وزارة التعليم العالي والبحث العلمي
جامعة عمار ثليجي الاغواط
كلية الحقوق

الموضوع

الاليات القانونية للحماية الجنائية للبيئة الإلكترونية

مذكرة مقدمة لنيل شهادة الماستر حقوق
تخصص قانون جنائي وعلوم جنائية

إعداد الطالب :
- سليمان بكار

تحت اشراف الدكتور:
* عبد الوهاب ملياني

لجنة المناقشة

الاسم واللقب	الدرجة العلمية	الصفة
خضرون عطاء الله	الدكتور	رئيسا
عبد الوهاب ملياني	أستاذ التعليم العالي	مشرفا ومقررا
بوقرين عبد الحليم	أستاذ التعليم العالي	مناقشا

السنة الجامعية 2023-2024


بسم الله الرحمن الرحيم

مقدمة

مقدمة:

يعرف العالم اليوم بعصر التكنولوجية الحديثة حيث التطور الهائل والسريع في تقنيات الاتصال الحديثة فقد انسابت المعلومات من كافة مصادرها عن طريقها وبواسطتها نظرا لالتفاف الأشخاص والجماعات والدول حولها وذلك من مختلف القارات والبلدان والأجناس حيث فعلت هذه التقنية ما لم تفعله السياسة في توحيد الشعوب والثقافات

فلا ريب الآن أن تلك النظم لها علاقة بالحواسيب وشبكة الأنترنت ذات الصبغة العالمية والتي تتحدد قيمتها لا من حيث مشتركيها فقط بل حتى من القدرة على تبادل المعلومات في تلك البيئة الافتراضية، لتصبح من ضروريات الحياة اليومية سواء بالنسبة للأشخاص الطبيعية ام المعنوية العامة منها او الخاصة، بل إن الدول والحكومات في وقتنا الحالي اتجهت لتسيير أعمالها أساسا على استخدام نظم المعلوماتية وهذا بالنظر لما تتميز به من سرعة و دقة في معالجة المعلومات الإلكترونية من تجميع لها وتخزين واسترجاع وتبادلها بين الأشخاص داخل الدولة أو خارجها ، لهذا أصبحت مكمن سرهم فيما تعلق بحياتهم الشخصية أو بطبيعة معاملاتهم المختلفة المالية منها على الخصوص والاقتصادية بصفة عامة ، كما أنها مكمن أسرار الدولة و البنوك و المؤسسات الاقتصادية .

فالخطورة التي تتجلى يوما بعد يوم لهذه الجرائم تتمثل بالخصوص في أنها سهلة الارتكاب نتيجة الاستخدامات السلبية للتقنية المعلوماتية بما توفره من تسهيلات ، هذا بالإضافة الى أنها عابرة للحدود الدولية ، إضافة للميزات التي يمتاز بها المجرم المعلوماتي من ذكاء و معرفة تقنية ، هذا بالإضافة الى الطبيعة المتميزة لمحل الاعتداء و المتمثل في المعلومات المتواجدة في تلك البيئة المتميزة مع أننا سنتكل بصفة عامة و متواصلة طيلة الدراسة عن النظام المعلوماتي على أساس أنه خزان المعلومات الإلكترونية بل إنه يمثل أساس تداولها فلولاه لما كانت المعلومات الإلكترونية محل دراستنا فهو الثغرة او المكان الذي يجد فيه المجرم المعلوماتي ضالته المتمثلة في المعلومات الإلكترونية ، وذلك باختراقه للنظام المعلوماتي ، الاطلاع عليها بطريق غير مشروع ، أو تخريبها ، أو إتلافها .....

ولماّ كان الحال كما ذكرناه أعلاه نجد أن المشرع الجنائي اتخذ موقفا حاسما في العديد من الدول بوضع نصوص خاصة لإضفاء حماية للنظام المعلوماتي من الأفعال التي تشكل تهديدا عليه فأضفى عليها الصبغة التجريبية.

وهذا الذي قام به المشرع الجزائري لما عدّل قانون العقوبات بالقانون رقم 04-15[1] والذي أفرد فيه قسما سابعا مكرر المتضمن لثمانية مواد من المادة 394 مكرر الى المادة 394 مكرر 7 والتي عالجت عدة جوانب تجريميه لأفعال مختلفة منها الدخول أو البقاء عن طريق الغش للمنظومة المعلوماتية، تخريب النظام المعلوماتي، إدخال أو إزالة تعديل المعطيات في النظام المعلوماتي، ...

