات الدخول إلى الأنظمة ، و نشطت قوة جرائم زرع و نشر الفيروسات عبر مواقع الانترنت التي تسهل من انتقالها إلى ملايين المستخدمين في نفس الوقت و ظهرت أيضا أنشطة الرسائل المعلوماتية الماسة بكرامة و اعتبار الأشخاص و للوقوف على أبعاد

هذه الظاهرة بشكل كامل فانه ينبغي تناولها من حيث تعريفها و دوافعها و خصائص ارتكابها و تصنيفها من خلال الفصل الأول.

المبحث الأول : المفاهيم المتعلقة بالجريمة المعلوماتية

مست المعلوماتية مختلف المجالات حتى المجال الإجرامي وبالتالي أصبح لدينا جريمة مستحدثة وجديدة في علم الإجرام، لاقت الكثير من التعاريف من قبل الفقهاء كل حسب نظرته... وكذلك تميزتبمجموعة من الخصائص جعلتها تختلف عن نظيرتها الجريمة التقليدية وهذا ما سنتناوله في المطلب الأول، كما انعكس الجانب الخصوصي للجريمة المعلوماتية على طبيعتها القانونية ومن ثم وضع لها نظاما قانوني معين...، وكذلك على جانبها الشخصي أي أطراف الجريمة المعلوماتية ويقصد بذلك المجرم المعلوماتي وهذا ما سنتناوله في المطلب الثاني.

المطلب الأول: مفهوم الجريمة المعلوماتية

كانت ولا تزال الجريمة المعلوماتية موضع اهتمام الفقهاء من أجل وضع تعريف لها، لكن نظرا لطبيعتها وحداثتها وتطورها فقد تم تحديد تعاريف متعددة لها حسب اتجاهات معينة مبنية على أساس متبناة من قبل فقهاء كل اتجاه وهذا ما سنعرج عليه في (الفرع الأول)، ومن جهة أخرى تتمتع الجريمة المعلوماتية، بمجموعة من الخصائص قد تكون مشتركة مع الجريمة التقليدية أو منفردة وهذا ما سنعرج عليه في(الفرع الثاني).

الفرع الأول: تعريف الجريمة المعلوماتية

لقد استقطبت الجريمة المعلوماتية فقهاء علم الاجرام لوضع تعريف لها ، فانقسموا نتيجة لذلك الى اتجاهين يضيق من تعريفها وهو ما سنتطرق اليه (أولا) واتجاه يوسع من تعريفها وهو ما سنتطرق اليه (ثانيا).

أولا: التعريف الضيق للجريمة المعلوماتية

لقد تعددت تعاريف الضيقة للجريمة المعلوماتية، حسب اعتماد معيار معين في كل مرة، فعرفت على أنها:

" كل نشاط غير مشروع موجه لنسخ أو الوصول الى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها".[1]

نلاحظ من خلال هذا التعريف أنه اعتمد على معيار واحد وهو المعيار الموضوع للجريمة المعلوماتية والمتمثل في المعلومات والمساس بها.

وأيضا "كل أشكال السلوك غير المشروع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب"[2]

أو هي "الجرائم التي فيها الحاسب يلعب دورا نشيطا بدلا من دور سلبي".[3]

من خلال التعريفين السابقين للجريمة المعلوماتية نجد أنه تم الاعتماد على معيار واحد أيضا وهو معيار وسيلة أو الأداة التي ترتكب بها الجريمة المعلوماتية.

وكذلك هي " كل فعل غير مشروع يكون العلم بتكنولوجيات الحاسبات الآلية بقدر كبير لازم لارتكابه"[4] أو هي"ذلك النوع من الجرائم التي تتطلب إلماما خاصا بتقنيات الحاسب الألي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها".[5]

بالنسبة لهاذين التعريفين فقد اعتمد على المعيار الشخصي وهو الدراية التقنية للجاني لارتكاب مثل هذا الفعل المجرم.

---

[1] محمود أحمد عبابنة، **جرائم الحاسوب وأبعادها الدولية**، الأردن: دار الثقافة، 2005، ص 17.

[2] مشتاق طالب وهيب، **مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها**، مجلة العلوم القانونية والسياسية، جامعة ديالي، المجلد الثالث، العدد الأول، 2014، ص 338.

[3] عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت**، مصر: دار الكتب الوطنية، 2005، ص 5.

[4] قورة نائلة، **جرائم الحاسب الاقتصادية**، القاهرة: دار النهضة العربية، 2004، ص 24.

[5] محمد بن عبد الله بن علي المنشاوي، **جرائم الإنترنت في المجتمع السعودي**، أطروحة مقدمة لنيل شهادة الماجستير، قسم العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص 10.

من خلال التعاريف السابقة المعتمدة من قبل أنصار الاتجاه الضيق لتعريف الجريمة المعلوماتية نجدهم قد اعتمدوا على عدة معايير في تعاريفهم، لكن كل تعريف يستند لمعيار واحد أما المعيار الموضوعي أو معيار الوسيلة أو المعيار الشخصي وهذا بحسبنا منتقد لأنه لا يعطي لذلك تعريف جامع ولو نسبيا...، فإهمال عنصر من العناصر المكونة للجريمة المعلوماتية في التعريف يؤدي ذلك إلى نقصانه وانتقاده، هذا ما يجعلنا نتناول الاتجاه الأخر الذي عرف الجريمة المعلوماتية تعريفا واسعا.

ثانيا: التعريف الواسع للجريمة المعلوماتية

عرفت الجريمة المعلوماتية من قبل أنصار هذا الاتجاه على أنها:"جرائم المعلوماتية تعني جرائم الشبكة العالمية التي يستخدم الحاسب وشبكاته العالمية كوسيلة مساعدة لارتكاب الجريمة مثل استخدامه في النصب وغسل الأموال وتشوبه السمعة والسب".[1]

كما جاء في مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي عقد في فيينا عام 2000 على أنها: "أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، وهذه الجريمة تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية".[2]

وعرفها أصحاب هذا الاتجاه أيضا: "كل جريمة تتم في محيط أجهزة الكومبيوتر".[3]

من خلال طرح أنصار اتجاه موسع لتعريف الجريمة المعلوماتية نجدهم أدمجوا مختلف المعايير التي اعتمدها أنصار الاتجاه الضيف في تعاريفهم ولو بشكل غير مباشر محاولين تجاوز انتقادات الطرح السابق، كما يمكن القول أن تعاريفهم أشمل من التعاريف السابقة حيث حاولوا حصر كل الأفعال الإجرامية التي تقع في وسط الكتروني أي معلوماتي... الخ.

---

[1] إقلولي أولد رابح صافية، **الطبيعة القانونية للجريمة المعلوماتية**، أعمال الملتقى الوطني حول "الجريمة المعلوماتية بين الوقاية والمكافحة"، يومي 16 و17 نوفمبر 2015، جامعة بسكرة، ص ص 03، 04.

[2] ناصر بن محمد البقمي، **مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية**، الطبعة الأولى، الإمارات العربية: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2008،ص.6.

[3] معاشي سميرة، **ماهية الجريمة المعلوماتية**، مجلة المنتدى القانوني، جامعة بسكرة، العدد السابع، ص 276.

كما يمكن إيراد تعاريف للجريمة المعلوماتية ونذكر منها:

تعريف محمد سامي الشواهي:"كل فعل وامتناع عمدي ينشأ من الاستخدام الغير مشروع لتقنية معلوماته بها يهدف الى الاعتداء على الأموال المادية أو المعنوية".[1]

وعرفها محمد علي عريان بأنها: "كل فعل ايجابي أو سلبي عمدي يهدف الى الاعتداء على التقنية المعلوماتية أي كان غرض الجاني".[2]

وعرفها أيضا هلالي عبد الإله على أنها " كل عمل أو امتناع يأتيه الإنسان اضرارا بمكونات الحاسب وشبكاته الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقابا".[3]

من خلال ما تقدم يمكن اقتراح تعريف للجريمة المعلوماتية على أنها: " كل فعل مجرم قانونا له علاقة بالتقنية المعلوماتية في وسط معلوماتي يمس مصالح محمية جنائيا يلحق أضرار بالضحية".

عرف المشرع الجزائري الجريمة المعلوماتية في المادة 2 من القانون رقم 09-04 على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات المعلوماتية" من خلال هذا التعريف نجد أن المشرع الجزائري تبنى الاتجاه الموسع في تعريفه للجريمة المعلوماتيةإذ حاول الالمام وحصر كل السلوكات المجرمة المعلوماتية من خلال الاحاطة قدر الامكان بجميع الجرائم التي يمكن أن تقع في البيئة المعلوماتية.[4]

بعد تقديم مختلف التعريفات التي قدمت للجريمة المعلوماتية ننتقل لمميزاتها التي جعلتها تتسم بطابع خصوصي في ميدان وعلم الإجرام، مادة 2 من قانون 09 – 04 بتعريف المشرع الجزائري منقوص موقف.

---

[1] محمد سامي الشوا، **ثورة المعلومات وانعكاساتها على قانون العقوبات**، القاهرة: دار النهضة العربية، 1994، ص 7.

[2] محمد علي عريان، **الجرائم المعلوماتية**، الإسكندرية: دار الجامعة الجديدة، 2004، ص 45.

[3] هلالي عبد اللاه أحمد، **تفتيش نظم الحاسب الآلي وضمانات المجرم المعلوماتي**: دار النهضة العربية، القاهرة ، 1997، ص 1060.

[4] القانون رقم 09 – 04 المؤرخ في 5 ماي 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، جريدة رسميه، عدد47 لسنة 2009.

الفرع الثاني: خصائص الجريمة المعلوماتية

تتمتع الجريمة المعلوماتية بمجموعة من الخصائص خاصة أنها مستحدثة و تقاوم التعريف نتيجة لتطورها المستمر و ظهور أشكال أخرى للجريمة المعلوماتية، وتتمثل هذه الخصائص في:

أولا: البعد الدولي للجريمة المعلوماتية:

حيث تلغى الحدود الجغرافية المكانية والدخول في عالم افتراضي بلا حدود...، اذ يمكن ارتكاب فعل اجرامي معلوماتي والنتيجة في بلد آخر.

ثانيا: خطورة الجريمة المعلوماتية:

وذلك بالنظر للمصالح المحمية جنائيا التي تمسها نت أمن انساني وقومي للدول، وما تتكبده من خسائر كبيرة.[1]

ثالثا: قلة التكلفة وخصوصية الهدف:

ارتكاب الجريمة المعلوماتية لا يحتاج الى تكاليف باهظة، فالجاني يمكن أن يرتكبها دون أن يغادر بيته وينتقل الى مكان آخر، كما أن الجريمة المعلوماتية تدمر في صمت، فهي متميزة الهدف والضحايا، فالمستهدف هو المعلومة والتي تتعرض للتزوير والقرصنة والتغيير والحذف والعرقلة... الخ وما يتسبب ذلك في أضرار للغير الذي يمتلك هذه المعلومة ويعتمد عليها في المجال السياسي والعسكري والتجاري... الخ.[2]

رابعا: صعبة الاكتشاف والإثبات:

أن عدد ارتكاب الجريمة المعلوماتية كثير لكن حالات الاكتشاف قليل إذا ما قورنت بالجرائم التقليدية وذلك راجع للوسط الافتراضي المعلوماتي المعقد الذي ترتكب فيه،بالإضافة الى أحجام الضحايا عن التبليغ...، كما يتم تدمير المعلومات التي تعتبر كدليل في الإثبات وذلك في مدة وجيزة، والأدلة في هذا النوع من الجرائم غالبا نادرة وغير مادية وإنما معنوية.

---

[1] حمشاشي أمينة، **ماهية الجريمة المعلوماتية**، مجلة الدراسات والأبحاث، العدد الأول، 2009، ص 7.

[2] محمد التدلاوي، **الجريمة المعلوماتية في القانون المغربي والمقارن**، مجلة الملف، العدد الثامن، 2006، ص 226.

خامسا:أسلوب ارتكاب الجريمة المعلوماتية:

ترتكب بشكل هادئ وناعم وسريع وعن بعد، إذ لا تتطلب سوى عدد من اللمسات الخاطفة على لوحة المفاتيح.[1]

سادسا: تتم عادة بتعاون أكثر من شخص:

حيث يكون هناك شخص يقوم بالجانب الفني للمشروع الإجرامي، وشخص آخر يغطي عملية التلاعب وتحول المكاسب اليه، وبالنسبة للاشتراك قد يكون سلبي أو ايجابي يتمثل الأول في الصمت عن الجريمة لاتهامها والثاني يتمثل في المساعدة الفنية والمادية.[2]

من خلال ما سبق رأينا أن الجريمة المعلوماتية تتمتع بجملة من الخصائص حاولنا حصرها كلها وأهمها، وهذه الخصائص نطبعها بطابع ينفرد عن الجريمة التقليدية وبالتالي فهي نوع جديد ومستحدث من الإجرام، وجب تحديد طبيعته القانونية وأشخاصه المتميزين وهذا ما سنوضحه في المطلب الموالي.

المطلب الثاني: مميزات الجريمة المعلوماتية

تميزت الجريمة المعلوماتية بسمات متعددة ومختلفة انعكس ذلك على كل ما يدور في فلكها المفاهيمي نذكر في ما يخص تحديد طبيعتها القانونية والتي ستكون محل دراسة (الفرع الأول) وكذلك أطراف الجريمة المعلوماتية من المجرم المعلوماتي وضحية معلوماتي الذين سيكونان محل دراسة (الفرع الثاني).

الفرع الأول: الطبيعة القانونية للجريمة المعلوماتية

إن التطرق للطبيعة القانونية للجريمة المعلوماتية يكون من خلال الإجابة على تساؤلأولي مفاده ما هو الوضع القانوني للمعلومة؟ وبالتالي تحديد النظام القانوني التجريمي للجريمة المعلوماتية هل هو تابع أم مستقل؟

ولقد انقسم الفقه بشأن ذلك الى اتجاهين وهما:

---

[1] رشيدة بوبكر، **جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن**، الطبعة الأولى، بيروت: منشورات الحلبي الحقوقية، 2012، ص 98.

[2] نهلا عبد القادر المومني، **الجرائم المعلوماتية**، عمان: دار الثقافة، 2008، ص 58.

أولا: الاتجاه الأول: المعلومات لها طابع خاص

يستند هذا الاتجاه التقليدي إلى فكرة أن القيم هي الأشياء المادية القابلة إلىالاستحواذ ووضع اليد غير ذلك لا يجوز، فالمعلومات لها طبيعة معنوية لا تكون محلا للاستئثارإلا عن طريق حق الملكية الفكرية سواءا الأدبية أو الذهنية أو الصناعية التي تكون خارج هذه المجموعة فهي خارج نطاق الحماية لذا حاول هذا الاتجاه أن يسوغ العقاب على أساس المنافسة غير المشروعة بقوله "إن الخطأ لا يجد أساسه في الاستيلاء نفسه على المعلومة التي تخص الآخرين، وإنما يجد أساسه في الظروف التي اقترنت بهذا الاستيلاء وبحيث يمكن تفادي الاعتراف بحق الاستئثار بالمعلومات.[1]واستبعاد الكيان المادي للمعلومة لا يجعلها محلا لحق مالي، لذا يلزم اخراجها من طائفة الأموال.[2]

ثانيا: الاتجاه الثاني: المعلومات مجموعة مستحدثة من القيم

يستند هذا الاتجاه الحديث إلىأن المعلومات عبارة عن مجموعة مستحدثة من قيم ويرجع الفصل في ذلك الى الأستاذين "بيير كاتالا" و"ميشيل فيفانت" حيث يذهب الأول للقول أن "المعلومة تقوم وفقا لسعر السوق متى كانت عبر محظورة تجاريا، وأنها منتج دون النظر إلى دعامتها المادية وعمل من قدمها، وأنها ترتبط بمؤلفها عن طريق رابطة قانونية تمثل بعلاقة المالك بالشيء الذي يملكه وهي تخص مؤلفها بسبب علاقة التبني التي تجمع بينهما"، "وبالتالي هناك حجتين لوصف القيمة على المعلومة إحداهما اقتصادية والأخرى علاقة التبني".[3]

ويرى الأستاذ " كاتالا" أن المعلومات بوصفها ملكية محددة وتخول لصاحبها ميزتين أساسيتين، تمثل الأولى حقه في ضمان سرية المعلومة والثانية في طلب التعويض عن الأضرارالتي تترتب عن أي عمل أي مشروع يتعلق بها.[4]

---

[1] محمد سامي الشوا، المرجع السابق، ص ص 178، 179.

[2] ناصر محمد البقمي، المرجع السابق، ص 17.

[3] محمد سامي الشوا، المرجع السابق، ص 183.

[4] نائلة قورة، المرجع السابق، ص 120.

ويتفق الأستاذ "فيفانت" مع الرأي السابق، وعلى ذلك يمكن أن تعد المعلومات مالا قابلا للتملك أو الاستغلال على أساسا قيمته الاقتصادية وليس على أساس كيانه المادي ولذلك فهو يستحق الحماية القانونية، ولأن البرامج في جوهرها معلومات معالجة آليا ولها قيمة اقتصادية لذا تجب معاملاتها معاملة المال.[1]

من خلال ما سبق نستنتج أن المعلومات لها قيمة ذاتية ومستقلة بحد ذاتها وبالتالي يمكن اعتبارها مصلحة محمية جزائيا من خلال قانون العقوبات والقوانين المكملة له، وبالتالي فان النظام القانوني للجريمة المعلوماتية يجب أن يكون مستقل، حتى وان كانت جرائم تقليدية ترتكب بواسطة التقنية المعلوماتية...

وبعد الحديث عن الطبيعة القانونية للجريمة المعلوماتية وتكملة لمميزاتها ننتقل للحديث عن أشخاص الجريمة المعلوماتية في الفرع الموالي.

الفرع الثاني: أشخاص الجريمة المعلوماتية

ونقصد بهم كل من المجرم المعلوماتي والذي سنعرج عليه (أولا) من خلال تبيان سماته وطوائفه و دوافعه لارتكاب مثل هذا النوع من الإجرام، والضحية المعلوماتي والذي هو سنعرج عليه (ثانيا) من خلال توضيح طبيعته وميدان عمله وكيفية تصرفه في مواجهة الجريمة المعلوماتية... الخ.

أولا: المجرم المعلوماتي

انعكست خصائص الجريمة المعلوماتية على المجرم المعلوماتي والذي هو الآخر يتميز بسمات ينفرد بها عن المجرم التقليدي وينقسم لعدة طوائف وفئات حسب الدافع والغاية من الجريمة.

[1] محمد علي العريان، المرجع السابق، ص 51.

1- سمات المجرم المعلوماتي:

وتتجلى فيما يلي:

قد يكون المجرم المعلوماتي من ذوي المناصب الرفيعة المستوى ومن ذوي الكفاءات العالية وله القدرة على التكيف الاجتماعي.[1]

- المجرم المعلوماتي ملم بالمعارف التقنية والوسائل المعلوماتية واجرامه اجرام الأذكياء لا يميل للعنف.

- المجرم المعلوماتي يشعر دائما بالخوف من كشف جرائمه بذلك قد يفقد مركزه الوظيفي...، كما يتميز بقوة الصبر فتجسيد الجريمة المعلوماتية واخراجها للواقع قد يتطلب وقته لتنفيذه.[2]

- المجرم المعلوماتي يبرر ارتكابه للجريمة، فهو يحس أن ما يقوم به لا يدخل في نطاق الجريمة، خاصة إذا كان لدافع هو تبيان التفوق على الحاسوب وتخطي الحماية...، كما أنه غالبا من الذين يتمتعون بالسلطة اتجاه معلوماته محل الجريمة وقد تتمثل في الرقم السري الخاص للولوج الى النظام، وقد تتمثل في حق استعمال الأنظمة المعلوماتية أو إجراء بعض التعاملات أو مجرد الدخول إلى الأماكن التي تحتوي الأنظمة...[3]

ويمكن اجمال عدد من القواسم المشتركة بين هؤلاء المجرمين نذكر منها:[4]

-أن سنهم وأعمارهم تكون محددة بين 18 و45 سنة.

