مكافحة جرائم الكمبيوتر على ضوء التشريعين الوطني والدولي

الدكتور خالد الشرقاوي السموني

جامعة محمد الخامس بالرباط-المغرب

يشهد العالم حاليا عصرا جديدا و معالم نهضة علمية تمثلت بشكل أساسي في ظهور الحاسب الآلي و ما صاحبه من قفزة هائلة في مجال الانترنت و الاتصالات . فلقد حدثت طفرة في الاتصالات حولت العالم إلى قرية صغيرة ، فأصبح الإنسان يستطيع أن يرصد ما يجري على الطرف الآخر من الكرة الأرضية بالصوت و الصورة في لحظة قيام الحدث ، و أصبحت عملية تبادل المعلومات و المعارف سهلة و سريعة من خلال استخدام وسائل الاتصال الحديثة .

و قد تعدى دور الحاسب الآلي مجرد إجراء العمليات الحسابية المعقدة ليشمل قضايا تهم الناس في جميع معاملاتهم بما فيها القضايا التجارية و المصرفية و غيرها . إن هذا التطور الكبير و المتسارع لدور الحاسب الآلي أضاف للإنسان قدرات هائلة على الاحتفاظ بالمعلومات و معالجتها بسرعة خيالية ، و ترافق مع تزايد الوعي لدى الشعوب بأهمية المعلومة باعتبارها مصدرا للقوة و للثروة أحيانا.

وهناك من يرى أن الإنسانية تعيش اليوم عصر ثورة المعلومات التي تقدم بصورة مذهلة ، حيث أصبحت تجارة المعلومات تمثل 8 % من قيمة التجارة الدولية العالمية، و لم يعد يوجد أي مجال اقتصادي أو اجتماعي أو صناعي أو إداري إلا و تلعب الحاسبات و تقنية المعلومات دورا رئيسيا في أدائه و تطويره.

و نتيجة لهذا التطور في عالم المعلوماتية ، نشأت و نمت أنواع جديدة من الجرائم التي ما كانت لتبصر النور لولا ظهور جهاز الكمبيوتر و التقدم المذهل لاستخدام شبكة الانترنت . وقد تنوعت هذه الجرائم واتخذت مظاهر مختلفة.

فهل هذه الجرائم تنتمي إلى جرائم الأموال؟ أم إلي جرائم الأشخاص ؟ أم إلي جرائم المصلحة العامة ؟هل هي من الجرائم التقليدية ؟ أم من الجرائم الاقتصادية ؟ أم هي لا تنتمي أي من هذا أو ذاك؟ بل نوعية جديدة من الجرائم ...إلخ. وقد اتخذت هذه الجرائم مسميات مختلفة منها : القرصنة ، و اعتبر منفذيها من المتطفلين الذين تم تقسيمهم على ثلاث مجموعات :الأولى تقوم بانتهاك أمن الشبكات ، والثانية تقوم بانتهاك امن التطبيقات البرمجية ، و الثالثة تقوم بابتداع برامج تهدف إلى تدمير القرص الصلب بجهاز الكمبيوتر أو غيره .

و لقد تنبه العالم إلى خطورة الجرائم التي تتم باستخدام الكمبيوتر و شبكة الانترنت ، و برز الاهتمام بمكافحتها في نهايات القرن المنصرم ، و لعل أبرز الجهود لمحاربتها هو اتفاقية الإجرام السيبيري[1] الصادرة عن المجلس الاروبي و الموقعة في بودابست في 23 نوفمبر2001،الأمر الذي شكل دافعا للعديد من الدول من خارج مجلس ارويا و القارة الأروبية إلى الانضمام إليها و أبرزها الولايات المتحدة التي صادقت عليها في 22 سبتمبر 2006 ، و دخلت بالفعل حيز النفاذ في الأول من يناير 2007 .

إن هذا الاهتمام الدولي باتفاقية الإجرام السيبيري جعل منها وثيقة ملزمة دولية بالنسبة للدول الأطراف فيها ، و تسعى العديد من الدول غير الأعضاء في المجلس الاروبي للانضمام إليها.

وقد عبرت اتفاقية المجلس الاروبي حول الإجرام السيبيري عن إدراك دول المجلس للمخاطر الجديدة التي تعرضها شبكات الكمبيوتر و سرعة تطورها و انتشارها ، اد جاء في ديباجتها ما يلي :

[1] للاطلاع على النص الكامل لاتفاقية الإجرام السيبيري ، يرجى مراجعة الموقع الالكتروني الخاص بالمجلس الاروبي :
http//www.conventions.coe.int/treaty/ENtreaties/html/185.htm

" - اقتناعا من الدول أعضاء مجلس الاتحاد الاروبي بضرورة منح الأولوية للسعي من أجل تنفيذ سياسة جنائية مشتركة تهدف إلى حماية المجتمع من أخطار جرائم الانترنت ، و هي التي تشمل أمورا من بينها تبني التشريع المناسب و دعم التعاون الدولي .