لذا تكمن **أهمية البحث** التي نوجزها أساسا في النقاط التالية:

معرفة تلك المشكلات القانونية التي تواجه دراسة أمن المعلومات في بيئة الأعمال الإلكترونية كونها من الإشكالات لتي تعالج نمطا جديدا ومستحدثا من انماط الجرائم وهي تلك الجرائم المتعلقة بالمعلوماتية وبالخصوص الاعتداءات الواقعة على النظام المعلوماتي حيث تعتبر من المستجدات التي لم تكن معروفة على الساحتين الوطنية والدولية بدليل ما نتج من اتفاقيات دولية وإقليمية لمكافحة تلك الجرائم التي منها اتفاقية بودابست المنعقدة في 23 ابريل 2001 بإشراف المجلس الأوروبي.

حيث **الهدف من الدراسة** هو الوقوف على مفهوم جرائم الاعتداء على النظام المعلوماتي وتحديد استقلاليتها عن باقي الجرائم التقليدية الأخرى والذي انعكس على التشريعات التقليدية، هذا بالإضافة لشرح مسألة مهمة جدا والتي تدخل في صلب الدراسة والمتمثلة في عجز النصوص التقليدية للتعامل مع تلك الجرائم والتي كانت سببا لتكريس قوانين خاصة تتعلق بأمن النظام المعلوماتي من الاعتداء الواقعة عليه، وفي محاولة منا على التعرف على النصوص القانونية المتضمنة لتجريم الاعتداءات الواقعة على النظام المعلوماتي لإبراز

[1] القانون رقم 04-15، المتضمن لجرائم المساس بأنظمة المعالجة الألية للمعطيات، المتمم للأمر رقم 66-156 المتضمن لقانون العقوبات، الصادر بتاريخ 10 نوفمبر 2004.

العناصر التي تقوم عليها تلك الجرائم للوصول الى مدى توفيق المشرع الجزائري من عدمه في المسائل الموضوعية.

والوقوف عند السياسة العقابية للمشرع الجزائري ومدى نجاحها في مواجهة تلك الظاهرة المستحدثة إجراميا للحد منها والحد هنا لا يقصد منه المنع المطلق أو الكلي بل بالعكس نريد منه المنع الوقائي الذي يصل به المشرع الجنائي لإيصال رسالته الردعية العامة للكافة بأن السلوك مجرم ومعاقب عليه، وإضافة الى ذلك الردع الخاص للجاني مرتكب الجريمة حال ارتكابه للجرم.

ومن هنا يظهر جليا **سبب اختيارنا لهذا البحث** حيث أنه يعد من أهم المواضيع التي ينبغي توضيحها خاصة ونحن متجهون كدولة إلى ما يعرف برقمة الإدارة أو الحكومة الإلكترونية التي تعتبر تحولا من إدارة المعلومات الورقية إلى إدارة المعلومات الإلكترونية، الأمر الذي يشكل خطورة حقيقية على معلومات الأفراد والمؤسسات وحتى معلومات الدولة ويضعها في مواجهة الاعتداءات من حيث تأمينها القبلي وأمنها البعدي الذي نحن بصدد دراسته أي الحماية الجنائية لها من كل اعتداء يقع عليها.

و من منطلق ما سبق يمكننا عرض **الإشكالية** التي يطرحها الموضوع ، التي ترتبط أساسا بالمعالجة التشريعية لأمن المعلومات الإلكترونية في بيئة الأعمال الإلكترونية بالتحديد طبيعة الجرائم التي ترتكب عليها ، من حيث تمييزها عن غيرها وصولا إلى مدى استقلاليتها عن غيرها من الجرائم ، و انعكاس ذلك على النصوص التشريعية في المجال الجنائي، و مدى توفيق المشرع في وضع إستراتيجية لمواجهة تلك الجرائم في الجانبين الموضوعي و الإجرائي .