- المهارة والإلهام الكامل والقدرة الفنية والتقنية في مجال المعلوماتية.

- انتمائهم إلى طبقة المثقفين والمتعلمين.

- الثقة بالنفس.

- عدم ادراكهم أن سلوكاتهم تستوجب العقاب.

---

[1] أحمد أمين الرومي، **جرائم الكمبيوتر والإنترنت**، الإسكندرية: دار المطبوعات الجامعية، 2003، ص 47.

[2] ربيعي حسين، **آليات البحث والتحقيق في الجرائم المعلوماتية**، أطروحة مقدمة لنيل شهادة الدكتوراه، قسم الحقوق، جامعة الحاج لخضر، باتنة، 2016، ص 32.

[3] قورة نائلة، المرجع نفسه، ص 54.

[4] ربيعي حسين، المرجع نفسه، ص 38.

هذه السمات جديرة بالذكر فهي حقا تجعل المجرم المعلوماتي له طابع خصوصي يختلف عن بقية المجرمين العاديين فهو عادة مجرم مختص ومحترف وعائد للإجرام.

2- فئات وطوائف المجرم المعلوماتي:

من بين أفضل التصنيفات التي قدمت لمجرمي التقنية الذي أورده كل من: William Vonstarchو David Covrو KarlSegerفي مؤلفهم "جرائم الكمبيوتر" الصادر عام 1995 حيث تم تقسيم مجرمي التقنية إلى ثلاث طوائف هي المحترفون والحادقون، كما أن من التصنيفات الهامة التمييز بين صغار السن من مجرمي الكومبيوتر وبين البالغين الذين يتجهون للعمل معا من أجل تكوين منظمات إجرامية خطيرة.[1]

وهناك تصنيف آخر من بين التصنيفات التي أعطيت المجرم المعلوماتي وهو ينقسم لـ 7 طوائف كالتالي:[2]

- **الطائفة الأولى:** وهم الأشخاص الذين يرتكبون جرائم المعلوماتية دون قصد احداث ضرر للغير، ويقصد بهم صغار مجرمي المعلوماتية المفتونين بها .
- **الطائفة الثانية:** تظم أشخاص هدفهم كسر الحواجز الأمنية لأنظمة الحاسب الآلي غير المصرح لهم الدخول اليه.
- **الطائفة الثالثة:** يندرج تحتها صانعي الفيروسات والذين يكون هدفهم إلحاق ضرر بالمجني عليه دون الحصول على مكاسب مادية.
- **الطائفة الرابعة:** تختص هذه الطائفة بفك الشفرات فقد دون تخريب الشبكة، هدفها تحقيق ربح مادي.
- **الطائفة الخامسة:** تعمل ضمن عصابات منظمة هدفها تحقيق مكاسب مادية.
- **الطائفة السادسة:** توظف معارفهم وخبرتهم في مجال المعلوماتية لنشر أذكارهم وتوجهاتهم السياسية والإيديولوجية...

[1] حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، رسالة الماجستير، قسم الحقوق، جامعة الحاج لخضر، باتنة، 2012، ص 35.

[2] مشتاق طالب وهيب، المرجع السابق، ص ص 353، 354.

– **الطائفة السابعة:** تظم فئة من الأشخاص يعملون لصالح مؤسسات وحكومات لاقتحام برامج ونظم حاسوبية معينة تديرها مقابل مبالغ من النقود.

من خلال ما تقدم نلاحظ أن التقسيمات التي أعطيت للمجرم المعلوماتي أسست وبنيت على دوافع ارتكاب الجريمة المعلوماتية كما أنه لا يعني انتماء مجرم معلوماتي لطائفة معينة يمنعه إلىالانتماء لطوائف أخرى... الخ.

3– دوافع ارتكاب الجريمة المعلوماتية:

تنوعت وتعددت نذكر منها:

– السعي لتحقيق الربح حيث يأتي في المرتبة الأولى من سلم دوافع ارتكاب الجريمة المعلوماتية، ففي دراسة أشار اليها "باركر" نجد أن نسبة 43%من حالات الغش المعلن عنها قد بوشرت من أجل الحصول على المال.[1]

–إثبات الذات وكذلك التهديد والانتقام.

–الدوافع السياسة: أصبح مجال المعلوماتية فضاء لنشر مختلف الأفكار أي المعتقدات السياسية، وأخبار ماسة بنظام الحكم وأمن الدولة.

– الدوافع الإرهابية: مثل انشاء مواقع ارهابية على شبكة الأنترنيت من قبل الإرهابين لممارسة أعمالهم الإجرامية كالتحريض على قتل و نشر الأفكار الإرهابية ... الخ.[2]

ولا تزال دوافع أخرى نذكر منها التنافس المعلوماتي بين مختلف الدول في مجالات متعددة. هذا فيما يخص أحد أطراف الجريمة المعلوماتية وهو المجرم المعلوماتي الذي يكون ضحيته من نوع خاص ومميز وهذا ما سنتعرض اليه الآن.

ثانيا: الضحية المعلوماتي

إن المجني عليه في مجال الإجرام المعلوماتي هو ضحية الاعتداء غير المشروع الذي يقع في البيئة المعلوماتية وقد يكون شخصا طبيعيا أو معنويا.

فالجريمة المعلوماتية تستهدف مجال المال والأعمال والسلطة وسيادة الدول، أي تلك الجريمة إما أن تسلط على مصالح المؤسسات المالية والبنوك مما ينتج عنه استيلاء غير شرعي

---

[1] محمود أحمد عبابنة، المرجع السابق، ص 24.

[2] محمد أمين الشوابكة، **جرائم الحاسوب والإنترنت**، عمان: مكتبة دار الثقافة، 2007، ص 29.

على أموال طائلة، أو أن تجعل الجاني ينفذ إلى المنظومات المعلوماتية للسلط الأمنية والإدارية وبالتالي يكتشف أسرار ليست من مصلحة الدول أن تكون في متداول العموم، وأمام تلك التصرفات يختلف رد فعل المعتدى عليهم فمنهم من يتخذ موقفا سلبيا ويخير عدم الكشف ما تعرض له تفاديا للتأثيرات السلبية منها المساس بسمعتهم في المجال الذي ينشطون فيه، وأن هذا الموقف يؤكد ما يعبر عنه "بقانون الصمت" الذي يتسم به ميدان نشاط هذه الجريمة، ومنهم من يختار طريق المواجهة واتخاذ الإجراءات القانونية اتجاه مقترفي تلك الجرائم.[1]

– كما أنه يصعب تحديد الضحايا المعلوماتيين، لأن هؤلاء لا يعلمون أي شيء عن الجريمة المعلوماتية إلا بعد وقوعها، وبالتالي لا يحبذ أكثرهم الإفصاح بأن نظامه المعلوماتي تعرض للاعتداء، لما قد يشكل هذا الاعتراف من دافع للمجرمين في الاستمرار في اعتدائهم.[2]

فكما أشرنا سابقا أن إحجام المجني عليه في مجال الإجرام المعلوماتي راجع لتجنب التأثيرات السلبية، فالمعلومات المستقاة من قبل القراصنة المعلوماتيين يمكن بيعها في السوق السوداء، حيث يختلف سعر بطاقات الائتمان بين إذا ما كان رقمها بدون رمز سري أو معه.[3]

كما أن الضحية يخاف من المسألة القانونية، إذا كان يقع عليه واجب الإشراف على المعلومات المستهدفة.[4]

الضحية المعلوماتي طرف ضعيف في حلقة الإجرام المعلوماتي إذ حجم خسائره كبير جدا له خصائص ومميزات تحدده من خلال طبيعته وميدان عمله وكيفية تصرفه اتجاه هذا أم الجديد، حيث غالبا ما يمتنع عن الإبلاغ بشأن تعرضه لجريمة معلوماتية وذلك راجع لعدة أسباب.

---

[1] الهاشمي الكسراوي، **الجريمة المعلوماتية**، مجلة القضاء والتشريع، مركز الدراسات القانونية والقضائية، تونس، العدد السابع، 2006، ص ص 29، 30.

[2] خالد عياد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت**، الطبعة الأولى، الأردن: دار الثقافة، 2011، ص 37.

[3] Myriam Quéméner, Yves Charpenel, **La Cybercriminalité**, édition economica, françe, 2010, P 13.

[4] محمد علي سالم وحسون عبيد هجيج، **الجريمة المعلوماتية**، مجلة العلوم الإنسانية،جامعة بابل، المجلد الرابع عشر، العدد الثاني، 2007، ص 90.

وخلاصة القول هو أنه من خلال هذا المبحث تم التطرق إلى مختلف ما يدور في الفلك المفاهيمي للجريمة المعلوماتية، مما يثير لنا دائما الفضول للتطرق إلى صور وأنواع هذه الجريمة والتي ستكون محل دراسة المبحث الموالي.

المبحث الثاني: تصنيف الجرائم المعلوماتية:

وهنا اختلاف في التصنيفات لهذا نتبنى أحدها وهي جرائم الحاسب الالي وجرائم الانترنيت، ندرسها على النحو التالي:

المطلب الأول: تصنيف جرائم الحاسب الآلي

كما أننا نجد ما يندرج تحتها من جرائم ينقسم إلى ثلاث نتطرق لها:

الفرع الأول: جريمة النصب والاحتيال المعلوماتي

أولا: جريمة السرقة المعلوماتية

"يوجد تعريف للسرقة المعلوماتية، لهذا يستند للسرقة لمفهومها الواسع بأنها الحصول على شيء من طرف آخر دون علمه وفي الغالب يترتب عليه أضرار بهذا الطرف سواءا أكان ضررا ماديا أو معنويا".[1]

وعرفها المشرع الجزائري في المادة 350 من قانون العقوبات: "كل من اختلس شيء غير مملوك له يعد سارقا".

* وبظهور التقنيات الحديثة عرف العالم السرقة عبرالإنترنت.

هناك العديد من صور السرقة التي تقع على جهاز الحاسب الالي ومن تلك الاعتداءات ما يلي:

1. **سرقة المعلومات و البرامج المخزنة آليا**

هناك العديد من الجرائم التي تقع على المعطيات المخزنة آليا بالنظر إلى المصلحة المحمية قانونا ومن تلك الجرائم ما يعد اعتداء على الحقوق المكية الفكرية عن طريق نسخ البرامج

[1] عبد الله حسين علي محمود،**سرقة المعلومات في الحاسب الالي** ، دار النهضة العربية ،القاهرة، 2001،ص ص 62،63،64

الأصلية وتسويقها واستخدامها مما يعرض الشركات المنتجة لهذه البرامج في الكثير من الخسائر الفادحة.[1]

2. سرقة خدمات الحاسب الآلي

وهو ما يعرف باصطلاح سرقة منفعة الحاسب الآلي أو الاستعمال غير المصرح به لنظام الحاسب واستخدام الحاسب الآلي لأغراض شخصية أو تجارية بدون علم مالكه أو حائزه القانوني.[2]

وهذا الفعل الغير مشروع من أكثر الجرائم المعلوماتية انتشارا وترتكب هذه الجريمة بواسطة مستخدمي الشركات الخاصة أو بواسطة المرافق العامة وفي معظم الأحيان تمارس هذه الجريمة بدون غرض اجرامي ولكن في بعض الحالات نجد مجموعة من المستخدمين تشغل جهاز عملهم الأصلي.[3]

وتتم سرقة خدمات الكومبيوتر باستخدام الغير مشروع لأنظمة المعلوماتية سرقة الخدمات المعلوماتية أو سرقة الوقت وهي واسعة الانتشار في مجال المعلوماتية كاستخدام أقام حسابات الشركة أو التلاعب ببيانات الكومبيوتر لمعرفة مثلا الوقت الفعلي لدفع الأجرة أو لمعرفة زبائن الركة أو الخدمات التي تقدمها.[4]

ثانيا: جريمة النصب والاحتيال المعلوماتي

1. النصب المعلوماتي

يقصد بالنصب: الاستيلاء على حيازة مال الغير الكاملة بوسيلة يشوبها الخداع تسفر عن تسليم ذلك المال ويتميز النصب عن السرقة في أن الاستيلاء على الحيازة الكاملة للمال تتم في السرقة بغير صلة من مالك أو حائز هذا المال يحصل في النصب بتسليم مشوب بالاحتيال عن طريق استعمال الجاني لأحد الطرق الاحتيالية التي يجرمها المشرع.

---

[1] عبد الله حسين علي محمود، المرجع نفسه، ص 210.

[2] محمد أمين أحمد الشوابكة، **جرائم الحاسوب والإنترنت – الجريمة المعلوماتية** –، دار الثقافة، الأردن، 2004، ص 170.

[3] محمد سامي الشوا، المرجع نفسه، 1998، ص ص 220، 221.

[4] محمد أمين الشوابكة، المرجع السابق، ص 171.

وبالحديث عن الطرق الاحتيالية فمن الممكن أن يكون الحاسب الآلي أحد وسائل الجاني في ارتكاب جريمة النصب بواسطة طرق احتيالية أو ما يعرف بالتلاعب المعلوماتي الذي يقصد به التلاعب بالبرامج والبيانات للتغيير فيها، مما يترتب عليه ايهام المجني عليه بصحتها مما يجعله يسلم بها فالجاني يتوصل إلى التلاعب في منظومات المعالجة المعلوماتية للبيانات للإستيلاء على مال الغير، كما يستخدم الحاسب لغرض التزييف والتزوير لإعداد سندات بطريقة الكترونية وحسابية من شأنها الإيحاء بوجود قوة أموال لأن الوثيقة المستخرجة من جهاز الحاسب تولد لدى الأشخاص ثقة كما ترتكب جرائم النصب المعلوماتي بواسطة الطرق التدليسية كاستخدام صفة غير صحيحة أو اسم كاذب باستخدام البطاقات البنكية الممغنطة أو الائتمانية من الجرائم المحيرة خصوصا في دول تتسم نظمها البنكية بدرجة عالية من التطور وقد جرم المشرع الجزائري النصب في المادة 372 من قانون العقوبات الجزائري فالنصب عند المشرع الجزائري هو الاستيلاء على مال الغير وذلك باستعمال طرق احتيالية حددها القانون.[1]

2. الاحتيال المعلوماتي

ينصرف اصطلاح الاحتيال بوجه عام إلى الغش والخداع الذي يعمد اليه أي شخص من الغير بدون وجه حق على فائدة أو ميزة ما.

ويقصد بالاحتيال المعلوماتي هو كل سلوك احتيالي يرتبط بعملية الحسيب الالكتروني بهدف كسب فائدة أو مصلحة مالية.

ويتميز الاحتيال المعلوماتي عن غيره من أنماط الاحتيال التقليدي أو العادي بالتعقيد الناجم عن استخدام المفاتيح والشفرات والدلائل المعلوماتية في ارتكابه، وينظر الكثيرين اليه باعتباره نوع من أنواع التحري الذهني، الزمن الازم لسلب الأموال بالاحتيال بالغش الى ثواني معدودة وهو ما انعكس من جهة و أصبحت هذه الأموال المتداولة عبر هذه الصور من الاحتيال

[1] المتضمن1966جوان 08الصادر في 66-156المعدل و المتمم للأمر رقم 15-19قانون رقم لقانون العقوبات الصادر في الجريدة الرسمية ، رقم 71 المؤرخة في 30 ديسمبر 2015.

المعلوماتي في المستقبل أكثر مما هي عليه الان نظرا للاعتماد على الأنظمة المعلوماتية في شتى المجالات.[1]

ثالثا: التعدي على البيانات

1. التعدي على البيانات و المعلومات المخزنة آليا

يرى الخبراء المتخصصون في أجهزة الحاسب الالي أن التلاعب في المعلومات والبيانات هو من أكثر أفعال الغش ارتكابا في الدول المتقدمة خاصة في الولايات المتحدة الأمريكية وأوروبا ويتم التلاعب إما عن طريق إدخال معلومات مصطنعة أو إتلاف المعلومات الموجودة بالفعل في جهاز الحاسب الآلي.[2]

*** اتلاف المعلومات الموجودة بالفعل في جهاز الحاسب الآلي:**

المسؤولون على تخزين المعلومات وحفظها يمكنهم وبكل بساطة أن يتلفوا ويغيروا المعلومات المكلفين بحفظها كاستبدال رقم برقم آخر أو وضع بطاقة محل أخرى، وهذه تتطلب فترة من الزمن قبل الكشف عنها.

ويتم إتلاف المعلومات أو تعديلها في أفعال الغش المعلوماتي بوسائل عديدة منها:

أ- ممارسة bluff: وتتمثل في استخدام أجهزة الحاسب الآلي.

ب- محو المعلومات.

جـ- التلاعب بالمعلومات عن بعد.[3]

2. التعدي على برنامج التطبيق ونظم التشغيل

هذا النمط من الجرائم هو من جرائم المتخصصين المحترفين فيستلزم معرفة فنية دقيقة وعميقة في مجال برمجة أجهزة الحاسب الآلي إلا أن تنفيذه صعب الا أنه يمكن أن يتحقق في عدة مراحل من صنع برامج التشغيل أو التطبيق أو في لحظة صيانتها أو تحديثها.

---

[1] محمد أمين الشوابكة، المرجع السابق، ص 180.

[2] محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر و الأنترنت (الجريمة المعلوماتية)، دار الثقافة، الأردن 2004، ص.ص.169، 170.

[3] محمد سامي الشوا، المرجع السابق، ص ص 71، 77.

أ-تعديل نظم أو برامج التطبيق:

هناك أيضا تقنية perruqueتتمثل في برمجة جهاز الكومبيوتر على استقطاب بعض السنتيمات من الإيداعات الدورية ويحولها إلى حسابات خاصة وهذه العملية تدر أرباحا كثيرة حيث تطبق هذه التقنية في البنوك التي تمنح فوائد للحسابات الجارية.

كما أنه هناك تقنية زرع برنامج فرعي غير مسموح به ومعروف لمستخدمه فقط في برنامج أصلي وسمح هذا البرنامج غير المشروع للجاني بالولوج غير المصرح به في موردات.[1]

الفرع الثاني: اختراق جهاز الحاسب الآلي واتلاف المعلومات

أولا: اختراق جهاز الحاسب الآلي

الاختراق هو الهجوم أو الدخول غير المصرح به لجهاز الحاسب الآلي ومن الممكن اختراق الحاسب أو انتحال هوية مستخدميه إما ماديا أو الكترونيا.

ويسمح الاختراق المادي بدخول الجاني إلى مناطق خاضعة للسيطرة عن طريق بوابة الكترونية أو آلية وأسلوب الاختراق الأكثر شيوعا هو أن يقف شخص مسموح له بالدخول أمام البوابات المغلقة حاملا بين ذراعيه متعلقات خاصة بالجهاز كالشرائط الممغنطة أو ينتظر حتى يتقدم شخص مسموح له بالدخول ويفتح له الباب فيدخل معه نفس الوقت لذا فان التواجد في صالات جهاز الحاسب الآلي هو أمر حتمي لارتكاب هذه الجرائم و تنطوي مشروعيتها في الإطلاع غير المصرح به للمعلومات في نظام المعلوماتية.[2]

وتتم عملية الاختراق كذلك ببرنامج يتم تصميمه ليتيح للمخترق الذي يريد اختراق جهاز الحاسب الآلي وهذا البرنامج (حصان طروادة) ويعتبر من أخطر البرامج على الإطلاق التي تستخدم في اختراق أجهزة الكومبيوتر نظرا لتمتعه بعدة ميزات منها ما يجعله قادرا على الاختراق دون القدرة على الكشف عنه وتتبعه.