- و إدراكا لعمق التغيرات التي أحدثها التحول إلى الرقمية و ارتباط شبكات الكمبيوتر مع بعضها البعض مع استمرار عولمتها .
- و انشغالا بمخاطر احتمال استخدام شبكات الكمبيوتر و المعلومات الالكترونية أيضا في ارتكاب جرائم جنائية ..."

أما فيما يخص العالم العربي ، فلا توجد اتفاقية أو مشروع خاص بالتعاون الإقليمي العربي في مجال مكافحة الجرائم التي تتم باستخدام الكمبيوتر أو شبكة الانترنت. ومن هنا تبرز أهمية نشر الوعي وزيادة المعرفة في هذا المجال في المنطقة العربية ، كما تبرز أيضا ضرورة تدريب سلطات إنفاذ القانون و الملاحقة القضائية على هذا النوع من الجرائم لاسيما في ظل التطورات السريعة التي يشهدها العالم.

وسنتطرق في هذا البحث إلى :

- الجرائم المتصلة بالكمبيوتر مع تحديدها و ذكر بعض أنواعها (المبحث الأول)

- التشريعات الدولية والوطنية لمكافحة هذا النوع من الجرائم (المبحث الثاني)

المبحث الأول: الجرائم المتصلة بالكمبيوتر : تحديدها و أنواعها

المطلب الأول : لمحة عامة عن مفهوم المعلوماتية و الجرائم المتصلة بها

المعلوماتية مصطلح استعمله لأول مرة البروفيسور Mikhailov مدير المعهد الاتحادي للمعلومات العلمية و التقنية (VINTTI) بالاتحاد السوفياتي سابقا و سما لعلم المعلومات

العليمة Science of Scientific Information [2]، ثم ذاع استخدامه بعد ذلك على مستوى جغرافي واسع ، و بمفاهيم متباينة ، حتى أحصى له البعض أكثر من ثلاثين تعريفا مختلفا في الكتابات المتخصصة في علم المعلومات .

و للأكاديمية الفرنسية تعريف للمعلوماتية أوجزته في أنه علم التعامل العقلاني ، على الأخص بواسطة آلات أوتوماتيكية ، مع المعلومات باعتبارها دعامة للمعارف الإنسانية ، و عمادا للاتصالات في ميادين التقنية و الاقتصاد و الاجتماعي .[3]

و لليونسكو (UNESCO) تعريف موسع و أكثر حداثة ، لتقنية المعلومات ، أو ما اصطلح على تسميته بالمعلوماتية ، يدرج في مفهومها الفروع العلمية و التقنية و الهندسية و أساليب الإدارة الفنية المستخدمة في تداول معالجة المعلومات و في تطبيقاتها و المتعلقة كذلك بالحسابات و تفاعلها مع الإنسان ، و الآلات ، و ما يرتبط بذلك من أمور اجتماعية و اقتصادية و ثقافية .[4]

ان التعريفات التي قدمت للجريمة المعلوماتية عديدة ، و متفاوتة فيما بينها ضيقا و اتساعا ، و يمكن بوجه عام تصنيفها إلى الفئات الاربع التالية :[5]

1- التعريفات المتمركزة حول وسيلة ارتكاب الجريمة .
2- التعريفات المتمركزة حول موضوع الجريمة
3- التعريفات المرتبطة بتوافر المعرفة بتقنية المعلومات
4- تعريفات مختلطة و متنوعة.

---

[2] TR.Russ.Informatika (A.I.Mikhailovet et al.1966, in Nauchno-technicheskaya informastiya XII.35) , f INFORMAATION : see – ICS

[3] في فرنسا ، ان الاستخدام الرسمي لكلمة المعلوماتية قد تم تكريسه في مجلس الوزراء ، تم اعتمده الأكاديمية الفرنسية في العام 1967 http : www.academie-francaise.fr: http//fr : wikipedia.org/wiki/informatique :

[4] www.unesco

[5] و قد قسم رجال القانون ، لاسيما الفرنسيين ، الجرائم المعلوماتية الى فئتين 1/ الجرائم المرتكبة بواسطة المعلوماتية 2/ الجرائم حيث المعلوماتية هي موضوع الجريمة .