من خلال الاعتماد على المنهج الوصفي الذي يصف الظاهرة بتحليلها لجزئيات ندرسها ونتعمق فيها لنفهم أصل الظاهرة وحقيقتها العلمية والقانونية. والمنهج التحليلي وهذا من خلال تحليل الاستراتيجية التشريعية المنتهية لتوفي الحماية للمعلومات الإلكترونية وذلك من خلال تفكيكها الى عناصر وتحليلها من خلال النصوص القانونية الموجودة.

ولعرض كافة الأفكار المتصلة بالموضوع يترتب علينا دراسة البحث وفق الخطة منهجية التي قسمناها الى فصلين رئيسيين حيث نتطرق في الفصل الأول منه للطبيعة القانونية الخاصة لجرائم الاعتداء على النظام المعلوماتي، وفي الثاني للواقع القانوني لأمن النظام المعلوماتي من أخطار الاعتداءات الواقعة عليه.

الفصل الأول

الطبيعة القانونية الخاصة لجرائم الاعتداء على النظام المعلوماتي

المبحث الأول: استقلالية جرائم الاعتداء على النظام المعلوماتي

المطلب الأول: مفهوم جرائم الاعتداء على النظام المعلوماتي

لتوضيح مفهوم هذه الجرائم سنتطرق لتحديد مدلولها وهذا في الفرع الأول من هذا المطلب، بينما نخصص الفرع الثاني للنظام المعلوماتي (البيئة الإلكترونية للمعلومات) محل الأمن من الاعتداء عليه.

الفرع الأول: مدلول جرائم الاعتداء على النظام المعلوماتي

أولا: جرائم المعلوماتية بصفة عامة

ان تحديد مدلول جرائم المعلوماتية يعني تمييز ها عن غيرها من الجرائم [1] ، ولما كانت هذه الجرائم تهدف إلى ايذاء الاشخاص، الاموال، الحكومة، الاخلاق، الخ، فهي تكمن في سلوك محظور، لما تتميز به بمجموعة من الخصائص التي ميزتها عن غيرها من الجرائم الأخرى، فهي تعد ظاهرة اجرامية مستجدة نسبيا وذلك لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات الحديثة.

حيث انها مرتبطة بتاريخ ظهور جرائم المعلوماتية الحديثة نسبيا، فهذه الجرائم مرتبطة في وجودها التاريخي بتاريخ ظهور الكمبيوتر، ومن الوجهة التاريخية، طرح أول كمبيوتر للشراء في الأسواق التجارية عام 1954 بالولايات المتحدة الأمريكية.[2]

ولم تمض فترة طويلة على ذلك حتى سجل وقوع أول جريمة معلوماتية في نفس البلد عام 1958. ومنذ ذلك الحين زادت نسبة هذه الجرائم يوما بعد يوم، وتنوعت أساليب ارتكابها، وتعددت اتجاهاتها، كما زاد حجم الخسائر الناجمة عنها وأخطارها حتى غدت اليوم واحدة من أكثر وأخطر الأنشطة الإجرامية انتشارا في العالم. ففي عقد الستينات من العقد المنصرم توسعت دائرة هذه الجرائم، فالتفتت إليها وسائل الإعلام، حيث بدأت الصحف لأول مرة تنشر المقالات بصددها، ومن ثم زادت حدة هذه الجرائم في فترة السبعينات بحيث بدأت ملامح ظاهرة الاجرام المعلوماتي تلوح في الأفق، وبدأت الابحاث المعتمدة على الأسس العلمية ببحث هذه الجرائم في منتصف هذه الفترة. وقد كان الإضرار بأجهزة الكمبيوتر وتخريب شبكات الهاتف من الصور الشائعة لهذه الجرائم في تلك الفترة. في حين أن فترة الثمانينات والتسعينات، سجلت

---

[1] – Susan Brenner–Is there such a thing as "Virtual Crime" ?– California Criminal Law Review 4 (2001)–www.boalt.org/CCLR/V4/brenner.htp.

[2] – See: Robert M.Couch, A Suggested Legislative Approch to problem of problem of Computer crime, 38 Washingtion and Lee Law Review 1173(1981) ,p.1173,n.1.