ثانيا: الإتلاف المعلوماتي

الإتلاف المعلوماتي إما أن يكون عن عمد وقصد وإما أن يكون بغير قصد بل مجرد اهمال، وينصب الإتلاف المعلوماتي على الكيانات المنطقية لجهاز الحاسب الآلي وهي الأوامر

---

[1] عبارة عن العناصر الضرورية لأي نظام قانوني.

[2] محمد عبد الله أبو بكر سلامة، المرجع السابق، ص 144.

والتعليمات الازمة لتشغيل أجهزة الحاسب الآلي وانجاز مهامه وأكثر ما يتوصل به لتنفيذ الإتلاف ذي الأثر التدميري الذي يستهدف محو كل البرامج أو ملفات جهاز الحاسب الالي والمعلومات المخزنة به، هي البرامج الخبيثة التي تصيب الجهاز بالعطل والشلل وهذه البرامج عديدة ولكل تسمية خاصة بها تعبر عن وظيفتها التخريبية والأضرار التي تلحق بجهاز الحاسب الآلي وأبرز ما سبب من خسائر مادية فادحة ما يلي:[1]

1-استخدام برامج القنابل المنطقية "logicbombs":

هي عبارة عن برنامج ويتم في شبكة المعلومات يهدف تحديد ظروف أو حالة مضمون النظام.

2-استخدام برنامج القنبلة الزمنية أو الموقوتة "time bombs":

على عكس القنبلة المنطقية تماما حيث تبقى ساكنة وغير فعالة وغير مكتشفة مدة تصل إلى عدة أشهر، بل وحتى سنوات وهذه المدة يحددها عادة مؤشر زمني يحتويه البرنامج بحيث ينشط البرنامج عند حلول ذلك التاريخ ويؤدي مهامه التدميرية، وتثير القنبلة الزمنية حدثا في لحظة زمنية ثم تنطلق أو تنفجر وهي مرتبطة بعنصر الزمن تتحدد وفقا للتحديد الزمني.[2]

3-استخدام برامج الدودة "worm software":

هي البرامج التي تستغل أية فجوات في نظم التشغيل جهاز الحاسب الآلي من جهاز إلىآخر مغطية بأكملها لتحدث في النهاية آثارها التخريبية، وتنتقل هذه البرامج من شبكة إلى أخرى عبر الوصلات التي تربط وأثناء انتقالها تتكاثر كالبكتيريا بإنتاج نسخ منها ومن أهم أهداف تلك البرامج شغل أكبر مجال ممكن من سعة الشبكة وبالتالي تقليل أو خفض كفاءتها.[3]

الفرع الثالث: تخريب البرامج المعلوماتية بالفيروسات

هو كذلك إتلاف ومحو المعلومات والبرامج أو البيانات التي تم معالجتها إلا أن التقنية المستخدمة تختلف عن التقنية سابقة الذكر، أي البرامج فهنا تستعمل الفيروسات لإصابة

---

[1] محمد أمبن الرومي، المرجع السابق، ص 56.

[2] محمد أمبن الرومي، المرجع السابق، ص 57.

[3] محمد عبد الله أبو بكر سلامة، المرجع السابق، ص 156.

جهاز الحاسب الآلي بالشلل التام أوإعاقته عن القيام بأداء وظائفه ونظرا لخطورة هذه الفيروسات وجسامتها.

أولا: تعريف الفيروسات

الفيروس هو عبارة عن مجموعة من التعليمات التي تتكاثر بمعدل سريع جدا وتصيب النظام المعلوماتي بالشلل.[1]

والفيروسات هي برامج مصممة بقدرة على التكاثر والانتشار من نظام إلى آخرإما بواسطة قرص ممغنط أو عبر شبكة للاتصالات، بحيث يمكنه أن ينتقل عبر الحدود من أي مكان إلى آخر في العالم، وهو ما يسمى عادة باسم أول مكان أكتشف فيه.[2]

ثانيا: تصنيف الفيروسات و أنواعها:

1. تصنيف الفيروسات

أ – بوت سكتور " **boot sector**": يصب هذا الفيروس القسم من القرص الصلب الذي يحتوي على نظام التشغيل والملفات والمعلومات بها.

ب – فايل "**file**": يصب هذا الفيروس ملفات com.exo ثم يقوم بنسخ نفسه كلما جرى تشغيل البرنامج المصاب.

ج–in the Wild: تعبير مخصص للفيروسات التي أفلتت ويجري تداولها دون ردع وهي كثيرة جدا.

د– الفيروسات الكبوية: هي أكثر أنواع الفيروسات شيوعا وهي تنتسب 80% من اصابات أجهزة الحاسب الالي بالفيروسات و أبرز تلك الفيروسات خاصة Word، Excelحيث تقوم الفيروسات بتنفيذ مجموعة معلومات أوتوماتيكية.

هـ– الفيروسات متعددة الأطراف: هذه الفيروسات تعتمد مجموعة متنوعة من التقنيات لينسخ نفسه وتنتشر بسرعة.

---

[1] محمد علي العريان، المرجع السابق، ص 83.

[2] نائلة عادل محمد فريد قورة، **جرائم الحاسب الآلي الاقتصادية**، مستندات الحلبي الحقوقية، مصر، الطبعة الأولى، 2005، ص 192.

و- الفيروسات ذات التبديلات المتعددة: "poly morplic"

وطبيعة تكوين هذه الفيروسات أنها تتبدل كلما انتشرت وهو ما يؤدي الى تغيير جذري في الفيروس كل مرة وهذه الخاصية تجعل من الصعب كشف الفيروسات.

ح-فيروساتzoo: هذه الفيروسات يقوم بها القراصنة أو علماء الكومبيوتر ويطورونها ضمن مختبرات خاصة ويقدر عددها بـ 18 ألف فيروس ولا يعرفها سوى مطورها.

8- فيروسات الحقبة: تعتمد على برمجيات خاصة يتيح لها الاختفاء فور تشغيل برنامج مضاد للفيروسات أي أنها مصممة في الأصل لتقاوم تلك البرامج ومعظم هذه الفيروسات يصيب نظام التشغيل Dos وليس Windows.[1]

2. أنواع الفيروسات:

الفيروسات خطيرة جدا فكتابة الفيروس هي في حد ذاتها من أخطر الجرائم ونشره في حسابات الاخرين هو جريمة أخرى لا تقل شرا أو خطورة ولقد قسمها الفقهاء إلى فيروسات من حيث تكوينها وأهدافها:

أ-فيروس عام العدوى: هو ذلك الفيروس الذي ينتقل إلى أي برنامج أو ملف معلوماتي.

ب- فيروس محدد العدوى: هو ذلك الفيروس الذي يستهدف نوعا محددا من النظم لينتقل إليها ويهاجمها ويتميز عن النوع السابق أنه أبطأ في الانتشار وأصعب في الاكتشاف.

ج- فيروس عام الهدف: ويندرج تحت غالبية الفيروسات التي اكتشفت حتى الان ويرجع ذلك إلى سهولة اعداد تلك الفيروسات واتسام مدى تخزينها.

د- فيروس محدد الهدف: يحتاج اعداده الى درجة عالية من الذكاء والكفاءة والمهارة، وقد يجري هذا الفيروس تلاعبا ماليا أو يدخل تعديلات في تطبيق عسكري وقد ينتهي وجوده بعد تنفيذ هدفه، وهي لا تؤدي إلى تعطيل عمل البرامج بل تبدل فقط الهدف.

*** أشهر أنواع الفيروس التي يتم رصدها على الساحة الإلكترونية:**

1- فيروس أنجلو.

2- فيروس الجمعة 13.

3- فيروس ألا ميدا.

[1] محمد علي العريان، المرجع السابق، ص ص 87، 88.

4- فيروس القردة.

5- فيروس ماكنتوش.

6- فيروس الجنس.

7- فيروس ناسا.

8- الفيروس الإسرائيلي.

9- فيروس الكريسماس.

10- فيروس الحب.

11- فيروسات باب المصيدة.

12- الفيروس المشفر.

13- الفيروس متعددة الأشكال (Polymorplic virus).

3. كيفية الوقاية من الإصابة بالفيروس:

فإذا لاحظ مستخدم الكومبيوتر بعض الأعراض السابقة أو إحداها فعليه أن يبادر إلى بذل الجهد الحريص اليقظ ليوقف الأضرار أو على الأقل أن يحد منها وذلك باتباع الإجراءات التالية:

1- ضرورة اغلاق الجهاز فور اكتشاف أي من الأعراض السابقة.

2- ادخال القرص المحمي الذي يحتوي على ملفات تحميل نظام التشغيل في وحدة الأقراص.

3- يتم اعادة تشغيل الجهاز وفي هذه الحالة يتم التحميل من القرص المحمي وليس القرص الصلب الملوث بالفيروس.

4- سرعة ارسال القرص الصلب الملوث بالفيروس ونسخ البرامج الملوثة به إلى معاهد الأبحاث المتخصصة في الفيروسات للتحقق من وجود الفيروس وتصميم البرامج – virusanti.[1]

[1] محمد علي العريان، المرجع السابق، ص ص 92، 93.

المطلب الثاني: جرائم الأنترنت

إن الشبكة المعلوماتية قد غزت العالم و تنوعت الجرائم التي ترتكب عن طريقها كتنوع المواقع التي تحتويها حيث سنجد أن هناك مواقع هي في حد ذاتها مخالفة للقانون ، نتعرف عليها في هذا المطلب.

الفرع الأول: المواقع المخلة بالآداب العامة و الهجوم على المواقع

أولا: المواقع المخلة بالآداب العامة

سوف نتحدث هنا باختصار شديد عن المواقع غير الأخلاقية على شبكة الأنترنت،حيث أن شبكة الأنترنت تتيح أفضل الوسائل لتوزيع الصور الفاضحة والأفلام الخليعة بشكل علني فاضح يقتحم على الجميع بيوتهم ومكاتبهم فهناك على الشبكة طوفان هائل من هذه الصور والمقالات والأفلام الفاضحة بشكل لم يسبق له مثيل في التاريخ[1]، هذه المواقع الإباحية تهدف إلى تحقيق مكاسب مادية، تعطي لزوارها بعض الصور الجنسية مجانا، لجذبهم في الأول ثم بعد التأكد من اعتيادهم لزيارة مواقعها تبدأ بفرض المبالغ المالية.[2]

المشرع الجزائري نص في المادة 333 من قانون العقوبات: "يعاقب بالحبس من شهر إلى سنتين كل من ارتكب فعلا علنيا مخلا بالحياء"، والمادة 333 مكرر يعاقب بالحبس من شهرين إلى سنتين كل من وضع أو أجاز أو استورد أو سعى في استيراد من أجل التجارة أو وزع أو أجر أو لصق أو أقام معرض أو عرض أو شرع في العرض للجمهور أو باع أو شرع في البيع أو وزع أو شرع في التوزيع كل مطبوع أو محرر أو رسم أو اعلان أو صور فوتوغرافية أو أصل الصورة أو قابلها أو انتج أي شيء مخل بالحياء.

ثانيا: ممارسة الدعارة عبر الإنترنت

ويوجد نوع من الشبكات تستعمل طرق احتيالية يصعب ضبطها وذلك بتهجير فتيات من أوروبا الشرقية مقابل مبالغ مالية واجبارهن تحت وطأة التهديد ممارسة الدعارة كما توجد

---

[1] حسن ظاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية الأمنية، الرياض،2000، ص 93.

[2] منير محمد الجهيني وممدوح محمد الجهيني، **جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها**، دار الفكر الجامعي، الإسكندرية، 2004، ص 29.

شبكات لنقل حفلات وعروض اباحية مباشرة وحية للترويج مقابل عمولات مالية يتم تحويلها في حساباتهم البنكية وبهذا تطورت إلى دعارة الكترونية.

ثالثا: الهجوم على المواقع والدخول إلى المواقع المحجوبة

يعتبر الهجوم على المواقع المختلفة في شبكة الانترنت (اقتحام المواقع) من الجرائم الشائعة في العالم، وقد تعرضت لهذا النوع من الجرائم في الولايات المتحدة مثلا كل من وزارة العدل و المخابرات المركزية والقوات الجوية كما تعرض له حزب العمال البريطاني، وفي مثل هذا النوع من الهجوم كثيرا ما يكون الضرر محدودا، كأن يقوم المهاجم بوضع صورة خليعة على هذا الموقع أو تعديل بعض العناوين من باب السخرية. هذه الأعمال التي تبدو تافهة و غير مؤذية تؤدي الى اضعاف الثقة في صحة بيانات هذه المواقع، وبالرغم أن المسؤولين عن هذه المواقع قد اعتادوا على ازالة اثار هذه العملية، الا أنه في بعض الأحيان قد يكون الضرر أخطر فقد يقوم المجرم بتعديل المعلومات على الموقع كأن يقوم بتعديل أسعار السلع أو اقتحام بعض الإعلانات عن بضائع وهمية غير مقدمة في هذا الموقع.[1]

أما بالنسبة للمواقع المحجوبة فهي ممنوعة على زائري شبكة الأنترنت دخولها ذلك يحجبها مثل المواقع التي لا تتماشى مع تقاليدنا الاجتماعية وديننا، والمواقع الجنسية الإباحية إلا أن بعض الأشخاص يعملون على تلك المواقع المحجوبة.

الإغراق بالرسائل الإلكترونية:

تتم عملية الإغراق بالرسائل (spamming) وهي تعتبر من جرائم نظم المعلومات عن طريق إرسال عشرات الرسائل من البريد الإلكتروني لشخص ما أو للعديد من مستخدمي الأنترنت. وقد بدأت هذه العملية في عام 1996 عندما أرسلت احدى الشركات اعلانات عنها بالبريد الإلكتروني إلى الآلاف من مواقع الأنترنت، وفضلا عن تعطيل الشبكة الذي نجم عن هذا الإغراق فقد تكلف متلقو هذه الرسائل الكثير في استقبالها ودفع ثمن مدة الاتصال اللازمة لاستقبال هذه الرسائل مع من يصاحبها من ملفات، ويقع الضحية لهذه الجريمة أيضا مقدمو خدمة الأنترنت حيث يتم ملء منافذ الاتصال(communication ports) و قوائم الانتظار(queves) لأجهزة الخدمة الخاصة بهم، وينتج عن ذلك انقطاع الخدمة عن زبائنهم.

[1] حسن داود، المرجع السابق، ص ص 83، 84.

وتجري حاليا من جانب شركات نظم المعلومات التطوير برامج تتعامل مع هذه الحالات باستقبال جزء محدود من الرسائل عندما يحدث سيل مفاجئ منها حتى لا تنقطع الخدمة.[1]

الفرع الثاني: الجرائم المنظمة والإرهاب الإلكتروني

أولا: الجرائم المالية

تشمل الجرائم المالية السطو على أرقام البطاقات الائتمانية ولعب القمار والتزوير، والجريمة المنظمة والمخدرات وغسيل الأموال، ولعل جرائم هذا النوع أوضح من ناحية كونها مجرمة، حيث لا تختلف في نتيجتها عن الجرائم التقليدية التي تحمل نفس المسمى والتي يعرف الجميع أنها مخالفة للنظام وللشرع، لأنها من الجرائم التي اشتهر لمحاربتها جنائيا، وهذه الجرائم هي كالآتي:

1 –جرائم تزوير بطاقات الائتمان:

تصدر بعض المؤسسات المصرفية والبنوك والشركات الكبرى بطاقات تستخدم كبديل للنقود أو الأوراق النقدية وتستخدم هذه البطاقات لسداد المشتريات كما تستخدم لسحب الأرواق النقدية عن طريق أجهزة وماكينات الصرف الإلكترونية.[2]

وبذلك أصبحت هذه البطاقات أكثر انتشارا واستخداما في أوروبا وأمريكا وكثير من دول العالم الأخرى، ولقد ظهرت بطاقات الائتمان خلال الخمسينات عندما صدرت بطاقات(Dinner club) في عام 1950 ثم تلاها أمريكان اكسبرس (American Express) عام 1959 صدرت بطاقات VISAمن بنك "أمريكا" ثم أصدر اتحاد البنوك بطاقة ماسترشارج (Master Charge) وعندما أصبح هناك عدد لا بأس به من هذه البطاقات لجأ مصدرو هذه البطاقات إلى زيادة وسائل الضمان ولحماية هذه البطاقات تمت اضافة الشريط الممغنط عام 1969.

وبانتشار هذه البطاقات وتعدد و تنوع استخداماتها ظهرت صور اجرامية لم تكن معروفة من قبل تشمل استخدام بطاقات مزيفة جزئيا، واستخدام بطاقات مزيفة كليا، وكذلك استخدام بطاقة ائتمان مسروقة، أو استخدام بطاقات صحيحة ظهرت بطريقة غير مشروعة، و كذلك

[1] حسن داود، المرجع السابق، ص 93.

[2] حسن داود، المرجع السابق، ص 94.

تواطؤ التجار مع المجرمين في استخدام البطاقات، ويعد هذا من أخطر أنواع هذه الجرائم ويتم بقبول بطاقات من أشخاص غير مصرح لهم باستخدامها وليسوا أصحابها.

وينتج عن هذه الجرائم فقدان مبالغ مالية طائلة من المؤسسات المالية والبنوك تبلغ سنويا حوالي ثلاثة ملايين دولار 50% منها بالولايات المتحدة الأمريكية وغيرها وكذلك يقوم بعض العملاء بتسديد فواتير شراء لم يقوموا أصلا بها كما نتج عن ذلك زيادة في الرسوم المستحقة على هؤلاء العملاء وقد ظهرت حديثا عصابات منظمة تتعامل بالبطاقات بصورة غير مشروعة أو تسئ استخدام هذه البطاقات.[1]

ويتعدى الأمر المخاطر الأمنية التي تتعرض لها بطاقات الائتمان، فتحت في بداية في بداية ثورة نقدية باسم النقود الإلكترونية (Electronic – Cash) أو (cyber–Cash) والتي يتنبأ لها أن تكون مكملة للنقود الورقية والبلاستيكية (بطاقات الائتمان) وأن يزداد الاعتماد عليها والثقة بها، كما أن هناك الأسهم والسندات الإلكترونية المعمول بها في دول الاتحاد الأوروبي، والتي أقر الكونجرس الأمريكي التعامل بها في عام 1990، وبالتالي فإن التعامل مع هذه الأسهم والسندات الإلكترونية من خلال الأنترنت سيواجه مخاطر أمنية ولا شك.

ولذلك لجأت بعض الشركات والبنوك إلى العمل سويا لتجاوز هذه المخاطر كالاتفاق الذي وقع بين مؤسسة هونج جونج وشنغهاي البنكية (HSBC) وهي من أكبر المؤسسات المصرفية بهونج كونغ وشركة كومباك للحاسب الآلي، وذلك لتطوير أول نظام آلي أمن للتجارة الإلكترونية والذي منح التجارة خدمة نظام دفع أمر لتحرير عمليات الشراء عبر الأنترنت.[2]

وجرائم السطو على أرقام البطاقات الائتمانية مجرمة شرعا وقانونا حيث تصنف ضمن جرائم السرقات.

---

[1] ندوة علمية عقدت في تونس في الفترة من 28 – 30 جوان 1999، تحت عنوان الظواهر الإجرامية، 1999، ص ص 219، 220.

[2] منير محمد الجهيني وممدوح محمد الجهيني، المرجع نفسه، ص ص 66، 67.