المطلب الثاني: خصائص الجرائم المتصلة بالكمبيوتر

اتسعت تطبيقات الجرائم المتصلة بالكمبيوتر في المجتمع مما أعطاها طابعا قانونيا خاصا يميزها مجموعه مشتركة من الخصائص أبرزها ما يلي :

1- الهدف و الدافع وراء الارتكاب :

إن أكثر هذه الجرائم تستهدف إدخال تعديل على عناصر الذمة المالية ، و يكون الطمع الذي يشبعه الاستيلاء على المال هو الدافع و المحرك لارتكابها ، و قد ترتكب أحيانا لمجرد قهر نظام الحاسب و تخطي الحواجز المادية المضروبة حوله ، او بدافع الانتقام من رب العمل .

2- التعاون و التواطؤ على الأضرار :

هدا هو الهدف الأكثر شيوعا في تلك الجرائم ، وغالبا ما يتضمن متخصص الحاسبات يقوم بالجانب الفني من المشروع الإجرامي ، و أخر خارج المؤسسة المجني عليها لتغطية عملية التلاعب و تحويل المكاسب عليه.

الإضرار :

هذه النوعية من الجرائم في تزايد خاصة فيما يتعلق بالمعاملات الاقتصادية و الدولية مما يضفي أبعادا غير مسبوقة من حيث الخسائر ، و الأضرار التي تنجم عن هذه الجرائم .

3- صعوبة الاكتشاف و الإثبات :

عادة ما يتعلق ارتكاب تلك الجرائم بأرقام و بيانات تتغير و تمحي من السجلات المخزونة في ذاكرة الحاسب . و لان هذه الجرائم لا تترك أثرا خارجيا فهي صعبة الاكتشاف ، فضلا عن عدم وجود اثر كتابي لها كونها تتم بالنبضات الالكترونية لنقل المعلومات . و ما يزيد من صعوبة اكتشافها هو إمكانية ارتكابها عبر الدول و القارات باستخدام شبكات الاتصال ، و الأحجام في مجتمع الأعمال عن الإبلاغ عنها تجنبا للإساءة إلى السمعة و اهتزاز الثقة في كفاءة المنظمات المجني عليها ، و أخيرا إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة تقل عن الثانية .

ج- أنواع الجرائم المتصلة بالكمبيوتر :

يختلف موضوع الجريمة المعلوماتية حسب ما إذا كان موضوع الجريمة هو أحد مكونات النظام المعلوماتي ، أو هي مرتكبة من خلال هذا النظام بحيث يكون هو وسيلة تنفيذها و أداتها . و في الحالة الأولى تجتمع الجرائم التقليدية البحتة و الجرائم المعلوماتية بمعناها الفني . فتتوافر أولادهما ادا كانت المكونات المادية للنظام ، كالأجهزة و المعدات و الكابلات ، هي محل الاعتداء أو موضوع الجريمة ، و لم يكن ثمة أهمية للتقنية في ارتكاب الجريمة كما هو الحال في سرقة او إتلاف الحاسب أو شاشته . و تتوافر الثانية حينما تكون المكونات غير المادية للنظام كالبيانات و البرامج في ذاتها هي محل الاعتداء، كما هو الحال في الاعتداء البيانات المختزنة في ذاكرة الحاسوب أو المنقولة عبر شبكات الاتصال بالسرقة او التزوير ، أو الاعتداء على البرامج ذاتها بادعاء ملكيتها أو سرقتها أو تقليدها أو إتلافها أو محوها أو تعطيلها . وصور الاعتداء الثانية أي الاعتداء على البيانات و البرامج ، لا الأولى ، هي التي لم يتم ، بسبب حداثتها النسبية ، معالجتها في معظم قوانين العقوبات القائمة .

و في الحالة الثانية ، أي الجرائم المرتكبة من خلال النظام المعلوماتي بحيث يكون هو وسيلة تنفيذها و أداتها نكون إزاء جرائم تقليدية أداة ارتكابها ووسيلة تنفيذها هي الحاسب أو النظام المعلوماتي . و من الوجهة النظرية ، كما تشهد بعض الحالات الواقعية ، يمكن استخدام الحاسب لارتكاب طوائف من الجرائم شتى مثل تنسيق الجماعات الإرهابية عن بعد ، و تنسيق جهود عصابات الجريمة المنظمة ، و السطو على اموال البنوك ، و ابرام صفقات وهمية بأسماء أشخاص آخرين ، و الاحتيال باستخدام بطاقات الدفع الالكتروني ، و غسيل الأموال القذرة ، و التهديد بالقتل ، و استثارة الغرائز الجنسية ، و نشر المطبوعات المخلة بالآداب العامة .