قفزة في حجم هذه الجرائم من حيث الكم والنوع، بحيث تحدد مفهوم وماهية هذه الجرائم، وتبلور مفهوم ظاهرة الإجرام المعلوماتي بصورة واضحة تماما.[1]

وذلك بعد أن زاد نطاقها بشكل هائل بفعل ظهور شبكة "الإنترنت" واستخدامها من قبل عدد هائل من المستخدمين، مما أدى إلى ظهور أنماط وصور جديدة من هذه الجرائم، ففي الثمانينات أظهرت دراسة قام بها معهد كولفيلد للتكنولوجيا في استراليا عام 1985 ، بأن ما تزيد عن 900 جريمة معلوماتية تقع سنويا في استراليا ، وفي اليابان كشفت الشرطة المركزية بالعاصمة طوكيو عام 1988 عن وقوع 1136 جريمة معلوماتية في اليابان خلال تلك السنة ، وفي التسعينات سجلت الشرطة الألمانية وقوع 5004 جريمة معلوماتية في المانيا خلال عام 1991 .[2]

أما الألفية الجديدة فإنها شهدت تزايدا لا مثيل لها في حجم هذه الجرائم ، فبحسب الإحصاءات التي قام بها مركز (IC3) لتلقي الشكاوى عن الجرائم المعلوماتية عبر الأنترنت ،وهو مركز مؤسس بشراكة ما بين كل من مكتب التحقيقات الفدرالي في الولايات المتحدة الأمريكية (FBI) المركز الأمريكي لمكافحة جرائم الياقات البيضاء (NW3C) ، لتكون بمثابة وسيلة لتلقي الشكاوى عبر شبكة الأنترنت عن الجرائم المعلوماتية في العالم ، بلغ عدد الشكاوى التي تلقاها المركز في عام 2001 ما مجموعة (4971) شكوى فيما بلغ عددها عام 2009 ما مجموعه (336655) شكوى.

وهذا يعني بأن نسبة هذه الجرائم في تزايد مستمر ، مع الأخذ بنظر الإعتبار أن النسب المذكورة تمثل فقط عدد جرائم المعلوماتية التي تم إكتشافها والإبلاغ عنها للمركز المذكور وليس العدد الكلي لها في العالم ، حيث أنه بمقتضى دراسة للمركز الأمريكي للإستراتيجيات والدراسات العالمية ، فإن حجم هذه الجرائم في العالم يبلغ ما يقارب 10 مليارات جريمة سنويا.[3]

الجريمة المعلوماتية فقد تعددت تعريفاتها بتنوع التعبيرات التي استخدمت للدلالة عليها ، وهو تعدد رافق سيرة نماء وتطور تكنولوجيا المعلوماتية ، ويمكننا أن نعزو السبب الرئيسي لهذا التعدد في التعريفات إلى

---

[1] نائل عبد الرحمان صالح ،واقع جرائم الحاسب في التشريع الأردني ، بحيث مقدم لمؤتمر القانون والكمبيوتر والانترنت الذي نظمته كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة (2000) بحوث مؤتمر القانون والكمبيوتر والأنترنت ، المجلد الأول ، الطبعة الثالثة ، كلية الشريعة والقانون جامعة (الإمارات العربية المتحدة ، 2004 ، ص 191.

[2] نائلة عادل فريد قورة ، جرائم الحاسب الآلي الإقتصادية ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، بيوت 2005 ، ص 80-85.

[3] أيمن عبد الله فكري ، جرائم نظم المعلومات ، دار الجامعة الجديدة ، الإسطندرية ، 2007 ، ص 103.

كون الإطار أو البيئة الخاضعة لهذه الظاهرة الإجرامية ، كانت و لا تزال في طور النماء والتطور ، حيث أن عامل التطور الزمني الذي واكب تكنولوجيا المعلومات و تكنولوجيا الإتصالات ، ساهم بشكل مباشر في تعدد الإصطلاحات والتعريفات التي استخدمت للدلالة والتعريف بهذه الظاهرة التي بدأت بالظهور مع بدايات ثورة تكنولوجيا المعلومات والتي نمت وتطورت بتطورها إلى أن وصلنا إلى مرحلة اندماج تكنولوجيا المعلومات وتكنولوجيا الاتصالات. [1]

كما أنه قد أبانت التجربة أن كثير من الدول يعاني المحققون فيها من مصاعب جمّة في التصدي لجرائم المعلوماتية بسبب عدم وضع تعريف محدد لهذه الجرائم وعدم تحديد الأفعال الإجرامية المشكلة لهذه الجرائم بشكل واضح.[2]