2 – القمار على الأنترنت:

مع انتشار شبكة الأنترنت فقد أصبح لعب القمار أسهل وأصبح تجمع اللاعبين من أنحاء العالم في مكان واحد على شبكة الأنترنت، حيث يتوفر لهم ما يحتاجونه من برامج للعب القمار فبات من الإمكان اللعب من المنزل مباشرة دون الاضطرار إلى الخروج فالأنترنت أسهمت بطريقة سلبية في انتشار لعب القمار، وقد يكون لعب القمار مصرح به في بعض البلدان إلا أن الأغلب الأعم من البلدان مصرح به بشكل محدود جدا، فنجد أنه حتى في أمريكا أن لعب القمار عبر الأنترنت غير مسموح به قانونا على الاطلاق ليتفادى أصحاب تلك المواقع المشاكل القانونية.[1]

3– غسيل الأموال:

معناها هو تنظيف الأموال القذرة المتأتية عن طريق الجريمة، ومع عدم الكشف عن المصدر الغير مروع لتلك الأموال، ويتم تنظيفها عن طريق ادخالها في القنوات المصرفية العادية ثم استخدامها في عمليات مالية والدخول في مجالات مشروعة للاستثمار وبالتالي تندرج في تلك المشروعات ويتعذر الرجوع الى أصلها، وقد زاد حجم الأموال القذرة الممنوعة في السوق بغسيلها عن طريق تغلغلها في السوق المشروع بإنشاء الشركات والفنادق والمطاعم...، وقد ظهر غسيل الأموال مع ظاهرة الاتجار بالمخدرات، ولذلك عرفت أولا عن ذلك الطريق ولكن غسيل الأموال فيما بعد شمل أكثر من نشاط اجرامي زيادة على الاتجار بالمخدرات وظهر ذلك النشاط كأخطبوط تتعدد أطرافه وذلك ليس فقط لأن النشاط الاجرامي مصدر المال يظل خفيا، وكذلك ليس فقط لأن المال المغسول يظهر على السطح كمال شرعي بعد أن تم تنظيفه من القذارة، أي نظافة للأموال القذرة التي تم الحصول عليها بواسطة الجريمة والجرائم التي ينتج عنها أموال يتم غسلها هي:

–المخدرات وهي أول مصدر غير مشروع لفت الانتباه لعملية غسيل المخدرات.

–تجارة الأسلحة غير المشروعة، فنجد أن الجماعات المسلحة لديها فائض من الأسلحة وكذلك لوجود قيود شراء الأسلحة من الدول والتي تضع شروطا لذلك، وجرائم أخرى.

---

[1] السنباطي عبد العاطي، **موقف الشريعة الإسلامية من جرائم الحاسب الألي و الأنترنت** ، دار النهضة العربية، 2002، ص ص 68، 69.

– الاتجار بالأعضاء البشرية، السياحية الجنسية، المتاجرة في العملة بطريقة غير شرعية.[1]
لقد قامت الدول الصناعية الكبرى أثناء قمة في باريس في جويلية 1989 بإنشاء مجموعة عمل مالي دولي، حيث كان تقريرين لرصد عمليات وحجم غسل الأموال وهو التقرير الحادي عشر في 03 فيفري 2000 عن الفترة 1999 – 2000 والثاني عشر في 01 فيفري 2001 عن الفترة 2000 – 2001 وجاء في هذين التقريرين أساليب غسيل الأموال عبر شبكة الأنترنت تتمثل في العمليات المصرفية وأنظمة التحويلات وهي الأنظمة السرية أو المصرفية الموازية، استخدام الجهاز المصرفي onlineلغسيل أموال المقامرة عبر شبكة الأنترنت.[2]

المشرع الجزائري قام بتشريع نصوص جديدة في التعديل ما قبل الأخير لقانون العقوبات على تجريم غسيل الأموال في المادة 389 مكرر 2، 389 مكرر 7.

ثانيا:الجريمة المنظمة:

تعتبر الجريمة المنظمة من الأنماط الحديثة للإجرام بجانب الجرائم التقليدية التي تحددها وتنص عليها التشريعات الجنائية للدول، ومع بداية التسعينات بدأت بشكل واضح ظهور الجريمة المنظمة عبر الدول على الساحة الدولية، ولعل أبرز هذه المتغيرات هو النمو الشامل والمتسارع للأنشطة التجارية المالية والاقتصادية أدى الى تجاوز للحدود الوطنية في التجارة والتحويل وشبكات الأنترنت، وأساس الجريمة يتمحور في أنها تقوم على تنظيم مؤسس ثابت وهذا التنظيم له شروط خاصة تنظم صلاحية القائد والأفراد وشروط الترقي في اطار التنظيم، وعنصر الاستمرارية طالما الجريمة المنظمة قائمة ومادامت تحقق نجاحا كبيرا، ولم تنجح أجهزة الأمن في القضاء عليها، الجريمة المنظمة تضم بين طياتها الالاف من المجرمين الذين يعملون وفقا لنظام بالغ التعقيد والدقة تفوق النظم التي تتبعها أكثر مؤسسات تطورا وتقدما كما يخضع أفرادها لأحكام قانونية سنوها لأنفسهم تفرض أحكام بالغة القسوة على من يخرج على ناموس الجماعة المنظمة ويلتزمون في إدارة نشاطاتهم الاجرامية بخطط دقيقة ومدروسة ويجنون من ورائها الأرباح الطائلة.

---

[1] الندوة العلمية التي عقدت في تونس، المرجع السابق، ص ص 25، 26، 27.

[2] محمد عبد الله أبو بكر سلامة، المرجع السابق، ص 204.

وتكون لهذه المجموعات الاجرامية قاعدة عمل في الدول الضغينة التي تؤمن ملاذا امنا تستطيع من خلاله ممارسة عملياتها العابرة للحدود الجغرافية، وفي الواقع يوفر هذا الأمر قدرا اضافيا من الحماية من تطبيق القانون ويمكن لتلك المجموعات من ممارسة نشاطها بأقل قدر ممكن من المخاطر.

والجريمة المنظمة موجودة منذ فترة طويلة أي لم تعتمد على التقدم التقني الحالي في تكوينها أو انشائها، انما استغلت التقدم في تقوية الروابط فيما بين أعضائها، وكذلك في تسهيل عملية توصيل الأوامر والتعليمات إلى أعضائها بصورة مشفرة دون أن يقوم بتعقبها أي جهاز قانوني محلي أو دولي.[1]

وتدخل ضمن الجرائم المنظمة تجارة المخدرات التي هي أحد أهم أخطر الجرائم على مستوى العالم لم تفلح الجهود المبذولة على مستوى العالم في تقليلها دون منعها نهائيا لوجود بعض دول العالم التي تتركز فيها تصنيع المخدرات وتهريبها إلى باقي دون العالم. وقد كان تجار المخدرات يلاقون صعوبات كثيرة في الاتفاق على عمليات التهريب على مستوى العالم إلا أن التطور التكنولوجي الكبير والمتمثل في انتشار شبكة الأنترنت فقد استغلها مصنعو ومصدرو المخدرات واستخدموها في الاتفاق على عمليات التهريب من بلد إلى آخر.[2]

ثالثا: الارهاب الالكتروني:

في عصر الازدهار الالكتروني وفي زمن قيام حكومات الكترونية، كما جاء في الامارات العربية المتحدة، تبدل نمطا الحياة وتغيرت معه أشكال الأشياء وأنماطها ومنها لا شك أنماط الجريمة التي قد يختلط بعضها بمسماها التقليدي مع تغير حصري أو يسير في طرق ارتكابها، ومن هذه الجرائم الحديثة في طرقها القديمة في اسمها، جريمة الإرهاب الالكتروني التي اخذت منحى حديثا يتماشى مع التطور التقني.

وقد انتبه الغرب إلى قضية الارهاب الالكتروني منذ فترة مبكرة، فقد شكل الرئيس الأمريكي السابق بين كلينتون لجنة خاصة مهمتها حماية البنية التحتية الحساسة في أمريكا والتي قامت في خطوة أولى بتحديد الأهداف المحتمل استهدافها من قبل الارهابيين ومنها مصادر

[1] منير محمد الجهيني وممدوح محمد الجهيني، المرجع السابق، ص ص 73، 74.

[2] منير محمد الجهيني وممدوح محمد الجهيني، المرجع نفسه، ص 77.

الطاقة الكهربائية والاتصالات اضافة إلى شبكات الحاسب الآلي، ومن ثم انشاء مراكز خاصة في كل ولاية مع احتمالات أي هجمات ارهابية الكترونية.

كما قامت وكالة الاستخبارات المركزية بإنشاء مركز حروب المعلوماتية وظفت به ألفا من خبراء أمن المعلومات، كما شكلت قوة ضاربة لمواجهة الارهاب على مدار الساعة، ولم يقتصر هذا الأمرعلى هذه الوكالة بل تعداه إلى الأجهزة الحكومية الأخرى كالمباحث الفيدرالية الجوية.

وكان أول عمل قامت به تلك اللجنة هو تحديد الأهداف المحتملة المستهدفة من طرف الإرهابيين، مثل مصادر الطاقة الكهربائية، قطاع الاتصالات، شبكات الكومبيوتر خاصة القطاعية منها، ثم قامت بإنشاء مراكز خاصة في كل ولاية للتعامل مع احتمالات وقوع أي هجوم إرهابي معلوماتي عليها.

وقامت أجهزة الاستخبارات المركزية الأمريكية (C.I.A) بإنشاء مركز حروب المعلوماتية ووظفت به 1000 اطار من خبراء أمن المعلومات.

فقد جاء في أحد التقارير المعدة من طرف وزارة الدفاع الأمريكية بأن شبكة الاتصالات ومصادر الطاقة الكهربائية، البنوك، وقطاعات النقل في أمريكا معرضة للهجوم من قبل أي جهة تسعى الى محارية أمريكا بدون أن تواجه قواتها.[1]

الفرع الثالث: جرائم القرصنة والتجسس

أولا: المواقع المعادية

المواقع المعادية هو مصطلح حديث بدأ استخدامه بعد التطور التكنولوجي الذي نعيشه، فصمموا تلك المواقع واستغلوا التكنولوجيا لخدمة أغراضهم الشخصية في عرض أفكارهم التي يمتلكون الشجاعة الكافية لعرضها عن طريق سلك الطرق الشرعية، ويكون الغرض من هذه المواقع المعادية تشويه صورة الدولة أو المعتقد أو الشخص المستهدف وتفصيلها كالآتي:

أ- **المواقع السياسة المعادية:** قد ينظر البعض الى انشاء هذه المواقع باعتبارها ظاهرة حضارية تتماشى مع الديمقراطية والحرية الشخصية، وهذا غير صحيح فللديمقراطية والحرية

[1] بورزام أحمد وكيل الجمهورية لدى محكمة باتنة بالمجلس القضائي، محاضرة بعنوان **جرائم المعلوماتية**، 2006/06/20، ص 23.

الشخصية حدود يجب ألا تتجاوزها وإلا أصبحت سوء أدب وهناك ولا شك طرق وأساليب يمكن معها عن الآراء الشخصية.ولذلك فليسفي إنشاء المواقع السياسية المعادية أي حرية رأي أو ديمقراطية بل هي سوء أدب ان لم يكن بغي يعاقب عليه الشرع بالقتل.[1]

ب-الوقائع الدينية المعادية:

فالإساءة الى بلد معين وإلى مواقف قادته السياسة من قضاياه الوطنية وهو غالبا ما يكونون من معارضي النظام السياسي القائم في بلد ما فيحاولون نشر الأخبار الفاسدة التي تنشر الفرقة بين أفراد الشعب والنظام السياسي.

والاساءة الى شخص معين لما يمثله من مواقف سواءا دينية أو سياسة، وما إلى ذلك من الأهداف التي لا يجد القائمين عليها من يستمع لآرائهم المغلوطة أو التي تتنافى مع الدين والمبادئ وعليه يجد هؤلاء في شبكة الأنترنت ضالتهم المنشودة في الوصول إلى أكبر عدد من الأشخاص لعرض آرائهم عليهم في محاولة منهم لكسب تأييدهم دون محاولة منهم بالتعريف عن أنفسهم خوفا من رد أفعال الناس التي غالبا ما ترفض تلك الأفكار نقض المواقف السياسية دون التعرض بشخصيات والأعراض هو من الأمور المقبولة أما التعرض للأديان فهو من الأمور الغير مقبولة.[2]

المطلب الثالث: كيفية ضبط جرائم الحاسب الآلي والأنترنت

يقدم الحاسب الآلي خدمات جليلة غير محدودة للإنسان في حياته اليومية، وبذات القدر يمكن أم يقدم الحاسب الالي للمجرمين خدمات في التخطيط للجريمة و الاعداد لها و تنفيذها والتخلص من آثارها. ومن الممكن أن يستخدم الحاسب الآلي أينما وجد في ارتكاب جريمة تتعلق بالمهمة التي يؤديها الحاسب الآلي في ذات الموقع أو غيره، ويستخدم الحاسب الآلي في ارتكاب انواع متعددة من الجرائم تبدأ من أبسط أنواع الجرائم مثل التلاعب بمعلومات الحسابات المالية، تمتد حتى أكثر أنواع الجرائم خطورة وتعقيد مثل استخدام الحاسب الآلي في التخطيط لمشروع إجرامي أو لبرهنة عملية تفجير احدى المنشآت، أو القرصنة الفضائية،

[1] السنباطي عبد العاطي، المرجع نفسه، ص 134.

[2] منير محمد الجهيني وممدوح محمد الجهيني، المرجع السابق، ص 82.

وفي ما يلي وصف لبعض أنماط جرائم الحاسب الآلي السائدة اليوم وطرق ارتكابها مع بيان لبعض المؤشرات التي تعين المحقق على جمع الأدلة الازمة لمعاقبة الجناة فيها وهي:

1- الغش المعلوماتي: "date didding"

هي أبسط جرائم الحاسب الآلي وأكثرها انتشارا، إلا أنه من الصعب اكتشافها وضبط الجناة فيها، ويتم تنفيذ هذا النوع من جرائم الحاسب الآلي بتعديل المعلومات قبل أو أثناء الادخال في الحاسب الآلي ويمكن أن لايتم التعديل من قبل أي شخص له الصلاحية في الوصول إلىإجراءات الأعداد، التسجيل، النقل، الفحص، المراجعة وتحويل تلك المعلومات.

2- حصان طروادة: "Trojan Horse"

عملية حصان طروادة هي تغطية أوامر الحاسب الآلي لتمكين الحاسب الآلي من الإتيان بوظائف غير مصرح له بها مع ترك البرنامج على حاله للاستثمار في تحقيق أهدافه، وهذه هي الطريقة الغالية في الاحتيال والتخريب بواسطة الحاسب الآلي، ويكون له القدرة في الوصول إلى جميع المعلومات والملفات ولا يمكن منع واكتشاف هذا النوع من الجرائم اذ كان المتهم لديه الذكاء والخبرة الكافية.

3- "Salami Techniques"

وهي السرقة الآلية لجزء قليل من الأرصدة المالية الكبيرة باستخدام اسم وهمي وشريك، مع امكانية التغيير مؤقتا من حساب لآخر بصفة مستمرة على شكل دائري لتقليل فرص الاكتشاف بحيث توزع الخسائر القليلة على عدد كبير من أصحاب الأرصدة من حيث لا يأبه الفرد بما يطرأ على رصيده عن اكتشاف مثل هذه الجرائم يحتاج إلى خبرة في مراجعة الحسابات وبناء برامج مراقبة داخل البرنامج المشتبه فيه.

4-القرصنة العالية:"Super Zapping"

القرصنة العالية تأخذ اسمها من التدخل فوق العادة، وهي برنامج للاستعمال الكبير المستخدم في كثير من مراكز الحاسب الآلي لمعالجة المشاكل المستعصية في الحاسب الآلي وهو بمثابة المفتاح العام (Master key) الذي يرجع اليه عندما تفشل الوسائل الأخرى.[1]

[1] محمد الأمين البشيري، **التحقيق في الجرائم، المستحدثة**، مركز الدراسات و البحوث، جامعة نايف العربية ، السعودية، 2004 ، ص ص95، 96.

5- أبواب الشراك:"Trap Doors"

لتطوير التطبيقات الكبيرة و نظم عمليات الحاسب الآلي يلجأ المبرمجون إلى وضع معينات لإيجاد فواصل في الكود تمكن من وضع كوداتإضافية وقدرات للمخرجات، وبما أن تصميم نظم عمليات الحساب الآلي يحول دون الوصول إلى الكود وتعديله يقوم المبرمجون أحيانا بوضع كود يسمح بالتسوية بين المطلبين أثناء وضع المعينات أو عند الانتهاء من تطوير النظام وحفظه، وتعرف هذه التسهيلات بأبواب الشراك وتتم ازالة هذه التسهيلات في النهاية إلا أنها تترك أحيانا للاستخدام مستقبلا. ويجوز وضع أبواب الشراك أحيانا على الدوائر الالكترونية للحاسب الآلي، وعند القيام بعمليات الصيانة أو الاستعمال العادي يكتشف بعض المبرمجون هذه التسهيلات ونقاط ضعفها ويستغلونها لأعمال غير مشروعة مثل ترجمة برامج أخرى أو الدخول عليها خاصة في الأجهزة التيع تعمل في شكل شبكات أو أنترنت.

6- القنابل المنطقية: "LogicBombs"

القنابل المنطقية هي برنامج حاسب آلي نفذ في وقت ملائم أو محدد في جهاز حاسب آلي يحدد ظروف الحاسب الآلي الذي يسهل أو يساعد الشخص الذي يقوم بالتحضير لعمل غير مشروع أو غش.

7-الهجوم المتزامن: "Asynchronons Attack"

يستغل الهجوم المتزامن الوظيفة التزامنية لنظام تشغيل الحاسب الآلي، اذ أن معظم نظم التشغيل للحاسب الآلي تقوم على هذه الوظيفة وهناك طريقة على درجة عالية من التقدم لإرباك نظام التشغيل وتمكنه من مخالفة البرنامج الذي يعزل كل ملف أو عملية عن غيره، وبإزالة العازل يسهل الوصول إلى تلك العمليات أو الملفات والتلاعب بمحتوياتها.

على المحقق أن يكون ملما باحتمالات الهجوم وأن يبحث عن المساعدات التقنية الازمة عند ظهور ما يبرر الشك أو الاشتباه.

8- البحث في المهملات:

البحث في المهملات طريقة من طرق الحصول على المعلومات المهمة حول جهاز الحاسب الآليمع تنفيذ عملية معينة.

9-تسريب المعلومات: "Data Leakage"

هناك أنواع كثيرة من الجرائم المتعلقة بالحاسب الآلي يحتاج تنفيذها إلىإخراج البيانات أو نسخ منها من الحاسب الآلي أو من مراكز المعلومات الخاصة بالحاسب الآلي، يقوم مرتكب الجرائم الحاسب الآلي بإعداد وتحضير الجوانب الفنية لجريمة داخل الجهاز أثناء عمله العادي ودون أن يدرك أحد ما يسعى إليه الجاني، ولكن قد لا تكتمل الجريمة التي يخطط لها الجاني وتحقق أهدافها المادية إلا بإخراج البيانات وتسريبها إلى مكان آخر، ويتم تسريب البيانات بعدة طرق فنية تتوقف على مدى كفاءة المبرمج وخبرته وذلك بإخفاء المعلومات المراد تسريبها بجانب البيانات العادية أو اعدادها بكود سري لا يفهمه إلا الجاني وتتوافر فرص إعداد الكود أو التشفير مع تطور القدرات الفنية للحاسب الآلي الذي أصبحالآن قادرا على إعداد الرسومات البيانية بأشكال وألوان مختلفة وصور وخرائط وانغام موسيقية، وذبذبات صوتية.[1]

10- انتحال الشخصية والتسلل: "Piggybacking and Impersonation"

تستخدم أساليب انتحال الشخصية أو التسلل الالكتروني للدخول إلى المناطق المؤمنة والمحمية الكترونيا أو الوصول إلى مراكز الحاسب اللي والدخول على قواعد المعلومات، قد يكون الدخول شخصيا أو الكترونيا. فالدخول الشخصي يتم عن طريق انتحال شخصية أحد العاملين في المكان المؤمن، أما الدخول أو التسلل الالكتروني يمكن أن يتم بتوصيل طرفيه إلى أحد الطرفيات المخولة لها بالدخول عن طريق خط هاتفي، ويجد الفرصة في المعلومات المركزية عندما تفتح الطرفية الأصلية بمفتاحها السري، وتواصل الطرفية المتسللة أيضا نشاطها عند توقف الطرفية الأصلية، وخاصة عندما تقفل تلك الطرفية بطريقة غير سلمية، ورغم امكانية السيطرة على هذا النوع من الاختراقات بالرسائل المتطورة والحراسات الشخصية والمراقبة الالكترونية الا أن المحاولات الذكية لمحتالين تتعدى كل الاحتيالات.[2]

[1] محمد الأمين البشيري، المرجع السابق، ص ص 100، 101.