و هنا يلاحظ أن الفاعل في مثل هذه الجرائم يقوم بالتلاعب في الحاسب و نظامه ، اما محلها المادي فيختلف بطبيعة الحال بحسب الشيء الذي ينصب عليه سلوك الفاعل و الذي يشكل محل الحق او المصلحة المحمية .

هذا التقسيم للجرائم التي تم باستخدام الكمبيوتر يبرز في التصنيف الذي اقرته وزارة العدل الامريكية لجرائم الكمبيوتر حيث تضمن :

1- السطو على بيانات الكمبيوتر
2- الاتجار بكلمة السر
3- حقوق الطبع والبرامج و الأفلام ، التسجيل الصوتي و عمليات القرصنة
4- سرقة الأسرار التجارية باستخدام الكمبيوتر
5- تزوير العملة باستخدام الكمبيوتر
6- تزوير الماركات التجارية باستخدام الكمبيوتر
7- تهديدات القنابل بواسطة شبكة الانترنت
8- الاحتيال بواسطة شبكة الانترنت
9- الإزعاج عن طريق شبكة الانترنت
10- الاتجار بالمتفجرات او الأسلحة النارية أو المخدرات و غسل الأموال عبر شبكة الانترنت .

المطلب الثالث: التحديات التي تشكلها الجرائم المتصلة بالكمبيوتر

كشف الانتشار الواسع في استخدام أجهزة الكمبيوتر عن خطورة ترتبط بهذا النوع من الاستخدام على عدة مصالح اجتماعية و مصالح فردية يعمل المجتمع على حمايتها ، فما لبث ان زاد استعمال الكمبيوتر الى الحد الذي تبين فيه كم هو ضروري لسير الحياة في المجتمع ، و خاصة في النشاط الاقتصادي و التجاري و الثقافي و العلمي ، بل و نشاط الافراد في حياتهم الخاصة . ان هدا التوغل في حياة الفرد و المجتمع برهن بجلاء عن ظهور قيم جديدة ترتبط بهذا الجهاز ، منها ضرورة الحرص عليه و حمايته من العدوان .

و العدوان على أنظمة الكمبيوتر يمكن ان يهدد الحياة بالشلل ، بل أنه ليس من المغالاة ان نقول ن العبث بأنظمة الكمبيوتر يمكن ان يهدد الأمن و السلم الدوليين ، من خلال الإرهاب الالكتروني حيث أن كثيرا من الأسلحة ، و منها النووية ، مرتبطة في انطلاقها بأنظمة الكمبيوتر . لذلك تبرز هنا أهمية تدارك التشريعات الوطنية لخطورة ذلك العدوان و سن التشريعات المجرمة للسلوك غير الشرعي و فرض العقوبات عليه ، و إبرام الاتفاقات الدولية بانضمام جميع الدول حتى يتسنى مكافحة ذاك السلوك .

ج- أنواع جرائم الانترنت .

أولهما : عندما تكون شبكة الانترنت هي هدف الجريمة او كما يسمى بالإجرام المعلوماتي على الانترنت كمهاجمة الشبكة بالفيروسات او إحداث أضرار بالشبكة او بنظام التشغيل و جعل الأجهزة غير صالحة للعمل أو الاكتساح او التشويش و التفخيخ .

ثانيهما : عندما تكون شبكة الانترنت هي الوسيلة المستخدمة في ارتكاب الجريمة او ما يسمى بالإجرام غير المعلوماتي في شبكة الانترنت و تشمل الجرائم التالية :

1- جرائم تقع على الأشخاص و تضم جرائم الأخلاق كالقذف والسب و التشهير عبر الانترنت و الاستغلال الجنسي للأطفال ، و كذا الاعتداء على حرمة الحياة الخاصة .
2- جرائم تقع على الأموال وتشمل السرقة و النصب و غسيل الأموال و ترويج المخدرات و جرائم التجارة الالكترونية و ارزها جرائم السرقة و النصب و الاحتيال عبر الانرنت .
3- جرائم الاعتداء على الملكية الفكرية كالاعتداء على حقوق النسخ و برمجيات الحاسوب و كذا العدوان على براءات الاختراع .
4- ظاهرة جرائم الإرهاب الالكتروني عبر الانترنت[6] .