ثانيا : الوصول لتعريف جرائم الإعتداء على النظام المعلوماتي

والآن بعد أن أوردنا التعريفات السابقة نرى بأنه من الضروري ان نحاول بدورنا وضع تعريف لجرائم الإعتداء على النظام المعلوماتي ، وفي هذا الاطار فإننا نرى بأنه عند وضع أي تعريف للجريمة عموما و لهذه الجرائم خصوصا فإنه ينبغي الاعتماد في ذلك على ما يمكن من خلاله تحديد أركان الجريمة أي أن يتضمن التعريف جميع اركان الجريمة التقليدية عموما و التي تعرّف بأنها : "**كل سلوك خارجي ايجابيا كان أو سلبيا جرّمه القانون وقرر عقابا اذا صدر عن انسان مسؤول**"[3] و قياسا على ذلك ، ولما كانت جرائم الإعتداء على النظام المعلوماتي لا تختلف عن الجرائم التقليدية إلا من حيث أن محلها هو دوما المعلومات أو البيانات الإلكترونية التي قد تكون متعلقة بالمال أو بالحياة الخاصة أو بالمصالح العامة وغيرها [4] ، و عليه نخلص إلى القول أن جرائم الإعتداء على النظام المعلوماتي هي تعبير شامل يشير إلى كل نشاط اجرامي مرتبط بإستخدام تقنية المعلومات الحديثة ، بحيث أن غياب الارتباط بها يمنع ارتكاب مثل هذا العمل غير المشروع ،و لا يختلف الأمر سواء كانت وسيلة تقنية المعلومات الحديثة أداة لإتمام النشاط الإجرامي أم كانت محلا له أو هدفا للإعتداء عليها .

---

[1] هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنيةالمعلومات – مكتبة الألات الحديثة – 1992 – ص 29.

[2] محمد الأمين البشري ، التحقيق في الجرائم المستحدثة ، الطبعة الاولى ، مركز الدراسات والبحوث بجامعة نايف العربية للعلوم الأمنية ، الرياض ، 2004 ، ص 87 و 88.

[3] علي حسين الخلف وسلطان عبد القادر الشاوي ، المبادئ العامة في قانون العقوبات ، مطابع الرسالة ، الكويت ، 1982 ، ص 134.

[4] خالد ممدوح ابراهيم ، الجرائم المعلوماتية ، ط1 ، دار الفكر الجامعي ، الإسكندرية ، 2009 ، ص 91-92.

لهذا يمكننا تعريف جرائم الإعتداء على النظام المعلوماتي بأنها : **كل سلوك متعمد ، يشكل اعتداء على المعلومات الإلكترونية ضمن بيئة إلكترونية ، يجرمه المشرع ويقرر له عقابا ، اذا صدر عن شخص مسؤول جنائيا .**

ولو قمنا بتحليل تعريفنا هذا نلاحظ فيه ما يلي :

1- أنه من حيث الركن المادي للجريمة ، يشمل جميع صور السلوك الإيجابية (فعل) والسلبية (الإمتناع).

2- أنه من حيث الركن المعنوي للجريمة يتعلق بالسلوك الصادر عن الشخص المسؤول جنائيا الذي يتوفر لديه القصد الجنائي بشقيه (العلم والإرادة) أو الخطأ غير العمدي . وهذا الشخص يستوي أن يكون شخصا طبيعيا أو معنويا.

3- أنه من حيث الركن الشرعي يشمل جميع صور السلوك الذي يجرمه المشرع في الحاضر والمستقبل ويفرض له عقابا ، فمهما كان السلوك لا يعتبر جريمة ما لم يجرمه المشرع فيجب مراعات أن جرائم الإعتداء على النظام المعلوماتي هي محصورة في النموذج الأمني ذي الأبعاد الثلاثة (سرية المعلومات ، سلامة المعلومات ، وجود و وفرة المعلومات) ، فهذه الجرائم لها صور متعددة تختلف بإختلاف الهدف المباشر في الجريمة ، بحيث أنها تنطوي على أنماط عديدة من السلوك الإجرامي ، وبالتالي تقتصر على كل فعل عمدي يتوصل فيه الجاني بغير وجه حق إلى نظام معلوماتي يتم الدخول إليه وترتب على الفعل الغاء أو حذف أو تدمير أو افشاء أو اتلاف أو تغيير أو اعادة نشر بيانات أو معلومات...الخ من صور الجرئم المنصوص عليها وفق قانون العقوبات.