[2] محمد الأمين البشيري، المرجع نفسه، ص ص 102، 103.

11-سرقة المكالمات الهاتفية والرسائل الالكترونية: "Wiretapping"

بدأت سرقة المكالمات الهاتفية عن طريق التنصت وتسجيل المكالمات مع تطور تقنية الاتصالات من البرقيات السلكية إلى الرسائل الالكترونية وشبكات الأنترنت أصبحت ظاهرة سرقة المعلومات تأخذ صورا خطيرة تتمثل في القرصنة الفضائية واعتراض الرسائل وتشويش الاتصالات بمقاصد مختلفة، لقد وفرت العلوم الحديثة تقنيات تحد من سرقة المكالمات الهاتفية والتنصت، كما أن الحصول على المعلومات قيمة من خلال التنصت يحتاج الى جهد كبير من رصيد كافة المكالمات التي تتضاعف أحجامها، إلا أن الحد من قرصنة المعلومات عبر الفضاء أو اعتراضها أو التشويش عليها يظل معضلة أمام كثير من الدول التي لام تحصل بعد على التقنيات المتقدمة في مجال الاتصالات، كما أن الاحتكار والسيطرة على الأقمار الصناعية جعل كافة قنوات الاتصال تحت تصرف الدول العظمى، وتنحصر أساليب الاكتشاف هنا في الحصول على التقنيات العالية والتنسيق والتعاون الدولي والاستفادة من تشفير المعلومات بواسطة المكونات المحلية كاللغات واللهجات الخاصة، كما أنه من الممكن الاستعانة ببيوت الخبرة المتقدمة العاملة في مجال تقديم خدمات عالية في التحقيق واكتشاف جرائم الحاسوب.[1]

[1] محمد الأمين البشيري، المرجع السابق ، ص ص 103، 104.

الـفـصـــل
الـثـا نـي

الفصل الثاني:مواقف التشريعات و الجهود الدولية لمكافحة الجريمة المعلوماتية

إن الأنترنت لا تعرف الحدود، و بالتالي يمكن الدخول إليها من خلال أي جهاز يتم توصيله بها فمستخدم الشبكة يمكنه التنقل بين أنحاء العالم وهو جالس في منزله أمام شاشة الحاسب الألي، و يترتب على هذه الطبيعة العالمية لشبكة الأنترنت أن الجرائم التي ترتكب عليها أو بواسطتها تكون لها صفة الجرائم المعلوماتية ، أو بالأحرى الجرائم العابرة للحدود فقد يساهم أكثر من شخص في الدول المختلفة في إرتكاب جريمة واحدة يقع ضحيتها عدة أفراد يقيمون في بلدان متعددة.

المبحث الأول: موقف التشريعات في مكافحة الجريمة المعلوماتية

نخص هذا المبحث بكل من التشريع الوطني لكافة الدول و مايجب أن تتضمنها من أساليب لمكافحة هذه الجرائم ، و نتعرض للتشريع الأمريكي لكونه يتساير مع أحدث الجرائم والتشريع الفرنسي لكون المشرع الجزائري عادة مايخذ نفس مساره .

المطلب الأول: موقف التشريع الفرنسي

إن حتمية الإقتصاد و الأمن الوطني و كذلك حماية المعطيات الشخصية، دفعت بفرنسا في سنة 1979 إلى إصدار أول تشريع لحماية الحريات و المعطيات، ثم تلاه قانون 1985 الذي ينظم و يحكم الجرائم المعلوماتية.

قام كذلك المشرع الفرنسي بسن تشريع خاص للإجرام المعلوماتي و ذلك في أغسطس 1986، حيث تقدم النائب " جاك جودافران" بإقتراح قانون تم إعتماده من قبل البرلمان الفرنسي و صدر في 05 يناير 1988 برقم 19 تحت عنوان " الجرائم في المواد المعلوماتية"، و تم إدماجه في الفصل الثاني من قانون العقوبات و خصصت له المواد من 02/432 إلى 09/462

الفصل المخصص لهذه الجرائم ألحق بالباب المتعلق بالجنايات و الجنح ضد الأشخاص، أي بعد الفصل الثاني المخصص بالجنايات و الجنح ضد الملكية، و هذا لكونها ركزت على

هدف مقترح وهو حماية النظام المعلوماتي للشخص لكونه يعد من الخصوصيات/، و بهذا هدفت بتجريم ردع الدخول الغير مشروع على البرامج المعلوماتية[1]

ولم يوضع القانون الجنائي الحديث أن يقوم بتغيير روح لقانون 1978 أو أن يقوم بتقليص سلطات اللجنة القومية للمعلومات و الحريات، و قد تضمن التشريع الجنائي الفرنسي الحديث المواد 41-44 من قانون 1978 في الفصل الخاص بحماية الشخصة و تناول الجرائم المتعلقة بالبيانات الإسمية و الأحكام الخاصة بالعقاب في المواد 16/226 إلى 24/226 و المادة 31/226 من قانون العقوبات الحديث مع إجرائه لبعض التعديلات في هذه الجرائم.[2]

و نأخذ أمثلة على ما تناوله المشرع الفرنسي من أنواع الجرائم المعلوماتية:

1. الدخول بطريقة الغش و البقاء على إتصال مع نظام المعالجة للمعلومات أليا:

تنص المادة 01/323 من القانون الفرنسي الصادر في 1994/03/01 على تجريم الدخول بطريق الغش في إتصال مع نظام المعالجة المعلوماتية أليا سواء كان الدخول إلى النظام كله أو جزء منه، و قررت لذلك عقوبة من شهر إلى سنة و غرامة من 2000 إلى 50.000 فرنك فرنسي [3]

2. جريمة إتلاف البرامج و المعلومات المعالجة أليا:

عاقب المشرع الفرنسي في القانون الجديد في المادة 01/323 /03/02 على جريمة إتلاف البرامج و المعلومات أليا و تخريبها أو حذف أو تغيير و قرر عقوبة حبس و غرامة 20.000 فرن فرنسي .

و قرر للمساهم في الجريمة نفس العقوبة المقررة للفاعل الأصلي فيها و هذا في المادة 01/323 و الفقرة 04 .[4]

و يتفرع عن هذه الجريمة الجرائم الأتية:

- جريمة عدم إتخاذ الإحتياطات الكافية لحماية المعطيات الشخصية.

---

(1) أحمد بن محمد اليماني، الحماية الجنائية للبريد الإلكتروني، دراسة تأهيلية مقارنة ، رسالة ماجستير ، تخصص سياسة جنائية، جامعة نايف العربية للعلوم الأمنية، السعودية، 2010.ص.99.

[2] قانون العقوبات الفرنسي

[3] محمد أمين الرومي، المرجع نفسه، ص 105.

[4] محمد أمين الرومي، المرجع نفسه، ص.108.

- جريمة الإعتداء على الحياة الشخصية للأفراد.
- جريمة مسك معلومات شخصية و الإحتفاظ بها خارج المدة القانونية المحددة لها.
- جريمة مسك معلومات شخصية للمبادلة عن نطريق النظم المناسبة إما تسجيلها أو حفضها.[1]

3.خصوصية المعلومات:

يتطلب القانون الفرنسي المسمى بنظم المعالجة الرقمية و الحرية الصادرة في 06 يناير 1978 عند معالجة أي بيانات إسمية شخصية من قبل أشخاص القانون الخاص وجوب إخطار اللجنة القومية للمعلوماتية و الحريات و يتطلب الأمر الحصول على تصريح سابق إذا كان من يقوم بجمع المعلومات من أشخاص القانون العام أو أشخاص القانون اللذين يعملون لمصلحة الدولة[2]

ورغبة اللجنة القومية للمعلوماتية و الحريات في تسير الإجراءات قامت بوضع توجيهات عامة بحيث يكتفي بإخطار مبسط للجنة إذا تعلق الأمر ببيانات لا تتسم بالخطروة، أما إذا تعلق الأمر ببيانات على قدر من الحساسية، فيتعين الحصول على موافقة صريحة من صاحب الشأن.

المطلب الثاني: التشريع الأمريكي

تعتبر الولايات المتحدة الامريكية من اولى الدول التي أحست بالحاجة إلى التشريع مستغل لمواجهة ظاهرة الإجرام المعلوماتي سواء فيما يتعلق بالولايات الاعضاء فيها كما هو الحال في ولاية تكساس ...إلخ،وتعتبر الولايات المتحدة نموذج النظام الانجلوامريكي التي طبقت القواعد الخاصة بالمعلومات في التشريعات الخاصة التي تعاقب على الجرائم المعلوماتية .[3]

---

[1] بورزام أحمد، المرجع نفسه، ص.13.

[2] http://imternet- juridique.net/ chroniques/sitejuridique.html

[3] أحمد خليفة الملط ، الجرائم المعلوماتية،الطبعة الثانية ،دار الفكر الجامعي،مصر، 2006. ص.ص.144.122.

حيث أن أول تشريع في مجال المعلوماتية ظهر سنة 1958 بولاية فلوريدا الأمريكية ثم تلا تشريع فدرالي لسنة 1984 الذي عدل سنة 1986 ثم سنة 1994 ثم 1996 ، و أخيرا في عام 2001.

و يتميز التشريع الأمريكي بما يتميز به نوعين من الجرائم المعلوماتية:

1. جريمة الدخول بدون إذن للنظم المعلوماتية :

تطبق هذه الجريمة على جميع الأشخاص مهما كاونوا ومهما كانت صفتهم ، مجرد دخولهم بلا إذن إلى النظم المعلوماتية تطبق عليهم العقوبة المقدرة لهذه الجرية و التي تختلف بإختلاف القوانين لكل ولاية من الولايات المتحدة.

2. جريمة تجاوز الصلاحية و الدخول في أنظمة معلوماتية :

و يقصد بهذه الجريمة بأن الدخول إلى الأنظمة المعلوماتية يكون مرخص به في مجال و نطاق معين فقط لكن اذا تجاوز مستخدم الحاسب الألي ذلك النطاق و الصلاحية و يدخل إلى مجالات أخرى محمية و سرية يعاقب عليها القانون.[1]

كما أن التشريع الأمريكي، قد أخص هذه الجريمةة بمجموع من القوانين، وهذا بدءا من قانون 1984 الذي أقره الكونجرس بشأن تجريم الإتصال غير المرخص به و الغش و إساءة إستعمال الكمبيوتر، و بعد صدوره جاءت مجموعة من الأحكام لضبط الإستحداثات التي طرحت على هذه الجرائم .[2]

وبعدها طرأت العديد من التطورات في هذا المجال حيث أصدر قانون إساءة غستعمال الكمبيوتر 1994ن ثم أصدر القانون الذي كان يتساير مع التكنولواجيات الحديثة و إرتباطها بالتجارة صدر في 30 يونيو 2000 قانونا إتحاديا" التوقيع الإلكتروني العالمي و التجارة الوطنية " أجاز بموجبه قبول و إستخدام التوقيع و السجلات الإلكترونية في التعاملات التجارية الدولية وبين الولايات ولكن قبل صدور هذا القانون فقد أقر بمساواة المحررات الإلكترونية بالمستندات الكتابية الصادرة في 20 مارس 1997 والتي وضعت لتطبيقها في

---

[1] أحمد بورزام، المرجع نفسه، ص.13.

[2]. رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الأنترنت، (رسالة ماجستير)، قانون عام، جامعة أبي بكر الصديق، تلمسان، 2012.ص.91.

مجال شركات الأجهزة و القانون الإتحادي للغذاء و الدواء و مستحضرات التجميل و قانون الخدمة الصحية.[1]

المطلب الثالث: مكافحة الجريمة المعلوماتية على المستوى الوطني

إن الجريمة المعلوماتية قد تزامنت بإشباع المستخدمين شبكة الإتصالات و المعلومات الدولية المعروفة بـ"شبكة الأنترنت" هذا فضلا عن إتجاه الدول لحفظ معلوماتها أسرارها في أنظمة الحاسب الآلي بجانب الحفظ التقليدي و المعروف باسم " الأرشيف"، ناهيك عن إستخدام البنوك التجارية و الشركات المالية لأجهزة الحاسب الآلي في تقديم خدماتها المصرفية و المالية المتنوعة.

ومن مظاهر مخاطرها عزوف المستثمرين بدء من صناعة البرمجيات و مرورا إلى إنتهاك الملكية الفكرية و صولا إلى غياب الأمن الإلكتروني أحيانا.

لهذا يطالب بضرورة مكافحة الجريمة المعلوماتية من خلال إدراك خصوصية مثل هذه الجرائم التي تختلف عن ما تخلفه الجرائم التقليدية ، حيث أن ما تبينه آخر الإحصاءات و منه في هذا المطلب سنتطرق إلى مكافحة الجريمة على المستوى الوطن

الفرع الأول : التدابير الموضوعية

أولا : الوطنية

1- يجب على كافة الدول أن تبين التدابير التشريعية و غيرها من التدابير االلازمة لإدراك عملية الدخول غير المشروعة إلى سائر جزء من أجزاء نظام الحاسب الآلي كجريمة جنائية وفقا لأحكام قوانينها الوطنية إذا ما ارتكبت هذه الأفعال بصورة عمدية و يجوز لأي دولة أن تحدد من بين متطلبات إرتكاب الجريمة أن يكون إرتكابها من خلال إختراق تدابير الأمن

2- يجب على الدول أن تتبين التدابير التشريعية اللازمة لإدراك أعمال الإضرار أو المحو أو إتلاف أو التعديل أو الإعاقة التي تستهدف بيانات الحاسب الآلي بدون وجه حق واعتبارها جريمة جنائية إذا ما ارتكبت على نحو عمدي

[1] رصاع فتيحة، المرجع نفسه، ص.92.

3- يجب على الدول أن تبين التدابير التشريعية اللازمة الإمكانية مساءلة الأشخاص المعنوية جنائيا عن جرائم ناشئة عن نظم المعلومات.[1]

ثانيا : التشريع الجزائري

_ نتيجة لتأثير الجزائر بما أفرزته ثورة تقنية المعلومات من أشكال جديدة للجرائم طالت مصالح جديدة غير تلك التي يحميها قانون العقوبات، فقد تطرق المشرع الجزائري إلى تحريم أفعال المساس بالأنظمة المعالجة الألية للمعطيات من خلال تعديل قانون العقوبات بموجب قانون رقم15/04 و الذي تظمن ثمانية مواد عمد المشرع من خلالها إلى حماية سرية و سلامة المعلومات و نظم معالجتها و ذلك من المواد 394 مكرر 07 أين جرم الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو في جزء منه المادة 394 مكرر

- الإتجار في معطيات مخزنة و معالجة أو مرسلة عن طريق منظومة معلوماتية.
- حيازة أو إنشاء أو نشر المعطيات المتحصل عليها بإرتكاب إحدى الجرائم المنصوص عليها في هذا المجال.

و الملاحظ أن تخصيص المشرع الجزائري لهذه الجرائم قسما خاصا في قانون العقوبات دلالة على إقراره بأنها ظاهرة مستجدة متميزة عن الجرائم التقليدية الأخرى من حيث المصالح التي تطالها، وكذا من حيث مينها و طبيعتها و محلها و من ثما لا يمكن إدراجها تحت أي عنون من الجرائم التقليدية [2]

- كما أنه لم يميز في وضعه لهذه النصوص القانونية نوعية المعلومات التي تطالها الجريمة فيما إذا كانت معطيات تتصل بمصالح إقتصادية أو مالية أو مسائل أمنية و ذلك سعيا من المشرع الجزائري إلى تعميم الحماية للمعلومات بكافة أنواعها ماعدا تجديد العقوبة إذا كانت المعلومات المستهدفة متعلقة بالدفاع الوطني أو الهيئات و المؤسسات الخاصة للقانون العام.

---

[1] عبدالله حسين علي محمود، سرقة المعلومات السرية في الحاسب الألي،دار النهضة العربية ، مصر، 2000. ص.ص.406.407.

[2] رشيدة بوبكر، **جرائم الإعتداء على نظم المعالجة الألية في التشريع الجزائري و المقارن**، منشورات الحلبي الحقوقية ، 2012، ص.127.

وقبل هذا القانون نجد أن المشرع الجزائري قد حاول مواجهة الجريمة المعلوماتية من خلال قانون الملكية الأدبية و الفنية وهو الأمر 14/73 المؤرخ في 1973/04/03 المعدل والمتمم بمقتضى الأمر 10/97المؤرخ في 1997/03/06والمعدل والمتمم بالأمر 05/03المؤرخ في2003/07/19. والمتعلق بحق المؤلف والحقوق المجاورة، حينما أدمج بموجب هذين الأمرين الأخيرين برامج الإعلام الآلي ضمن المصنفات الأصلية التي تشملها الحماية القانونية وقرر للإعتداء عليها عقوبة الحبس والغرامة.[1]

وتجدر الإشارة إلى أن هذه المستجدات التي اعتمدها المشرع الجزائري من خلال الأمرين10/97و 05/03تعود لأسباب أهمها أنه من شروط الإنضمام إلى المنظمة العالمية للتجارة هو المصادقة على إتفاقية" **بيرن** "وهو ما فعلته الجزائر بموجب المرسوم الرئاسي 341/97 بالإضافة إلى تبني أحكام إتفاق جوانب الملكية الفكرية المتعلق بالتجارة، والذي ورد في نص المادة 10منه أن برامج الإعلام الآلي سواء كانت في صورة برنامج مصدر أو صورة منقوشة فهي محمية على أساس أنها مصنفات أدبية، كما أن الإتفاقية الدولية حول الإجرام المعلوماتي نصت على تجريم الإعتداءات على حق المؤلف والحقوق المجاورة إذا ارتكبت هذه الإعتداءات عن طريق نظام معلوماتي في نطاق تجاري.[2]

الفرع الثاني: التدابير الإجرائية

أولا: الوطنية

1. يجب على الدول أن تتخذ التدابير التشريعية التي تحولها سلطة التفتيش.

- أخذ أنظمة الحاسب الألي أو جزء منه و البيانات المخزنة فيه.
- أخذ الوسائط التي تكون بيانات الحاسب المخزنة به ، و ذلك في أراضيها أو أحد الأماكن الأخرى التي تمارس عليها سلطاتها لأغراض التحقيق

[1] نص المادة 04من الأمر10/97: " تعتبر على الخصوص مؤلفات أدبية أو فنية محمية ما يأتي: المصنفات الأدبية المكتوبة مثل....ومصنفات وقواعد البيانات"

[2] عطا الله فشار. بحث حول مواجهة الجريمة المعلوماتية في التشريع الجزائري كلية الحقوق والعلوم السياسية بجامعة الجلفة. بدون ترقيم

2. يجب على الدول أن تتخذ التدابير التشريعية اللازمة لتحويل سلطاتها المعنية في إصدار أمر لأي شخص سواء كان متواجد في إقليمها أو في أي مكان آخر تمارس عليها سلطتها السيادية لكي يقدم أي بيانات واقعة تحت سيطرته و مخزنة في أحد أنظمة الحاسب أو الوسائط المستخدمة في تخزين البيانات
3. يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإجبار الشخص التي تتخذ حياله إجراءات حفظ البيانات المعروضة للنقد و التعديل على الإحتفاظ بسرية الإجراءات لمدة محددة من الزمان وفقا للإطار الذي يسمح به القانون
4. يجب على الدول أن تتخذ التدابير الإجرائية اللازمة لمدة إختصاصها القضائي على أي من الجرائم المشار إليها إذا ما ارتكبت :

- بصورة كلية أو جزئية على أراضيها أو على متن طائرة أو باخرة أو قمر صناعي عملها و مسجل لديها
- من قبل أحد مواطنيها إذا كان الجريمة من الجرائم المعاقب عليها وفقا لأحكام القانون الجنائي الساري في محل إرتكابه أو إذا كانت الجريمة قد ارتكبت خارج إقليم أي دولة.