وتختلف جرائم الانترنت أو الجرائم الالكترونية عن الجرائم التقليدية في أطرافها حيث يتميز مرتكبها بمهارات تقنية عالية اذ ان له خبرة فائقة بالقدر اللازم بأمور الحوسبة و الانترنت لذلك فان معظم من يرتكبون هذه الجرائم هم من الخبراء في مجال الحاسوب الآلي و اول من تبحث عنهم الشرطة عند ارتكاب مثل هذه الجرائم هم خبراء الكمبيوتر و الانترنت و بهذا الصدد فقد صنف الباحثون فاعل الجريمة الالكترونية الى ثلاث مجموعات و ذلك على النحو الأتي ":

1- العاملون بمراكز الكمبيوتر من الشباب الهواة حديثي العهد بالمعلوماتية الذين ليست لديهم نوايا سيئة لارتكاب الجريمة و إنما تحقيق انتصارات تقنية فقط و هم يمثلون الغالبية العظمى.

2- العاملون بمراكز الكمبيوتر الخاصة بالشركات و الوزارات الذين تحولت لديهم الهوايات إلى الاحتراف فارتكبوا بحق المنشات التي يعملوا بها أفعال غير مشروعة .

4- الهاكر الخبيث الكراكر الذي يعد مجرم الانترنت المتميز و الخطير .

أما عن الضحية في هذه الجرائم فقد يكون شخص طبيعي او اعتباري ، و أداة ارتكابها ذات تقنية عالية و مكان ارتكابها لا يتطلب بالضرورة انتقال فاعلها إلى ذلك المكان بشخصه كون الجريمة تتم باستخدام شبكات الاتصال بين الجاني و مكان الجريمة .

[6] نبيلة هبة هروال نفس المرجع السابق ص 57 – 62 – 63

ليس ذلك فحسب بل أن الجرائم الالكترونية تعد من الجرائم النظيفة لصعوبة اكتشاف دليل ثبوتها فلا اتر فيها لأية عنف أو دماء و إنما مجرد أرقام و بيانات يتم تغييرها أو محوها من السجلات المخزونة في ذاكرة الحاسبات الآلية و ليس لها اثر خارجي مادي .[7]

وهذا يعود إلى أن فاعلها يتمتع بدراية فائقة في مجال الانترنت الامر الذي سهل اخفاء معالم الجريمة و التخلص من اثارها ، و بالتالي صعوبة التحقيق فيها و تتبع مرتكبيها فضلا عن اعتمادها على الذكاء و المهارة و الخداع في ارتكابها .

ومما لا شك فيه ان ظاهرة الجرائم الالكترونية كظاهرة ناتجة عن التقدم التقني عامة و تقنية الحاسوب خاصة كانت بحاجة إلى قانون ينظمها بهدف إحداث مواءمة بين المجتمع و بين التنظيم الطبيعي لتلك الظاهرة الناشئة في ارض الواقع .[8]

المبحث الثاني:التشريعات المتعلقة بجرائم الكمبيوتر

سوف نتحدث في هذا المبحث عن المواجهة التشريعية لهذا الخطر المتنامي في المجتمع و ذلك على النحو الأتي :

أولا : التشريعات الدولية لجرائم الكمبيوتر.

ثانيا : التشريعات الوطنية لجرائم الكمبيوتر.

المطلب الأول: التشريعات الدولية

[7] محمد علي العريان – الجرائم المعلوماتية – دار الجامعة الجديدة للطباعة و النشر ص 53-63

[8] الدكتور / عمر محمد ابو بكر بن يونس – الجرائم الناشئة عن استخدام الانترنت الاحكام الموضوعية و الجوانب الاجرائية – دار النهضة العربية ص 85

إن الأمم المتحدة و اغلب المنظمات الدولية و الإقليمية تولي هذا الموضوع اهتماما خاصا ، و هو الأمر الذي افرز مجموعة من المعايير الدولية ، إلا أن المجتمع الدولي لازال في حاجة إلى اتفاقية دولية ملزمة في هذا المجال .

وفي هد السياق نشير إلى أهم الصكوك الدولية التي تتناول هذا النوع من الجرائم :

أولا: اتفاقية مجلس أوروبا بشأن الإجرام السيبيري لعام 2001 :

هي الاتفاقية الوحيدة المتعددة الأطراف المعنية بمكافحة الجرائم التي تتم باستخدام / أو ضد الكمبيوتر و باستخدام شبكة الانترنت ، و هي تمثل ركيزة أساسية منذ دخولها حيز النفاذ في الأول من يوليو لعام 2004 على مستوى الدول أعضاء مجلس الاتحاد الاروبي[9] . و كما سبق الإشارة ، ، فلقد وقعت عليها العديد من الدول من غير أعضاء مجلس اروبا مثل كندا و اليابان و جنوب إفريقيا ، كما صادقت عليها الولايات المتحدة الأمريكية.