4- أنه من حيث صور وقوع هذه الجرائم فهي تشمل جميع صور الإعتداء (الحالية والمستقبلية) على المعلومات أو البيانات الإلكترونية ضمن بيئة إلكترونية. وبناء على ذلك نستبعد من نطاق هذه الجرائم جميع صور السلوك التي تتعلق بالمكونات المادية للكمبيوتر أو التي تتعلق بالمعلومات أو البيانات في صورتها المادية ، لأنها تخضع للنصوص التقليدية الخاصة بالجرائم التقليدية من دون أن تثير أية مشكلة.

5- ومن ناحية أخرى يجب توضيح خصوصية هذه الجريمة بحيث يبدوا واضحا الدور الذي تقوم به وسيلة تقنية المعلومات الحديثة في ارتكاب الجريمة ، ولا يعني ذلك في تقديرنا أن يصل هذا الدور إلى

الحد الذي لا يمكن أن تتم الجريمة بدونه بل يكفي أن تسهل ارتكاب الجريمة ، أي أن يكون لها دور في اتمامها على النحو الذي تمت فيه.

و بناءا على ما سبق نجد أن المشرع الجنائي الجزائري قد تبنى تعريفا لجرائم الإعتداء على النظام المعلوماتي و ذلك بموجب الفقرة أ من المادة الثانية من الفصل الأول المعنون بالأحكام العامة فيما تعلق بالمصطلحات من القانون رقم (04/09)[1] " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة اخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الإتصالات الإلكترونية ".

الفرع الثاني : النظام المعلوماتي (البيئة الإلكترونية للمعلومات) محل الأمن من الإعتداء عليه

المعلومات الإلكترونية تشمل جميع المعلومات التي تمت معالجتها من نصوص أو صور أو أصوات أو رموز أو برامج ، و مهما كانت حالتها سواء معلومات مدخلة (معطيات) ، معلومات معالجة ، مخزنة عن طريق وجود ما يصطلح عليه بنظام المعلوماتية أو نظام المعالجة الآلية للمعطيات الذي يسمح بنقلها و تداولها أو يجعلها في حالة سكون هذا النظام الذي يتكون من مكونات أساسية . لهذا فإن دراسة النظام المعلوماتي يشكل أساسية في بحثنا كي نفهم الطبيعة الخاصة للجريمة المعلوماتية بحيث يعتبر بيئة لتواجد المعلومات الإلكترونية فهو محل حماية من السلوكات الإجرامية و حمايته من حماية تلك المعلومات المتواجدة فيه بل انها تمثل أصل الحماية و الأمن من أي إعتداء قد تتعرض له .

أولا : تعريف النظام المعلوماتي

نظام المعلومات Information System هو عبارة عن آلية و إجراءات منظمة تسمح بتجميع و تصنيف ، و فرز المعطيات و معالجتها ، و من ثمّ تحويلها إلى معلومات يسترجعها و يستخدمها الإنسان عند حاجته لها ، ليتمكن من إنجاز عمل أو إتخاذ قرار أو القيام بأية وظيفة ، عن طريق المعرفة التي سيتحصل عليها من المعلومات المسترجعة من النظام .

و لقد عرفه قانون الأنسترال النموذجي بشأن التجارة الإلكترونية بأنه" النظام الذي يستخدم لإنشاء رسائل البيانات أو إرسالها أو إستلامها أو تخزينها أو لتجهيزها على أي وجه آخر"

[1] القانون رقم (04/09) ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها ، المؤرخ في 05 غشت 2009، الجريدة رسمية ، العدد 47 ، ص (05)

في حين عرفته الإتفاقية الدولية الخاصة بالإجرام المعلوماتي المبرمة ببودابست من خلال المادة الأولى في فقرتها –أ– منها بأنه" أي جهاز أو مجموعة الأجهزة المتصلة ببعضها البعض أو التي ذات صلة بذلك ، و يقوم أحدها أو أكثر من واحد منها ، تبعا للبرنامج ، بعمل معالجة آلية للبيانات" مع العلم انها قد أطلقت عليه تسمية منظومة الكمبيوتر[1].