ثانيا : في التشريع الجزائري

ان المشرع الجزائري أخذ بثلاث مراحل يجب أن يمر بها في الجانب الإجرائي ن نفصلها على مايلي.

فيما يخص التفتيش فقد تعرض له المشرع الجزائري في المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائري أنه اذا لزم الامر في الوصول لنتائج في التفتيش في الجريمة فيمكن التنصت حيث نصت على :" إذا إقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة الألية للمعطيات أو جرائم تبيض الأموال... يجوز لوكيل الجمهورية المختص أن يأذن بمايلي:

- إعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية و اللاسلكية.

- وضع الترتيبات التقنية، دون الموافقة المعنيين، من أجل إلتقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو إلتقاط صور الأشخاص ..."[1]

و نستنتج من نص المادة أن الإعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الإتصالات السلكية و اللاسلكية و هذه المراسلات عبارة عن بيانات قابلة للإنتاج و التوزيع و التخزين و الإستقبال و العرض.

يكون الحل في بعض أنواع الجرائم الإكترونية ، و لتكون المعاينة لا بد من وجود مسرح الجريمة ، و هذا ما يصعب تحديده و بالتالي صعوبة الحفاظ عل الآثار المادية هذا إن وجدت و قد يكون الفارق الزمني بين حدوث الجريمة و إكتشافها أو التحقيق فيها كبير و من أجل المعاينة لا بد من التبليغ و الشخص المبلغ له يجب أن يكون عالما بالتقنية من أجل التحفظ على الأدلة إن وجدت.

كما يجب العمل على الخبرة، لما أخص عليه المشرع الجزائري لها في المواد من 143 إلى 156 من قانون الإجراءات الجزائية. حيث أورد فيها كل ما يتعلق بشروط كل من الخبرة و الخبير، و جمع البيانات

كما ذكرها المشرع في المادة 05 من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام.

[1] قانون رقم 22/06 المؤرخ في 20 ديسمبر 2006 المعدل و المتمم لقانون الإجراءات الجزئية ، الجريدة الرسمية عدد 84.

المبحث الثاني: مكافحة الجريمة المعلوماتية على الصعيد العربي و الدولي

في عالم مزدحم بشبكات اتصالية دقيقة متطورة تنقل وتشغل المعلومات والبيانات من أماكن متباعدة باستخدام تقنيات لا تكفل لها أمنا كاملا، ويتاح في ظلها التلاعب عبر الحدود بالمعطيات المنقولة أو المخزونة، مما قد يسبب لبعض الدول أو الأفراد أو الشركات أضرار فادحة يغدو عندها التعاون الدولي واسع المدى في مكافحة الجرائم المعلوماتية وخصوصا جرائم الانترنت.

ومع ضرورة هذا التعاون والمناداة به، إلا أنه ثمة صعوبات ومعوقات تقف دون تحقيق ذلك وأصبح صعب المنال تحقيق الغاية المرجوة منها، ومن خلال هذا المبحث سوف نحاول جاهدين إبراز أهم تلك الصعوبات أو المعوقات.

المطلب الأول: مكافحة الجريمة المعلوماتية على الصعيد العربي

إن ثورة المعلومات هي القوة الحالية و القادمة لجميع الدول ، ومع دخول وسائل الإتصال الحديثة مثل الأنترنت لوجدنا الكم الهائل من المعلومات التي لا يستطيع أي إنسان إستيعابها و دراستها بشكل سليم، و لهذا أصبح إنتاج المعلومات و إستغلالها بالشكل الصحيح أحد أهم عوامل نجاح إقتصاد الدول، ولو أدركنا أن الدول تهتم بالمعلومات و البيانات و الإحصائيات الدقيقة التي تستطيع من خلالها تحريك عصا إقتصادها و توفير فرص العمل لشعوبها و جذب رؤوس الأموال من جميع أنحاء العالم نجد منه الجانب الأخر الدول العربية التي لم تستطيع إستيعاب كرة و أهمية المعلومات إلا في الأونة الأخيرة.

في مجال الملكية الفكرية إبرام الإتفاقية العربية لحماية حقوق المؤلف حيث نصت في مجال المعلوماتية ، على توفير الحماية القانونية للبرامج المعلوماتية، بالإضافة إلى حث و تشجيع الدول الأعضاء على ضرورة تطوير تشريعاتها الجزائية لمواجهة الجرائم المرتكبة عبر الأنترنت.[1]

[1] محمود أحمد عبابنة ،المرجع نفسه .ص.181.

القانون العربي الإسترشادي لمكافحة الجريمة المعلوماتية:

إعتمدت جامعة الدول العربية عبر الأمانة العامة مجلس وزراء العدل العرب ما سمي بالقانون العربي الإسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، أين تم اعتماده من قبل مجلس وزراء العدل العرب في دورته التاسعة عشر بالقرار

رقم495(د19-2003/10/08)ويعد هذا القانون أبرز الجهود العربية المبذولة في مجال الحماية من الجرائم المعلوماتية من الناحية التشريعية. وقد تضمن هذا القانون 27مادة موزعة على أربعة أبواب يعالج الباب الأول الجرائم المعلوماتية.

والتي تم النص عليها في المواد من 3إلى 22ومن أهمها:

-جريمة الدخول بغير حق إلى موقع أو نظام معلوماتي، مع تشديد العقوبة إذا كان بغرض إلغاء أو إتلاف أو إعادة نشر بيانات أو معلومات شخصية.

-جريمة تزوير المستندات المعالجة في نظام معلوماتي واستعماله.

-جريمة الإدخال الذي من شأنه إيقاف الشبكة المعلوماتية عن العمل، أوإتلاف البرامج أو البيانات فيها.

-جريمة التنصت دون وجه حق على ما هو مرسل عن طريق الشبكة المعلوماتية.

- الجرائم المخلة بالآداب العامة عبر الشبكة المعلوماتية.

وتناول الباب الثاني التجارة والمعاملات الإكترونية، أما الباب الثالث فقد تناول حماية حقوق المؤلف عبر الوسائط المعلوماتية في حين عالج الباب الرابع الإجراءات المتعلقة بالجريمة المعلوماتية[1].

وإن كان القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها جاء موفقا إلى حد ما في أحكامه الموضوعية حيث شملت بيانا لأهم الجرائم التي يمكن أن ترتكب في مجال الأنظمة المعلوماتية، إلا أنه يؤخذ عليه خلوه من الأحكام الإجرائية

[1] تم إعداد هذا القانون من قبل لجنة مشتركة بين المكتب التنفيذي لمؤتمر وزراء العدل العرب والمكتب التنفيذي لمؤتمر وزراء الداخلية العرب حيث جرى إقراره بوصفه منهجا استرشاديا للمشرع الوطني عند إعداد تشريع يتعلق بالجرائم المعلوماتية.

الضرورية لملاحقة هذه الجرائم، فلم يتعرض لمسألة الإختصاص القضائي بشكل واضح ولم يشر إلى إخضاع البيانات والمعلومات لإجراءات التفتيش والضبط، ولم يتعرض كذلك لمفهوم الدليل التقني وشروطه وحجيته.[1]

اهتمت جل الدول العربية **بالتجارة الالكترونية، والتعاقد والتوقيع الالكتروني** خلال الفترة الممتدة ما بين 2000و ،2009ومن النادر اليوم أن نجد خلو تشريع هذه الدول من قوانين تنظم التجارة الالكترونية والتوقيع الالكتروني .

كل دول المغرب العربي اهتمت بهذا الموضوع ، كما حال الخليج العربي، والدول الأخرى. وهكذا ففي مملكة البحرين صدر قانون التجارة الالكترونية بتاريخ14 سبتمبر ،2002كما صدر في الأردن القانون رقم 85لسنة ، 2001قانون المعاملات الالكتروني. وفي تونس صدر القانون عدد 83لسنة 2000الخاص بالمبادلات الالكترونية والمؤرخ في 9غشت 2000.

ويسرى نفس الشيء على المغرب، والجزائر وتونس وليبيا ولبنان والإمارات العربية المتحدة.فإذا كان استخدام الانترنت في الأغراض التجارية بدأ في الانتشار على الصعيد العالمي منذ ،1992فصار كمروج للسلع والخدمات. وبدأ رجال الأعمال وأصحاب المؤسسات والشركات التجارية في الإقبال على المواقع الخاصة بهذا الغرض، وأصبحوا يبرمون الصفقات عن طريق مراسلاتهم عبر البريد الالكتروني، كما صاروا يعرضون منتجاتهم وخدماتهم من خلال مواقع لهم على شبكة الانترنت.[2]

ورغم صعوبة ضبط وصعوبة مكافحة جرائم الانترنت على الصعيد العربي إلا أن هناك جهود جماعية وفردية في محاربة قراصنة الانترنت وإحالتهم قانونا على المحاكم .ولكن أيضا هذه الجهود فيها ما هو مضاد لحرية التعبير ويمكن أن نذكر من بين الجهود الجماعية العربية، ما حصل من تعاون عربي في هذا الصدد بمناسبة انعقاد "مؤتمر وزراء الداخلية

[1] سعيداني نعيم، أليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، (رسالة ماجستير) ، تخصص علوم جنائية،جامعة الحاج لخضر ، باتنة، 2013، ص.87.

[2] رصاع فتيحة، المرجع نفسه، ص.104.

العرب في تونس سنة 2006".عندما قدم وزير الداخلية المصري اقتراحا بتوحيد الجهود العربية للعمل على استصدار قرار من مجلس الأمن بالتزام
الدول التي تتبعها المؤسسات، والشركات العالمية الكبرى، التي تباشر إدارة واستقبال شبكات المعلومات والاتصال، بإغلاق المواقع التي تبث بيانات للأفكار والأيديولوجيات المتطرفة. قد قوبل هذا المطلب بمواجهة عنيفة من قبل المنظمات الحقوقية التي اعتبرت مثل هذا الإجراء ما هو إلا تقييد لحرية الرأي والتعبير[1].
كما تحركت مصر والسعودية مرة أخرى في مؤتمر وزراء الإعلام العرب 2008 "بتقديم مسودة مشروع مقترح لتشكيل لجنة عليا للإعلام الالكتروني"، وهو خطوة أخرى ظاهرها مكافحة الجرائم المعلوماتية وباطنها هو تقييد حرية الرأي والتعبير، مستندين على أن الإعلام الالكتروني في الدول العربية يتسم بالخطورة ولا تحكمه أية معايير أو ضوابط مهنية واضحة يمكن الالتزام بها .

وعلى العموم يمكن القول إن الدول العربية لم يعمم فيها بعد وبشكل كافي، إصدار قوانين خاصة بجرائم الانترنت، باستثناء بعض النماذج المشار إليها مثل الإمارات العربية المتحدة، وتونس، والسودان ويبدو اليوم أن هناك لدى هذه الدول شعور عميق بتنظيم الجرائم المرتكبة عن طريق الانترنت، وهي تحضر مشاريع قوانين في هذا الاتجاه. ويعود سبب الاهتمام بتنظيم جرائم الانترنت إلى كون القانون الجنائي التقليدي غير قادر على استيعاب الجرائم المعلوماتية الحديثة النشأة والتي ظهرت لأول مرة كمصطلح في استراليا عام. [2]

ولكي يتم التنظيم الجدي لهذه الجرائم على المستوى العربي من الضروري وضع اتفاقية إطارية جماعية تحدد جرائم الانترنت وتكون كتشريع موحد عربي لمواجهتها تهتدي به التشريعات القطرية ولا تخرج عن مضمونه. ولعل هذه المهمة موكولة إلى مؤسسة النظام الإقليمي العربي.

[1] رصاع فتيحة، المرجع نفسه، ص.107.

[2] رصاع فتيحة، المرجع نفسه، ص. 109.

المطلب الثاني : مكافحة الجريمة المعلوماتية على الصعيد الدولي

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

الفرع الأول : المجلس الأوروبي في مكافحة الجريمة المعلوماتية

ونجد فيه قسمين حيث نتعرض لأهم ماأصدره وهي اتفاقية بودابست و القسم الثاني نتعرض فيه لباقي ما أصدره المجلس.

أولا:إتفاقية بودابست

شهدت العاصمة المجرية بودابست في أواخر عام 2001ميلاد أولى المعاهدات الدولية تكافح جرائم الانترنتInternet Crimes" " وتبلور التعاون والتضامن الدولي في محاربتها ومحاولة الحد منها لاسيما بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص والممتلكات.

في إطار التصدي أكثر لمكافحة الجريمة المعلوماتية عقد المجلس الأوروبي في 11ديسمبر 1995مؤتمر وزراء الدول الأعضاء لبحث مشاكل صياغة اتفاقيات لمكافحة الجريمة المعلوماتية بعقد اتفاقية بودابست في 23نوفمبر ،2001ولقد بينت المذكرة التفسيرية لهذه الاتفاقية أن تحديد الجرائم المعلوماتية فيها هدفه تحسين ٍواصلاح وسائل منع وقمع الجريمة المعلوماتية، من خلال تحديد معيار بالحد الأدنى المشترك، الذي يسمح باعتبار بعض التصرفات من قبل الجرائم المعلوماتية، وأنه بالإمكان أن يتم استكمال هذه القائمة في القوانين الداخلية، كما أنه يأخذ في الاعتبار الممارسات غير المشروعة الأكثر حداثة والمرتبطة بالتوسع في استخدام شبكات الاتصال عن بعد.[1]

[1] مزغيش سمية، جرائم المساس بالأنظمة المعلوماتية، (مذكرة ماستر)، تخصص قانون جنائي، جامعة محمد خيضر ،بسكرة،2014.ص.37.

1. الجانب الموضوعي في اتفاقية بودابست

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

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 (م**02**)

-الاعتراض الغير قانوني (م**03**)

-الاعتداء على سلامة البيانات (م**04**)

-الاعتداء على سلامة النظام (م**05**)

-إساءة استخدام أجهزة الحاسب (م **06**)[1]

أما بخصوص الطائفة الثانية فإنها تحتوي على:

الطائفة الثانية :الجرائم المعلوماتية (الجرائم المتصلة بالحاسب.)

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

- التزوير المعلوماتي حسب نص المادة **07**من الاتفاقية.
- الغش المعلوماتي 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

---

[1] هلالي عبد اللاه احمد ، **اتفاقية بودابست لمكافحة الجرائم المعلوماتية** ، دار النهضة العربية ،القاهرة ،2007.ص.47.

تقوم على الانتهاكات الواقعة على الملكية الفكرية هي احد أشكال الإجرام المعلوماتي ،الأكثر شيوعا ، والذي بازدياد نسبته يزداد قلق و انشغال العالم بأسره[1].

ثانيا: الجانب الإجرائي

أ –تنسيق عناصر الجرائم التي لها علاقة بالقانون الجنائي الأساسي الوطني والنصوص ذات الصلة بموضوع جرائم الحاسب الآلي، ثم توفير للقانون الجنائي الإجرائي الوطني السلطات الضرورية في التحقيق و ملاحقة الجرائم المعلوماتية و جرائم أخرى ترتكب بواسطة وسيلة المعلومات أو في إطار يوجد به أدلة إلكترونية.

ب –وضع نظام سريع و فعال للتعاون الدولي :حيث تناولت هذه الاتفاقية في قسمها الثاني وصف بعض الإجراءات التي يجب اتخاذها على الصعيد المحلي و التي تخدم التحريات الجنائية التي تجرى حول الجرائم التي ترتكب عن طريق المنظومة المعلوماتية و جمع الأدلة ذات الطابع الإلكتروني والمرتبطة بالجريمة.

ت -كما تشير الاتفاقية في مجال المكافحة الإجرائية إلى وجوب إقرار الدول الموقعة عليها بأن قانونها الداخلي يتضمن معلومات رقمية أو إلكترونية فتستخدم كأدلة أمام القضاء، و ذلك في إطار الإجراء الجنائي و أيا كانت طبيعة الجريمة الجنائية المطلوب متابعتها.

ث -على الدول الأعضاء أن تقوم بتفعيل بعض الإجراءات النابعة من قانونها الداخلي، أما كيفية تطبيق وسريان هذه الصلاحيات و الإجراءات في إطار نظامها القضائي و تطبيق الصلاحيات و الإجراءات في بعض الحالات الخاصة يجب أن ينبع من التشريعات و الإجراءات الداخلية لكل طرف[2].

نصت هذه الاتفاقية على بعض الإجراءات الجنائية الجديدة لمكافحة الجريمة المعلوماتية وهي:

أ -الحفظ السريع للمعطيات المخزنة :نصت على هذا الإجراء كل من المادتين 16و 17من

---

[1] هلالي عبد اللاه احمد ، **اتفاقية بودابست لمكافحة الجرائم المعلوماتية** ،المرجع السابق، ص.91.

[2] علي حسن محمد الطوالبة، **التفتيش الجنائي على نظم الحاسوب و الأنترنت** .دار الجامعة الجديدة 2008ص.ص.77.78.79.

الاتفاقية و يقصد به الاحتفاظ بالمعلومات السابقة و تخزينها مع حمايتها من كل ما يمكن أن يفسدها أو يتلف نوعيتها.

ب -تجميع المعلومات الخاصة بالمشتركين :نصت اتفاقية بودابست كذلك في إطار التحقيق الجنائي على أهمية المعلومات الخاصة بالمشتركين لتحديد هوية الفاعل في الجريمة المعلوماتية، و هذه المعلومات تشمل تلك المرتبطة بالاستعانة بالخدمة و المدة التي يشترك فيها الشخص في الخدمة كأن تتضمن مثلا حفظ رقم الهاتف أو العنوان الإلكتروني أو عنوان الموقع.....إلخ

ت -التفتيش المعلوماتي :كما نصت الاتفاقية على إجراء التفتيش، أي تفتيش البيانات في المادة 19منها، و قد بينت انه يجب توفر شرط الحصول على إذن رسمي للتفتيش، بعد الاعتقاد بتوفر بيانات في مكان محدد يساعد على إثبات وقوع جريمة معلوماتية محددة بمقتضى القوانين الداخلية، و تفتيش البيانات المعلوماتية و المعطيات يتم تجميعها في الوقت المتاح للتفتيش مع وجوب توفر شرط الحصول على إذن رسمي للتفتيش.[1]

ث -كما تلزم هذه المادة الدول الأطراف تخويل سلطاتها المختصة بمكافحة الجريمة الحق في فحص و الدخول على المعطيات المعلوماتية الموجودة في نظم المعلومات، أو أي جزء منها، و يقصد بنظم المعلومات هنا كل جهاز منفصل أو مجموعة من الأجهزة المتصلة أو المدمجة كالحاسب المحمول أو الطابعة...إلخ، و الاعتراض في الوقت الفعلي لها من أجل إمكان جمع الأدلة الإلكترونية .

ج -اجراء التنصت :كما نصت اتفاقية بودابست على إجراء التنصت، و هو إجراء جديد في إطار المكافحة الإجرائية للجريمة المعلوماتية كما أنه إجراء خاص قد يمس بحقوق الأفراد الخاصة، لذلك لا يجوز اعتباره إجراء قانوني إلا إذا اتخذ بموافقة السلطات القضائية، و مفاد هذا الإجراء هو اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية، كالخطوط الهاتفية مثلا، ووضع الترتيبات التقنية بدون موافقة المعنيين من أجل

[1] طرشي نورة، مكافحة الجريمة المعلوماتية، (رسالة ماجستير)، قانون الجنائي،جامعة الجزائر1، الجزائر ، 2012،ص.ص.95.96.