كما أن هده الاتفاقية بمثابة دعوة موجهة إلى دول العالم للتفاعل مع الانترنت جاءت نتيجة محاولات عديدة منذ ثمانيات القرن العشرين حتى ظهرت بشكلها النهائي في 2001/11/23 م في بودابست وقعت عليها ثلاثون دولة أروبية بما في ذلك الدول الأربعة من غير الأعضاء في المجلس الاروبي المشاركة في اعداد هذه الاتفاقية و عي كندا و اليابان و جنوب افريقيا و الولايات المتحدة الأمريكية .

و قد تضمنت هذه الاتفاقية الأقسام التالية :

القسم الأول : تحديد المصطلحات

القسم الثاني : الخطوات الواجب اتخاذها في إطار التشريع الوطني

[9] للاطلاع على النص الكامل لاتفاقية الاجرام السيبيري و لمعرفة مزيد من التفاصيل حول تطبيق هذه الاتفاقية ، يرجى مراجعة الموقع الالكتروني الخاص بالمجلس الاروبي .
http///www.coe.int/t/e/legal-affairs/legal-co-operation/combating-economic-crime/6-Cy bercrime/
http://www.conventions.coe.int/treaty/EN/treaties/html/185.htm

القسم الثالث : التعاون الدولي

القسم الرابع : الشروط النهائية حول الانضمام إلى الاتفاقية

كما حددت الجرائم التي يجب أن تتضمنها التشريعات الوطنية للدول الأعضاء و ذلك على النحو التالي :

1- الجرائم المتعلقة بأمن الشبكات الدخول و المراقبة غير المشروعة و العدوان على الثقة في البيانات او على النظام و الإساءة إليه .
2- الجرائم المعلوماتية كما هو الشأن في الاختلاق و الانتحال و النصب و الاحتيال المعلوماتي ...الخ
3- جرائم الأخلاق مثل إنتاج او بث او حيازة ما يتعلق بدعارة الأطفال .
4- جرائم العدوان على حقوق الملكية الأدبية و الفكرية كاستنساخ المصنفات المشمولة بالحماية .
5- المسؤولية الجنائية للأشخاص المعنوية .

و كذلك الاهتمام بالإجراءات الجنائية لاسيما في مرحلة التحقيق و الملاحقة القضائية مثل التحفظ على الأدلة و التفتيش و الضبط و ما إلى ذلك .

وقد حملت هذه الاتفاقية الطابع التوجيهي للخطوات التي يلزم اتخاذها في إطار التشريع الوطني في كل دولة فيما يتعلق بالأحكام الموضوعية و الإجرائية كما اشرنا أعلاه.

ولزمت الدول الأعضاء بمراعاة حقوق الإنسان و حرياته الأساسية التي تضمنتها الاتفاقيات الدولية و التشريعات الوطنية على حد سواء و الالتزام بعدم انتهاكها. مع إمكانية الدول الأخرى غير الأعضاء في الاتفاقية الاستعانة بهذه الاتفاقية عند إعداد التشريعات الوطنية باعتبارها مصدر تاريخي في مجال مكافحة الجريمة على الانترنت.

من ناحية أخرى تولى مجموعة الثمانية الكبار أهمية خاصة للجرائم التي تتم باستخدام أو ضد الكمبيوتر ، و قد شكلت عدة مجموعات عمل صدرت عنها مجموعة كبيرة من التوصيات و القرارات في مجال مكافحة هذا النوع من الجرائم ، و ابرز هذه القرارات ما صدر

عن مجموعة العمل المعروفة باسم Lyon Group التي شكلت أثناء قمة هاليفاكس في كندا عام 1995 تحت مسمى توصيات من اجل مكافحة الجريمة المنظمة عبر الوطنية بفعالية.