في حين نجد أن المشرع الجزائري قد عرفه بموجب المادة الثانية في فقرتها –ب– من القانون رقم (04/09)بأنه "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

الملاحظ على التعريفات السابقة أنها لم تحدد العناصر المكونة للنظام و إكتفت بذكر عنصر عملية المعالجة الآلية بإعتبارها تنطوي على مراحل سابقة و لاحقة (الإدخال ، التخزين ، النقل ...الخ) ، و هذا ما نلمسه من خلال إستعمال التعريفات السابقة الذكر لمصطلحي (...المتصلة....) و (...المرتبطة...) الذين يفسران أن هناك مراحل و مكونات للمعالجة الآلية للمعطيات كونها مسألة تقنية و فنية قد يقوم بها جهاز واحد أو مجموعة متضافرة و متشابكة مع بعضها البعض و هو المقصود بالإتصال و الإرتباط هنا.

ثانيا : مكونات النظام المعلوماتي

هو نظام يعتمد على الأفراد الذين يطلق عليهم العنصر البشري و الحاسب الآلي الذي يشمل على المكونات المادية أو مجموعة الأجهزة Hardware، و المكونات المنطقية أو البرمجية(التعليمات أو الأوامر) Software للحاسوب في معالجة المعطيات و إخراج المعلومات من خلال النشاط الذي يقوم به ، هذا بالإضافة إلى شبكة المعلومات ، و سنستعرضها وفق ما يلي:

أ – **العنصر البشري** : الذي يلعب دورا ضروريا و هاما في هذا النظام للقيام بالعمليات و الإجراءات فبدونه لا يستطيع النظام المعلوماتي العمل في جميع مراحله المختلفة فهو حلقة أساسية في مكونان النظام المعلوماتي و من مكونات العنصر البشري نجد المستخدمين النهائيين و الإختصاصيين الفنيين المسؤولين عن تشغيل و إدارة نظم المعلومات فنيا و منهم محللو النظم و مطورو البرمجيات و مشغلو النظام و مهندسو الصيانة و الإتصالات ....الخ.

[1] أسامة أحمد المناعسة وآخرون ، جرائم الحاسب الآلي والأنترنت ، ط1 ، دار وائل للطباعة والنشر ، عمان ، 2001 ، ص 77 و 78.

ب – الحاسب الآلي : يعرّف الحاسب الآلي بأنه "عبارة عن جهاز إلكتروني مصنوع من مكونات يتم ربطها و توجيهها بإستخدام أوامر خاصة لمعالجة و إدارة المعلومات بطريقة ما ، و ذلك بتنفيذ ثلاثة عمليات أساسية هي : إستقبال المعطيات المدخلة إليه (الحصول على الحقائق المجردة) ، و معالجة المعطيات إلى معلومات (إجراء الحسابات و المقارنات و معالجة المدخلات) ، و إظهار المعلومات المخرجة (الحصول على النتائج)". [1]

و يمتاز الحاسوب بعدة خصائص و مميزات جعلت منه أداة رئيسية في حياتنا المعاصرة نوجزها وفق الآتي ذكره :

- السرعة في معالجة المعطيات و أداء الوظائف و القيام بالعمليات الحسابية فالحاسوب يقوم بوظائفه بسرعة مذهلة مقارنة بالبشر ، وهي ميزة وفرت على الإنسان الكثير من الوقت .
- تخزين المعلومات و إستعادتها فالحاسوب يتمتع بقابليته لتخزين كمية كبيرة جدا من المعلومات و البيانات التي يمكن إستعادتها و الرجوع إليها للإستفادة منها في أي وقت يحتاج إليها الإنسان و تبقى هذه المعلومات مخزنة لفترة طويلة جدا دون أن يحدث لها أي تغيير .
- دقته في إستخراج النتائج من المعطيات المقدمة إليه لتكوين المعلومات النهائية .
- قابليته للبرمجة فتصميمه مبني على إمكانية أدائه لوظائف لا حدود لها و ذلك عن طريق البرامج التي يمكن تطويرها من أجل تحسين الأداء الوظيفي للحاسوب .
- إمكانية التعامل عن بعد و من أي مكان في العالم عن طريق وسائل الإتصال السلكية و اللاسلكية و هذا بما يعرف بشبكة المعلوماتية .