التقاط و تثبيت و بث و تسجيل الكلام المتفوه به من طرف شخص أو أشخاص و في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في أمكنة خاصة، و ذلك من أجل التحري و الوصول إلى أدلة تثبت قيام جريمة معلوماتية.

ح -التعاون الدولي :و لتفعيل الإجراءات السابقة نصّت الاتفاقية في المادة 23على ضرورة تعاون الدول فيما بينها، في أوسع نطاق ممكن، مع تقليل الصعوبات التي قد تواجه تبادل المعلومات و الأدلة حتى تتم بصورة سريعة على المستوى الدولي، كما وضحت المفهوم العام لالتزام التعاون الدولي في مجال الجرائم المعلوماتية المتعلقة بنظم المعلوماتية، كما تناولت الأحكام الخاصة بتسليم المجرمين وشروط التسليم الذي يطبق في حالة الجرائم المنصوص عليها في المواد 2إلى 11منها و التي يعاقب عليها قانون الدولتين المعنيتين بالتسليم بالسجن لمدة قصوى لا تقل عن سنة أو بعقوبة أكثر صرامة في المادة 24منها.[1]

ثانيا:باقي إصدارات المجلس الأوروبي

ومن الأمثلة الجيدة ماجاء في احترام الحقوق الأساسية نظام شنجين للمعلومات ويتكون نظام معلومات شنجيSIS من قسم مركزي مقره مدينة ستراسبورج وأقسام وطنية في كل دولة من دول المنظمة، كذلك به بنك معلومات كبير تسجل فيه المعلومات التي ترسلها إليه قوات الشرطة والسلطات القضائية في كل دولة، من بين هذه المعلومات عناوين الأفراد سواء أولئك المطلوب تسليمهم من قبل دول أخرى، أو الممنوعين من دخول أراضي دولة ما، أو المعلَن اختفاؤهم أو المطلوب تقديمهم للعدالة بأمر قضائي لأي سبب كان. ولا يتم الرجوع إلى نظام المعلوماتSIS إلا في حالة القيام بإجراءات المراقبة على الحدود. من طرف الشرطة والجمارك وكذلك تسليم تأشيرات الدخول وكذا الإقامات 124وفي أثناء وضع هذا النظام، لم تغب عن نظر المشرع الأوروبي إمكانية وقوع انتهاكات في هذا الصدد، فقام بإضافة شرط إلى الاتفاقية يُلزم كل دولة انضمت إلى الاتفاقية أن تضمن في قانونها الوطني حماية البيانات ذات الطابع الشخصي125. تم فرض حد أدنى من الحماية من خلال اتفاقية المجلس الأوروبي بتاريخ 28يناير/كانون الثاني 1981من أجل حماية الأفراد فيما يتعلق

[1] طرشي نورة، المرجع السابق ، ص.ص.98.99.

بالمعالجة الآلية للبيانات ذات الطابع الشخصي[1].

والأفضل من ذلك أنه تم تكليف سلطة رقابة مشتركة بمهمة دعم العمل الآلي لنظام المعلومات شنجين. وتتم عملية الرقابة طبقا للإجراءات التي حددتها هذه الاتفاقية، واتفاقية مجلس أوروبا بتاريخ 28يناير 1981لتوفير حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات ذات الطابع الشخصي وجاءت مقسمة الى سبعة فصول تضمنت التوصيات العامة ، الاسس المبدئية لحماية المعلومة ، انتقال المعلومة خارج حدود البلد ، التعاون المتبادل بين الدول ، اللجنة الاستشارية ، التعديلات الجائز اقتراحها من الاعضاء ، البنود الختامية ، فالمادة الاولى منها عرفت الهدف من الاتفاقية وهو حماية الافراد وحماية حياتهم الخاصة فيما يتعلق بالمعالجة الالية للمعلومات بغض النظر عن اصولهم او جنسياتهم ، اما المادة الثانية فقد اوضحت معاني المصطلحات المستعملة في الاتفاقية مثل المعلومة الشخصية بأنها تلك المعلومة المتعلقة بفرد بعينه _محدد _ ويقصد بملفات المعلومات اي مجموعة من المعلومات تعالج الياً بالحاسوب ، ويقصد بالمعالجة الالية تخزين المعلومة في الحاسوب ونقل وتبادل البرامج او تغيير المعلومة او مسحها ، او توزيعها كذلك ، قامت هذه الاتفاقية بتحديد من يطلق عليهم مراقب الملفات او المسؤول عنها بكونه كل شخص طبيعي اوقانوني او سلطة عامة او وكالة او اية جهة مصرح لها وفقاً لقانون البلد بتحديد الهدف من جمع المعلومات وكيفية او هدف معالجتها مع الأخذ بعين الاعتبار التوصية رق R15 87الصادرة عن لجنة وزراء مجلس أوروبا بتاريخ 17سبتمبر/أيلول 1987بهدف تقنين عملية استخدام البيانات ذات الطابع الشخصي من قبل قوات الشرطة وطبقا للقانون الوطني للجهة المتعاقدة والمسؤولة عن وظيفة الدعم الآلي. وتتمتع سلطة الرقابة المشتركة أيضا بصلاحية تحليل وتفسير الصعوبات التي يمكن أن تطرأ خلال عملية استخدام نظام معلومات شنجين من أجل دراسة الصعوبات التي يمكن أن تحدث خلال مزاولة سلطات الرقابة الوطنية

[1] جان فرنسوا هنروت ، **أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي** ،ندوة إقليمية الجرائم المتصلة بالكمبيوتر،المغرب ، 2007.ص.109.

للجهات المتعاقدة نشاط الرقابة المستقلة، أو خلال ممارسة حق الدخول على هذا النظام، ولوضع اقتراحات ملائمة بهدف إيجاد حلول مشتركة للمشاكل الموجودة.[1]

ومن إصدارته أيضا التوصية المرقمة (46/95) المتعلقة بحماية الافراد فيما يخص المعلومات المتعلقة بهم وعملية تناقلها والصادرة في 1995/10/24 وتتكون هذه التوصية من 34مادة يسبقها مقدمة من 76مادة تحظى بأهمية خاصة كونها دليل لفهم مضمون التوصيات ، واهم ما تضمنته هذه التوصية الترخيص بالتنقل الحر دون ادنى قيود للمعلومات الفردية عبر الملفات التقليدية ما كان منها مكتوباً او مخزناً في ذاكرة الحاسب الالي والمتنقل عبر شبكات المعلوماتية للدول المؤلف منها السوق الاوربية المشتركة ذلك ان هذه المعلومات اصبحت ذات قيمة اقتصادية تستوجب حمايتها اضافة لقيمتها الانسانية، وهذا استتبع توحيد النظم القانونية المكرسة لحماية الافراد في الدول الاعضاء في السوق الاوربية وذلك من اجل تأمين الحد الادنى من الحماية لتلك المعلومات عند انتقالها عبر الحدود ، وبموجب هذه التوصية يحق لاي فرد اوربي ان يلزم القضاء المحلي في اي من دول السوق الاوربية بأحترام هذه التوصية واخذاً بالاولوية من حيث التطبيق على القانون المحلي خصوصاً ما تعلق منها بالجانب الجزائي.[2]

إتفاقية الجرائم المعلوماتية للمجلس الأوروبي من أحدث الاتفاقيات لمكافحة الجريمة المعلوماتية على المستوى الدولي، و قد صدرت عن المجلس الأوروبي بعد أن وقعت عليها اثنان و ثلاثون دولة و دخلت حيز التطبيق في أول جويلية 2004 .
ونصت هذه الاتفاقية على مجموعة من الجرائم التي تمس النظام المعلوماتي، و بينت الأساليب التحقيقية فيها، و هذه الجرائم هي الجرائم المرتكبة ضد سرية و تكامل و توافر البيانات أو نظم الحاسبات كجرائم التدخل و الاختراق على أجهزة الحاسبات الآلية، ثم الجرائم المتصلة بالمحتوى و التي يقصد بها الجرائم الخاصة بالإنتاج أو النشر غير

[1] جان فرنسوا هنروت،المرجع السابق،ص.109.

[2] htpp// www.Stanford.edu.html.p.52_39

مشروع للمواد الإباحية الطفولية عبر النظم المعلوماتية، ثم الجرائم التي تتضمن انتهاكا لحقوق الملكية الفكرية و ما يتصل منها من حقوق[1]

الأساليب الإجرائية التي نصت عليها هذه الاتفاقية لدينا :

أ -إرساء كل من إجراء تفتيش و ضبط أنظمة الحاسبات الآلية

ب -إجراء الحفظ السريع لبيانات، الحاسب المخزونة التي تم جمعها و حفظها فعليا بمعرفة حائز البيانات و هذا الإجراء هو إجراء تحقيقي جديد و هام، خاصة فيما يتعلق بالجرائم التي ترتكب على شبكة الانترنت.

ت -إجراء الأمر بإصدار نسخة من البيانات، و هذا الإجراء يمكن السلطات المختصة من إجبار الشخص على تقديم بيانات الحاسب المخزونة أو المحددة أو أحد عناوين Internet" service provider" ISPالمعنية، و قد أعطت الاتفاقية (اتفاقية المجلس الأوروبي)اهتماما خاصا لإجراء التفتيش و الضبط في البيئة المعلوماتية ،اعتمدت أيضا على إجراء الجمع الفوري لبيانات الحاسب و الذي يعتمد على الجمع الفوري لبيانات النقل و الذي يخص أحد البيانات المتعلقة بأحد الاتصالات التي تتم بواسطة نظام الحاسب الآلي.

ث -كما نصت هذه الاتفاقية على إجراء اعتراض بيانات المحتوى و التي تعني اعتراض محتوى الاتصال سواء كان رسالة أو معلومة منقولة، و لزيادة فاعليتها على المستوى الدولي تبنت هذه الاتفاقية الخطوات المتبعة لمكافحة الجريمة المعلوماتية في كل من اجتماع (إبيك في بن كوك سنة 2002لمكافحة الجريمة المعلوماتية، و توصيات اجتماع منظمة الدول الأمريكية بنيويورك سنة2004 و مؤتمر الجريمة المعلوماتية في ستراسبورغ في سبتمبر ،2004و قمة رؤساء الدول و الحكومات المنعقد بوارسو في ماي 2005.[2]

الفرع الثاني: منظمة الأمم المتحدة في مكافحة الجريمة المعلوماتية

بدأ اهتمام الولايات المتحدة الأمريكية المتحدة بمكافحة الجريمة المعلوماتية في 1966في أول قضية HANCOCKE USTATEتعرض لموضوع إساءة استخدام الحاسبات الآلية

[1] طرشي نورة، المرجع نفسه ، ص.ص.101.102.

[2] طرشي نورة، المرجع نفسه ، ص.103.

وتتلخص وقائع هذه القضية في اتفاق مبرمج لحاسبات آلية بإحدى الشركات بالاتفاق مع صديق له يعمل بشركة أخرى على أن يقوم الأول بطبع المعلومات التي يحتوي عليها 59 برنامجا ملكا للشركة التي يعمل بها والتي هي ذات أهمية كبيرة وتسليمها للشركة الأخرى مقابل تلقيه 5ملايين دولار وأثناء التسليم، تم القبض على المتهم وقدم للمحاكمة بتهمة السرقة.[1]

تسعى الأمم المتحدة من خلال هيئتها والوكالات التابعة لها لوضع الإطار التشريعي لهذه الظاهرة الإجرامية المستحدثة وكانت الانطلاقة في المؤتمر السابع المنعقد بميلانو 1985والذي أكدت على الاستفادة من التطورات العلمية والتكنولوجية في مواجهة هذه الظاهرة، وقد أشارت إلى مسألة الخصوصية واختراقها بالاطلاع على البيانات الشخصية المخزنة داخل نظام الحاسب الآلي وضرورة اعتماد ضمانات لحماية سريتها.

ففيما يخص مؤتمرات الأمم المتحدة في هذا المجال نجد المؤتمر السابع المنعقد بميلانو عام 1985الذي كلف لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعالجة الآلية والإعتداء على الحاسب الآلي وإعداد تقرير يعرضه على المؤتمر الثامن، وقد عقد هذا الأخير في هافانا عام 1990وقد خرج العديد من التوصيات أهمها التأكيد على ضرورة الإستفادة من التطورات العلمية والتكنولوجية في مواجهة الجريمة المعلوماتية، وأشار إلى مسالة الخصوصية واختراقها بالإطلاع على البيانات الشخصية المخزنة داخل النظام المعلوماتي، كما أكد على ضرورة تحديث القوانين التي تتناول هذه الجرائم وتحسين تدابير الأمن والوقاية المتعلقة بها، وتدريب القضاة والمسؤولين على كيفية التحقيق والمحاكمة فيها، وكذا التعاون مع المنظمات المهتمة بهذا الموضوع[2].

من المهم التوقف أمام إعلان مؤتمر الأمم المتحدة العاشر الذي صدر في فيينا عام 2000، وورقة الخلفية الخاصة بورشة العمل التي عقدت للتحضير للمؤتمر. وقد أسفرت الورشة المذكورة بشكل واضح عن تقدم كبير في مواجهة الجرائم المتعلقة بالكمبيوتر بطرق

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية و تطبيقية، دار النهضة العربية، .2004.ص.147.

[2] محمود أحمد عبانة ، المرجع نفسه،ص.159.

غير عادية، بحيث يحتم التتابع المنطقي وطبيعة المسائل المطروحة أن تتخذ أعمال الورشة المقبلة خطوة أو خطوات إلى الأمام، ومن ثم، ينبغي أن ينصب تركيزنا على وضع تصورات ومقاييس تتيح فرصة جديدة للمجتمع الدولي[1]

قدمت الأمم المتحدة اجتماعات إقليمية عدة، ومن خلال استعراض ما انتهت إليه تلك الاجتماعات يمكننا معرفة التوجه الدولي حيال هذا الموضوع المهم.

وفيما يتعلق بالاجتماع التحضيري لغرب أسيا المنعقد في بيروت، في أبريل ،2004عرضت مصر مبادرة رائعة من ثمان نقاط حول الإجراءات الخاصة بالعمل الدولي فيما يتعلق بجرائم الإنترنت وركزت توصيات التقرير الختامي على تعزيز التعاون وتبادل الخبرات بين الحكومات والقطاع الخاص لإنشاء آلية لمكافحة الجرائم المتعلقة بالكمبيوتر وتنفيذها. وأكدت التوصيات أيضا على البحث عن وسائل لتعزيز قدرة الحكومات على تحديث واستخدام أساليب كافية للتحقيق والملاحقة.

وفيما يتعلق بالمؤتمر التحضيري الأفريقي الذي عقد في أديس أبابا في مارس ،200453لم يذكر التقرير الختامي أية إشارات مهمة فيما يتعلق بالجرائم المتعلقة بالكمبيوتر، واكتفى باستعراض عناوين ورش العمل التي سيتم عقدها بما فيها ورشة العمل الخاصة بالجرائم المتعلقة بالكمبيوتر.

أما بالنسبة للاجتماع التحضيري الخاص بمنطقة آسيا والمحيط الهادي الذي عقد في بانكوك في مارس ،2004 تضمن التقرير الختامي إشارات ايجابية تشبه إلى حد ما تلك التي صدرت في اجتماع غرب آسيا[2]

الفرع الثالث: الصعوبات التي تواجه التعاون الدولي وكيفية القضاء عليها

في عالم مزدحم بشبكات اتصالية دقيقة متطورة تنقل وتشغل المعلومات والبيانات من أماكن متباعدة باستخدام تقنيات لا تكفل لها أمنا كاملا، ويتاح في ظلها التلاعب عبر

---

[1] إيهاب ماهر السنباطي، **الجرائم الإلكترونية (الجرائم السيبيرية) قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد** ، ندوة إقليمية الجرائم المتصلة بالكمبيوتر،المغرب ، 2007.ص.28.

[2] إيهاب ماهر السنباطي،المرجع السابق، ص.29.

الحدود بالمعطيات المنقولة أو المخزونة، مما قد يسبب لبعض الدول أو الأفراد أو الشركات أضرار فادحة يغدو عندها التعاون الدولي واسع المدى في مكافحة الجرائم المعلوماتية وخصوصا جرائم الانترنت.

ومع ضرورة هذا التعاون والمناداة به، إلا أته ثمة صعوبات ومعوقات تقف دون تحقيق ذلك وأصبح صعب المنال تحقيق الغاية المرجوة منها، ومن خلال هذا الفرع سوف نحاول جاهدين إبراز أهم تلك الصعوبات أو المعوقات في مطلب أو

أولا: الصعوبات التي تواجه التعاون الدولي

التعاون الدولي بكافة صوره في مجال مكافحة ومواجهة الجرائم المتعلقة بشبكة الانترنت كان يعد مطلبا تسعى إلى تحقيقه أغلب الدول إن لم يكن كلها، إلا أنه ثمة صعوبات ومعوقات تقف دون تحقيقه أهمها:

1. عدم وجود نموذج للنشاط الإجرامي:

بنظرة متأنية للأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم المعلوماتية، يتضح لنا من خلالها عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الانترنت الواجب تجريمها[1].

2. تنوع واختلاف النظم القانونية الإجرامية:

بسبب تنوع واختلاف النظم القانونية الإجرائية نجد أن طرق التحري والتحقيق والتفتيش التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى أو قد لا تقوم بإجرائها[2].

وكما هو الحال بالنسبة للمراقبة الالكترونية والتسليم المراقب وغيرها من الإجراءات الشبيهة فإذا ما اعتبرت طريقة ما من طرق جمع الأدلة أو التحقيق أنها قانونية في دولة

([1]) محمد الأمين البشيري، المرجع نفسه، ص 217.

([2])عبد الله حسين علي محمود، المرجع نفسه، ص 408.

معينة، فقد تكون ذات الطريقة غير المشروعة في دولة أخرى، وبالتالي فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنفاذ القانون في الدولة الأخرى على استخدام ما تعتبره هي أنه أداة فعالة.

3. عدم وجود قنوات اتصال:

أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة والمجرمين الحصول على المعلومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لزاما أن يكون هناك نظام يسمح للجهات القائمة على التحقيق بالاتصال بالجهات الأجنبية لجمع أدلة معينة أو معلومة معينة، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العملية التي تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين، وبالتالي تنعدم الفائدة من التعاون[1].

4. التجريم المزدوج:

التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين، فهو منصوص عليه في أغلب التشريعات الوطنية والدولية المعنية بتسليم المجرمين، بالرغم من أهميته نجده عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية وإن معظم الدول لا تجرم هذه الجرائم، الأمر الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم المتعلقة بالانترنت.

5. الصعوبات الخاصة بالمساعدات القضائية الدولية:

نعلم أن الأصل بالنسبة لطلبات الإنابة القضائية الدولية والتي تعد من أهم صور المساعدة القضائية الدولية في المجال الجنائي أن تسلم بالطرق الدبلوماسية وهذا بالطبع يجعلها تتصف بالبطء والتعقيد، والذي يتعارض مع طبيعة الانترنت وما تتميز به من سرعة وهو الأمر الذي انعكس على الجرائم المتعلقة بالانترنت. كذلك الصعوبات الكبيرة في مجال

([1]) جميل زكريا محمود، ورقة عمل مقدمة للمؤتمر الولي لأمن المعلوماتية الإلكترونية، ص 17.

المساعدات القضائية الدولية المتبادلة التباطؤ من حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد على الطلب بسبب الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد معها وغيرها من الأسباب[1].

ثانيا: كيفية القضاء على الصعوبات التي تواجه التعاون الدولي[2]

فيما يتعلق بالصعوبة الأولى المتمثلة في عدم وجود نموذج موحد للنشاط الإجرامي فإن الأمر يقتضي توحيد هذه النظم القانونية، ولاستحالة هذا الأمر فإنه لا مناص من البحث عن حلول أخرى تساعد على إيجاد تعاون دولي يتفق مع طبيعة هذا النوع المستحدث من الجرائم لما فيها من الفوارق بين الأنظمة العقابية الداخلية وتتمثل هذه الوسيلة في تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية، وإبرام اتفاقيات خاصة يراعى فيها هذا النوع من الجرائم.