ثانيا: قانون الانسيترال النموذجي بشأن التجارة الالكترونية لعام 1996:

هذا القانون تم اعتماده من قبل لجنة الأمم المتحدة عام 1996 ، وهو يعتبر من الجهود الدولية لمكافحة جرائم الانترنت في مجال التجارة الالكترونية قامت اللجنة بإعداده كقانون نموذجي انطلاقا من ولايتها المتمثلة في تعزيز تنسيق و توحيد القانون التجاري الدولي بغية إزالة أية عقبات لا لزوم لها أمام التجارة الدولية تنتج عن أوجه القصور و الاختلاف في القانون المتعلق بالتبادل التجاري ، و قد جاء إعداده في الأساس استجابة للتغير الرئيسي الذي حدث في الوسائل التي تتم فيها الاتصالات بين أطراف يستخدمون في أعمالهم التقنيات الحاسوبية أو غيرها من التقنيات الحديثة.

و قد كان القصد منه أن يكون نموذجا تهتدي به البلدان فيما يتعلق بتقييم و تحديث جوانب معينة من قوانينها و ممارساتها في ميدان العلاقات التجارية، و مساعدة جميع الدول على تحسين تشريعاتها و على تدارك المساوى الناجمة عن قصور التشريعات على الصعيد الوطني مع تقديمه للمشرعين الوطنيين مجموعة من القواعد المقبولة دوليا في هذا المجال.

المطلب الثاني : التشريعات الوطنية

في بعض الدول العربية كمصر واليمن ،مثلا ، نجد أن مكافحة جرائم الكمبيوتر تمت معالجتها بقوانين عامة كالقانونين المدني والجنائي. ففي نجد المادة التاسعة من القانون 260 لسنة 1980 في شان الأحوال المدنية المعدل بالقانونين رقمي 11 لسنة 1965 و 158 لسنة 1980 على أن البيانات التي تحويها سجلات الأحوال المدنية تعتبر سرية و قد جاء بالمذكرة الإيضاحية للقانون " أنه لما كانت هذه السجلات تحوي أدق البيانات عن حالة الشخص فقد أسبغت عليها السرية حتى يطمئن كل شخص على ما يقدمه من بيانات . أن نطاق السرية يمتد إلى كل من لا يفرض عليه واجبة طبقا لقانون الأحوال و لائحته التنفيذية و القرارات

المنفذة له الاطلاع على هذه البيانات ، و ذلك ما لم تصدر سلطة قضائية أو سلطة تحقيق قرارا بالاطلاع عليها أو فحصها لان الصالح العام يفضل صالح الشخص في المحافظة على سرية بياناته ، و باعتبار هذه البيانات سرا فان إفشاءها من قبل الموظف الملزم بكتمانها يوقعه تحت العقاب المنصوص عليه في المادة 310 من قانون العقوبات".

ومثل هذه الحماية لا وجود لها في التشريعات العربية، و إنما مجرد نصوص فرعية متفرقة في قوانين مختلفة مثل حماية سجلات الأحوال المدنية في قانون الأحوال المدنية ، و كذا حماية بيانات الضمان الاجتماعي و عدم جواز استخدامها لأغراض أخرى كما هو في قانون الضمان الاجتماعي و هذه النصوص في مجملها لا يمكن اعتبارها تشريعا خاصا يحمي حق الخصوصية ، و إنما مجرد تطبيقات بسيطة لمثل هذا الحق مما يستلزم سنها في تشريعات خاصة تتلاءم معها .

وفي اليمن نجد أن القانون الجنائي قد نص على مجموعة من المقتضيات ترمي إلى مكافحة الجريمة في مجال الاعتداء على الأموال كالسرقة و الاحتيال و الابتزاز و خيانة الأمانة و التزوير و ذلك في المواد التالية (318,313,310,210) من القانون رقم (12) لعام 1994 م بشان الجرائم و العقوبات، وكذا في مجال الاعتداء على الأشخاص كجريمة التهديد ، انتهاك حرية المراسلات ، الاعتداء على حرمة الحياة الخاصة ، و التهديد باداعة الأسرار الخاصة كما هي ثابتة المواد257.256.255.254من نفس القانون.

إلا أنه ومع الاستخدام المتزايد لتقنية المعلومات في شتى مجالات الحياة و ظهور المعلوماتية و تطبيقاتها المتعددة و ما ترتب على ذلك من ظهور تقنيات جديدة في ارتكاب الجريمة التقليدية كالاستيلاء على الأموال عن طريق الاحتيال المعلوماتي أو كإرسال بريد يتضمن تهديد بالقتل أو اختراق شبكات المعلومات، جعل القانون الجنائي أمام قصور بين في مواجهة تلك الجرائم.

و هذا يرجع في الأساس إلى أن مواد القانون الجنائي اليمني نصوص تقليدية وضعت أساسا لحماية الأشياء المادية في مواجهة صور الاعتداء التقليدي عليها ، و بالتالي فقد تعذر تطبيق تلك النصوص على حالات الاعتداء على المكونات غير مادية للأنظمة المعلوماتية.

لكن في المقابل هناك دول عربية سارعت إلى سن قوانين خاصة بالجرائم الالكترونية ونذكر على سبيل المثال المملكة العربية السعودية والإمارات العربية المتحدة والمغرب.

فقد وافق مجلس الوزراء في المملكة العربية السعودية سنة 2007 على نظامي مكافحة جرائم المعلوماتية والتعاملات الالكترونية، وكان ذلك للحد من وقوع الجرائم المعلوماتية وتحديد الجرائم المستهدفة بالنظام والعقوبات المقدرة لكل جريمة أو مخالفة، وتحديد جهة الاختصاص بمتابعتها وتطبيق العقوبات.

ويرمي هذا القانون إلى تأمين استخدام أجهزة الكمبيوتر وشبكة المعلومات الدولية (الانترنت) من عبث العابثين الذي يتمثل في ارتكاب جرائم الأموال وجرائم الآداب وجرائم الإرهاب وجرائم السب والقذف، وجرائم غسل الأموال.

وفي الإمارات العربية المتحدة صدر القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات، حيث تنص المادة 2 من القانون على أن "كل فعل عمدي يتوصّل فيه بغير وجه حق، إلى موقع أو نظام معلوماتي، سواء بدخول الموقع أو النظام، أو بتجاوز مدخل مصرّح به، يعاقب عليه بالحبس وبالغرامة، أو بإحدى هاتين العقوبتين، فإذا ترتّب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات، فيعاقب بالحبس مدة لا تقلّ عن 6 أشهر، وبالغرامة أو بإحدى هاتين العقوبتين".

فيما تنص المادة 3 من القانون السالف الذكرعلى أن كل "كل من ارتكب أياً من الجرائم المنصوص عليها في البند 2 من المادة 2 من هذا القانون، أثناء أو بسبب تأدية عمله، أو سهّل ذلك للغير، يعاقب بالحبس مدة لا تقل عن سنة، ويغرّم ما لا يقلّ عن 20 ألف درهم، أو بإحدى هاتين العقوبتين".

وفي المغرب فقد صدر قانون يتعلق بجرائم نظم المعالجة الآلية للمعطيات، لسد الفراغ التشريعي الحاصل في مجموعة القانون الجنائي في ما يتعلق بتجريم الأفعال المرتبطة بتكنولوجيا المعلوميات ووضع العقوبات الملائمة لها بغية تحصين المغرب ضد هذا النوع من الجرائم ومواكبة التطور الذي يشهده العالم في هذا الإطار ، إضافة إلى منح القضاء الآليات القانونية للفصل في الجرائم المعروضة عليه من هذا النوع.

ويتضمن القانون مختلف الأفعال التي تعتبر جرائم ضد نظم المعالجة الآلية للمعطيات والعقوبات الملائمة لها حسب درجة خطورتها والمتمثلة أساسا في ولوج نظم المعالجة الآلية للمعطيات عن طريق الاحتيال وعرقلة سير نظم المعالجة الآلية للمعطيات أو إحداث خلل بها أو إتلافها.

وفي هذا السياق ندعو الحكومات العربية التي لم تصد بعد قوانين لمكافحة جرائم الكمبيوتران تسرع في إصدارها نظرا للتزايد المضطرد لهذا النوع من الجرائم وما يحمله من خطورة عله المجتمع والأفراد وتهديد للنظام والأخلاق والقيم الاجتماعية.

بعض المراجع المعتمدة:

- دة. شيماء عبد الغني محمد عطا الله ،كلية الأنظمة والعلوم السياسية: مكافحة الجرائم المعلوماتية في المملكة العربية السعودية

- لاتفاقية الاجرام السيبيري ، يرجى مراجعة الموقع الالكتروني الخاص بالمجلس الاروبي : http//www.conventions.coe.int/treaty/ENtreaties/html/185.htm

-TR.Russ.Informatika (A.I.Mikhailovet et al.1966, in Nauchno-technicheskaya informastiya XII.35) , f INFORMAATION : see – ICS

- د.محمد علي العريان – الجرائم المعلوماتية – دار الجامعة الجديدة للطباعة و النشر ص 53-63

- د. عمر محمد ابو بكر بن يونس – الجرائم الناشئة عن استخدام الانترنت الأحكام الموضوعية و الجوانب الإجرائية – دار النهضة العربية ص 85

- د- عمر بن يونس ,مركز حرية الإعلام ، نونبر 2007