وبالنسبة للمعوقة الثانية والخاصة بتنوع واختلاف النظم القانونية الإجرائية، نجد أن الاتفاقية الدولية الصادرة من الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام تقنيات التحقيق الخاصة الشيء الذي يخفف من اختلاف النظم القانونية الإجرائية ويفتح المجال أمام تعاون دولي فعال، فمثلا المادة عشرون اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطن تشير في هذا الصدد إلى التسليم المراقب، والمراقبة الالكترونية التي تعتبر من أشكال المراقبة والعمليات المستترة والتي تعتبر من أهم التقنيات المستخدمة في التصدي للجماعات الإجرامية المنظمة بسبب الأخطار والصعوبات الكامنة وراء الوصول إلى عملياتها وتجميع المعلومات وأدلة الإثبات لاستخدامها فيما بعد في الملاحقة القضائية المحلية منها أو الدولية في دول أطراف في سياق نظم المساعدة القانونية وهذا ما أكدت عليه الاتفاقية الأوروبية للإجرام المعلوماتي حيث نصت المادة 29 أن الطرف المساند إذا اكتشف وجود مؤدي في بلد آخر قد شارك في نقل هذا الاتصال فإن عليه أن يكشف على وجه السرعة إلى الطرف الآخر تقديم المساعدة كمية كافية من البيانات المتعلقة بالتجارة

([1]) محمد الأمين البشيري، المرجع نفسه ، ص 219.

([2]) جميل زكريا محمود، المرجع نفسه ، ص 19.

غير المشروعة حتى يمكن تحديد هوية مؤدي الخدمة هذا والطريق الذي تم الاتصال من خلاله.

كما أشارت المادة 31 من هذه الاتفاقية إلى المساعدة المتعلقة بالدخول إلى البيانات المخزنة حيث أجازت لأي طرف أن يطلب من طرف آخر أن يقوم بالتفتيش أو أن يدخل بأي مشابهة وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة المعلومات داخل النطاق المكاني لذلك الطرف والتي يدخل فيها أيضا البيانات المحفوظة ويجب الاستجابة لمثل هذا الطلب بأسرع ما يمكن في الحالات الآتية:

- إذا كانت هناك أسباب تدعو للاعتقاد أن البيانات المعنية عرضة على وجه الخصوص لمخاطر قابلة للتعديل.
- أو أن الوسائل والاتفاقيات والتشريعات الواردة في الفترة الثانية من المادة 31 تستلزم التعاون بين الطرفية في حين نجد أن المادة 32 من ذات الاتفاقية سمحت بالدخول للبيانات المخزنة خارج الحدود بشرط أن يكون ذلك بموجب اتفاق، أو أن تكون هذه البيانات متاحة للجمهور.
- أيضا نصت المادة 33 على تعاون الدول الأطراف فيما بينها لجمع البيانات في الوقت الحاضر عن التجارة غير المشروعة والمرتبطة باتصالات خاصة على أرضها تتم بواسطة شبكة المعلومات وفي إطار ما هو منصوص عليه في الفقرة الثانية.

وينظم هذا التعاون الخطوات والإجراءات المنصوص عليها في القانون الداخلي ويمنح كل طرف تلك المساعدة على حل هذه المشكلة.

ونلاحظ مما سبق أن الاتفاقية الأوروبية للإجرام المعلوماتي أوجدت بعض الحلول التي تمكن من التغلب على مشكلة اختلاف النظم الإجرائية أمام التعاون الدولي لمواجهة الجرائم المتعلقة بالانترنت[1].

([1])محمد الأمين البشيري، المرجع نفسه، ص. 219.

وللحد من ظاهرة عدم وجود قنوات اتصال بين جهات إنفاذ القانون فنلاحظ أنه غالبا ما تشجع القوانين الدولية إلى التعاون فيما بينها وتدعو إلى إنشاء قنوات اتصال للجهات المختصة ووكلائها ودوائرها المتخصصة بغية التسيير في الحصول على هذه المعلومات ومن الأمثلة على هذه القوانين الدولية اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطن في المادة 27 منها والمادة 9 من اتفاقية 1998 والمادة 48 من اتفاقية الأمم المتحدة لمكافحة الفساد والبند الثاني من المادة 27 من ذات الاتفاقية الأوروبية بشأن الإجرام المعلوماتي والمادة 35 من ذات الاتفاقية الأوروبية التي أوجبت على الدول الأطراف فيها ضرورة وجود قناة اتصال تعمل لمدة 24 ساعة يوميا طوال أيام الأسبوع لكي تؤمن المساعدة المباشرة المتعلقة بجرائم البيانات والشبكات، أو استقبال الأدلة ذات الشكل الالكتروني كما أوجبت ذات المادة على الدول الأطراف ضرورة أن تتمكن نقطة الاتصال من الاتصال بنقطة اتصال الطرف الأخر وأن يعمل كل طرف على أن يتوافر لديه الأفراد لتسهيل عمل الشبكة[1].

([1]) جميل زكريا محمود، المرجع نفسه، ص .20.

خـاتمـة

خـاتـمـة :

ان خاتمة البحث تقدير لأهم النتائج التي توصلنا إليها على ضوء هذه الدراسة و إبراز كذلك التوصيات التي يرمي إليها ، لأنه قد بات من المحتم على شعوب العالم الانهيار التدريجي في بوتقة المعلوماتية كنتيجة حتمية لمواكبة التطور التقني و التكنولوجي في ظل التحول الالكتروني لمختلف نواحي الحياة لتحقيق المجتمع الافتراضي في عالم مفتوح تتسيده المعلومات و التي أضحت و بحق مصدر القوة و التسلط و المعرفة ، و أضحت المعيار المحدد لتطور ونمو الشعوب و مستقبلها و ذلك بزيادتها للفوارق الاقتصادية و الاجتماعية القائمة بين مجتمع و أخر .

لذلك كله وجب علينا ان نسلم بما صاحب الثورة المعلوماتية من تحطيم للحدود الجغرافية والسياسية بميلاد و نمو شبكة الانترنت ، فغدا العالم قرية كونية صغيرة تتلاطم فيها القوانين وتحكمه المبادئ الذاتية و الحقوق الدستورية ، حتى ظهرت مبادئ عدة مسشتحدثة يتربع على عرشها مبدا الحق في المعلومات، لذا ينبغي العمل على تحقيق التوازن ما بين الاستخدام الحر و الكامل للمعلوماتية من ناحية ، و من حماية الوطن و حرياته من ناحية اخرى ، و هو ما يمكن تصوره في اطار دولة واحدة تتولى في نفسها عمل الانترنت بالكامل ، و منه نستخلص ان شبكة الانترنت كاداة ارتكاب جريمة اما ان تكون اداة ايجابية او اداة سلبية للمجرم الالكتروني ، اي ان تكون وسيلة لارتكاب جريمة او محلا لها فهي تسهل للمجرم المعلوماتي ارتكاب جرائم اخرى و تشكل اغلب جرائم الاعتداء على الاشخاص بدء من جرائم الاعتداء على حق الانسان في شرفه و سمعته و اعتباره و حقه في حرمة الحياة الخاصة ، و مرورا بالاعتداء على سلامة الجسم و ايذائه و انتهاء بالاعتداء على حق الانسان في حياته.

و نستنتج ايضا ما تثيره الاساليب الاجرامية المستحدثة من صعوبات قانونية شتى في تطبيق النصوص الجنائية التقليدية و غيرها من مواضيع القانون الأخرى اذ ان هناك اركان في الجريمة التقليدية لا تثير صعوبة ، فسواء ارتكبت الجريمة عن بعد عبر الانترنت او ارتكبت

بغير ذلك كتحقق بعض عناصر الركن المادي او القصد الجنائي او غير ذلك ، و هناك اركان اخرى تثير صعوبة في تكليفها ، كطبيعة المال المعلوماتي و ملكيتها و كذلك قصور قواعد الاجراءات الجنائية في مواجهة

جرائم الحاسب الالي كفشلها في مجال التحقيقات الخاصة بالجريمة المعلوماتية او في فرض ضمانات قانونية للمتهم المعلوماتي تثير صعوبات جمة في التعاون الدولي للقضاء على هذه الجريمة و مواجهة العقبات التي تحول دون تحقيق هذا التعاون بالاضافة الى الصعوبات الكثيرة في اقامة المسؤولية الجنائية و مستخدمي الشبكة كاشخاص طبيعين ،

او المسؤولية الجنائية للاشخاص الاعتبارية كالمؤسسات العامة على التقديم و التزويد خدمة الاتصال و الربط

و في ضوء النتائج السابقة خلصت بعض التوصيات و التي امل ان نجد لها صدى في اثراء الفكر الجنائي المعلوماتي ، و حقول البحث العلمي و هي تتمثل في :

- ضرورة تحديث نصوص القانون العقوبات لمواجهة ظاهرة الاجرام المعلوماتي بحيث تعرف الجريمة المعلوماتية على نحو واسع ، و تفرض العقوبة المناسبة لها.
- ايضا يلاحظ وجود صعوبات تكتنف دليل الجنائي بالنسبة للجريمة المعلوماتية سواء من حيث الحصول عليه او من حيث طبيعته فالحصول عليه قد يحتاج الى عمليات فنية وحسابية معقدة اضافة الى طبيعته الخاصة .
- اتخاذ التدابير اللازمة لحل المشكلات الاختصاص القانوني التي تثيرها جرائم الانترنت العابرة للحدود في اطار تنسيق دولي متكامل فيما يتعلق بمكافحة الجريمة.
- ضرورة تكاثف الجهود الدولية و توافق السياسات الجنائية في مواجهة هذه الظاهرة الاجرامية .
- ضرورة تدريب و تاهيل افراد العدالة الجنائية من العاملين في الادعاء العام و القضاء على كيفية تعامل مع هذا النوع من الجرائم .

خـاتـمـة

- على المشرع الجزائري استحداث قانون خاص يحكم هذه الظاهرة بدلا الاكتفاء بقانون من بضعة مواد فقط لا تصل الى تجريم نوع واحد فقط من كل الجرائم التي تناولناها .
- اتخاذ قانون دولي موحد .

قائمة المصادر

والمراجع

قائمة المصادر و المراجع:

- **القوانين** :
- قانون رقم 22/06 المؤرخ في 20 ديسمير 2006 المعدل و المتمم لقانون الإجراءات الجزئية ، الجريدة الرسمية عدد 84.
- القانون رقم 09 – 04 المؤرخ في 5 ماي 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، جريدة رسميه، عدد47 لسنة 2009.
- قانون رقم 15-19المعدل و المتمم للأمر رقم 66-156الصادر في 08جوان1966 المتضمن لقانون العقوبات الصادر في الجريدة الرسمية ، رقم 71 المؤرخة في 30 ديسمبر 2015.
- قانون العقوبات الفرنسي
- إتفاقية بودابست
- اتفاقية مكافحة استعمال تكنموجيا المعمومات لأغراض إجرامية،رقم،63/55 الصادرة عن هيئة الأمم المتحدة، الجلسة العامة ،81ديسمبر .2000.

2-مؤتمر هيئة الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المعمومية عبر الوطنية، المنعقد بفيينا في 18 – 22أكتوبر.

- أمر رقم 09-04المؤرخ في / 2009 2/5المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47لسنة2009.
- معاهدة بودابست بشأن الاعتراف الدولي بإيداع الكائنات الدقيقة لأغراض الإجراءات الخاصة بالبراءات الموقعة ببودابست في 28 أبريل 1977 و المعدلة في 26 سبتمبر 1980 من طرف المنظمة العالمية للملكية الفكرية.

- **المراجع بالعربية:**

- أحمد خليفة الملط ، الجرائم المعلوماتية،الطبعة الثانية ،دار الفكر الجامعي،مصر، 2006.
- رشيدة بوبكر، **جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن**، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت ، 2012
- السنباطي عبد العاطي، **موقف الشريعة الإسلامية من جرائم الحاسب الألي و الأنترنت** ، دار النهضة العربية، 2002.
- عبد الفتاح بيومي حجازي، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت**،: دار الكتب الوطنية، مصر 2005،
- عبدالله حسين علي محمود، سرقة المعلومات السرية في الحاسب الألي،دار النهضة العربية ، مصر، 2000
- علي حسن محمد الطوالبة، **التفتيش الجنائي على نظم الحاسوب و الأنترنت** .دار الجامعة الجديدة 2008.
- قورة نائلة، **جرائم الحاسب الاقتصادية**، القاهرة: دار النهضة العربية،2004.
- محمد أمين أحمد الشوابكة، **جرائم الحاسوب والإنترنت – الجريمة المعلوماتية** –، دار الثقافة، عمان، الأردن، 2004،
- محمد أمين الرومي، **جرائم الكمبيوتر والإنترنت**، الإسكندرية: دار المطبوعات الجامعية، 2003
- محمد سامي الشوا، **ثورة المعلومات وانعكاساتها على قانون العقوبات**،: دار النهضة العربية، القاهرة 1994.
- محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر و الأنترنت (الجريمة المعلوماتية)، دار الثقافة، الأردن 2004

- محمد علي عريان، **الجرائم المعلوماتية**، دار الجامعة الجديدة، الإسكندرية 2004.
- محمود أحمد عبابنة، **جرائم الحاسوب وأبعادها الدولية**، الأردن: دار الثقافة، 2005.
- منير محمد الجهيني وممدوح محمد الجهيني، **جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها**، دار الفكر الجامعي، الإسكندرية، 2004
- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية و تطبيقية، دار النهضة العربية، .2004
- نهلا عبد القادر المومني، **الجرائم المعلوماتية**، عمان: دار الثقافة، 2008.
- هلالي عبد اللاه أحمد، **تفتيش نظم الحاسب الآلي وضمانات المجرم المعلوماتي**، القاهرة: دار النهضة العربية، 1997.
- **المذكرات و المقالات:**
- أحمد بن محمد اليماني، الحماية الجنائية للبريد الإلكتروني، دراسة تأهيلية مقارنة ، رسالة ماجستير ، تخصص سياسة جنائية، جامعة نايف العربية للعلوم الأمنية، السعودية، 2010
- إقلولي أولد رابح صافية، الطبيعة القانونية للجريمة المعلوماتية، أعمال الملتقى الوطني حول "الجريمة المعلوماتية بين الوقاية والمكافحة"، يومي 16 و17 نوفمبر 2015، جامعة بسكرة.
- إيهاب ماهر السنباطي، **الجرائم الإلكترونية (الجرائم السيبيرية) قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد** ، ندوة إقليمية الجرائم المتصلة بالكمبيوتر ،المغرب ، 2007.
- بورزام أحمد وكيل الجمهورية لدى محكمة باتنة بالمجلس القضائي، محاضرة بعنوان **جرائم المعلوماتية**، 2006/06/20.
- جان فرنسوا هنروت ، **أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي** ،ندوة إقليمية الجرائم المتصلة بالكمبيوتر، المغرب ، 2007.

قائمة المصادر و المراجع

- حمشاشي أمينة، ماهية الجريمة المعلوماتية، مجلة الدراسات والأبحاث، العدد الأول، 2009.
- ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة الدكتوراه، قسم الحقوق، جامعة الحاج لخضر، باتنة، 2016.
- طرشي نورة، مكافحة الجريمة المعلوماتية، (رسالة ماجستير)، قانون الجنائي،جامعة الجزائر 1، الجزائر ، 2012
- عطا الله فشار. بحث حول مواجهة الجريمة المعلوماتية في التشريع الجزائري كلية الحقوق والعلوم السياسية بجامعة الجلفة
- رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الأنترنت، (رسالة ماجستير)، قانون عام، جامعة أبي بكر الصديق، تلمسان، 2012
- محمد الأمين البشيري، التحقيق في الجرائم، المستحدثة، مركز الدراسات و البحوث، جامعة نايف العربية ، السعودية، 2004.
- محمد التدلاوي، **الجريمة المعلوماتية في القانون المغربي والمقارن**، مجلة الملف، العدد الثامن، 2006.
- محمد بن عبد الله بن علي المنشاوي، جرائم الإنترنت في المجتمع السعودي، أطروحة الماجستير، قسم العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003
- محمد علي سالم وحسون عبيد هجيج، **الجريمة المعلوماتية**، مجلة العلوم الإنسانية،جامعة بابل، المجلد الرابع عشر، العدد الثاني، 2007.
- مشتاق طالب وهيب، **مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها**، مجلة العلوم القانونية والسياسية، جامعة ديالي، المجلد الثالث، العدد الأول، 2014.
- معاشي سميرة، **ماهية الجريمة المعلوماتية**، مجلة المنتدى القانوني، جامعة بسكرة، العدد السابع..

- المهندس حسن ظاهر داود، جرائم نظم النعلومات، أكاديمية نايف العربية الأمنية، الرياض،2000
- ناصر بن محمد البقمي، **مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية**، الطبعة الأولى، الإمارات العربية: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2008.
- ندوة علمية عقدت في تونس في الفترة من 28 – 30 جوان 1999، تحت عنوان الظواهر الإجرامية، 1999.
- **مراجع لاتينية:**
- Myriam Quéméner, Yves Charpenel, **La Cybercriminalité**, édition economica, françe, 2010.
- **.مواقع ألكترونية:**
- htpp// www.Stanford.edu.html.p.52_39

الفـهرس

الفصل الأول: ماهية الجريمة المعلوماتية

الفصل الثاني:مواقف التشريعات و الجهود الدولية لمكافحة الجريمة المعلوماتية

مـلخص:

شبكة الأنترنت غزت العالم حتى أدركت الجرائم .مما جعلها تتنوع لتستحدث جرائم المعلوماتية التي أصبحت تهدد الأمن العالمي مما أوجب التحدث عن التشريعات المكافحة لها والعمل على التصدي و الوقاية منها ولهذا تمحور موضوعنا حول التعريف بهذه الجرائم وذلك من خلال ذكر كل مايتعلق بها من مصطلحات و التعرض لخصائصها لفرزها عن باقي الجرائم التي تشابهها، وكيف كانت وجهة نظر القانون لها بتحديد طبيعتها و من هم أطرافها و مايميزهما عن أطراف باقي الجرائم ، وهنا نجد أن فكر الجاني ينوع في الجرائم لنجد أصناف مختلفة في هذه الجرائم منها المتعلقة بالأنترنت وأخرى بالحاسب الألي ، وهذه النقاط هي ماتعرضنا لها في الفصل الأول أما الفصل الثاني فجاء للجانب التشريعي الدولي و الوطني لنجد الصدراة لكل من المشرع الأمريكي لطبيعة التطور الذي مسها في مجال المعلوماتية مما إضطرها لحصرها ومكافحتها، وكذلك الأمر بالنسبة للمشرع الفرنسي الذي هدف لحماية الأمن الإقتصادي للإنتهاكلت التي مست القطاع لنصل للتشريع الوطني لنجد فيه كيفية مكافحة الدول لهذه الظاهرة على المستوى الداخلي ومنها وجهة نظر المشرع الجزائري التي اخصها بحماية إجرائية و موضوعية ككافة التشريعات الأخرى، وبعدها تتوسع الدراسة لتصل للمكافحة الإقليمية على المستوى العربي الذي أصدر في شأنها عدة قوانين و عقد لها العديد من المؤتمرات و الندوات ، لتساير بهذا الحماية الدولية التي تعرض لها المجلس الأوروبي الذي أصدر أهم إتفاقية لمكافحة الجريمة المعلوماتية وهي إتفاقية بودابست و غيرها ، و كذلك الأمر بالنسبة للأمم المتحدة التي عملت جاهدة لسن ماقد يخفف من الجرائم في هذا النوع و الحد منها ، و هذه المكافحة واجهتها العديد من الصعوبات التي حددت لأجل قيام التعاون الدولي لمحاربتها و القضاء عليها .