ج – المعلومات الإلكترونية

المعلومات لغة جمع معلومة و هي مشتقة من كلمة "علم" و دلالتها تتمحور بوجه عام حول المعرفة التي يمكن نقلها و إكتسابها ، علمت الشيء أعلمه أي عرفته ، و أعلم فلان الخبر أي أخبره به ، و أعلم فلان الأمر حاصلا أي جعله يعلمه ، و العلم نقيض للجهل ، و يقارب معنى المعلومة في اللغة الفرنسية مصطلح Information الدالة على عملية الإتصال التي تستهدف نقل و توصيل إشارة أو رسالة أو الإعلام عنها و إتخاذ وظيفتها في نقل المعارف Trransfert de Connaissances ، أما في اللغة

[1] طارق ابراهيم الدسوقي عطية ، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية) ، دار الجامعة الجديدة ، الإسكندرية 2009 ، ص 159.

الإنجليزية فنجد مصطلح Informatio اللاتينية الأصل و ترجمتها للعربية تدل على شيء قابل للإبلاغ و التوضيح أو على عملية الإبلاغ أو النقل و التوصيل للفكرة إلى الغير .

أمّا إصطلاحا فقد تعددت التعاريف للمعلومات من طرف باحثين من تخصصات و ثقافات مختلفة حتى يكاد يستحيل إدراك المعنى المراد منها و في هذا يرى البعض أنها كالجاذبية و الكهرباء لا نستطيع وصفها بدقة ، و لكننا نعرف كيفية عملها . و ما يهمننا هنا هي التعريفات الدائرة حول المعلومة المتخذة لشكل يجعلها قابلة للتوصيل إلى الغير بإعتبارها محل التأمين من الإعتداء عليها ، و التي نذكر بعضا منها وفق مايلي : [1]

1- الشروط الخاصة بالمعلومات الإلكترونية :

كون المعلومات الإلكترونية لها قيمة بوصفها نتاج نشاط إنساني ، فهذا يجعلنا نحدد شروطها كي تكون محل الحماية ضمانا لحقوق أصحابها و هذه الشروط نوجزها في العنصرين التاليين :

- **التحديد و الإبتكار (Precise et Inventive):** كي نقول عن المعلومات الإلكترونية أنها موجودة يجب أن تكون محددة ، فالمعلومات لابد أن تأخذ شكلا معينا داخل النظام المعلوماتي ، و هذا الشكل هو المحدد لها ، و التحديد هنا يفرض نفسه ، و بإنعدامه تزول القيمة الحقيقية للمعلومات ، وفي هذا قال الأستاذ كاتالا(Gatala) "أن المعلومة قبل كل شيء تعبير و صياغة مخصصة من أجل تبليغ رسالة ، و يكون هذا التبليغ عن طريق علامات أو إشارات مختارة لكي تحمل الرسالة إلى الغير" ،و من هنا و بإعتار المعلومة فكرة للتبليغ فهذا يفترض فيها أن تكون محددة **(Precise)** ، ذلك أن التحديد بدوره يعتبر أمرا مطلوبا في مجال الحماية القانونية لانه يحصر المعلومة في دائرة خاصة .

و من جانب آخر يجب أن تكون المعلومات مبتكرة **(Inventive)** ومعناه أن تكون المعلومة غير شائعة من قبل يسهل الوصول إليها من الكافة و بدونها لا تعد معلومة بالمعنى الفني الدقيق و تبعا لذلك فإن إستخدامها دون تدخل مصدرها يمثل إنتهاكا للحق في المعلومات و حالتها التقنية هي التي وضعها في متناول الناس المستفدين منها لكن هذا لا ينفي الحقوق الناشئة عنها . [2]

---

[1] محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت ، ط2 ، دار النهضة العربية ، القاهرة ، 2009 ، ص 35.

[2] نسرين عبد الحميد نبيه ، الجريمة المعلوماتية والمجرم المعلوماتي ، منشأة المعارف ، الغسكندرية ، 2008 ، ص 50.

- **الجدة(Nouveauté) و الإستئثار(Exclusivité)** : الجدة هنا يقصد بها أن لا يكون قد سبق و أن وضع ذات المعلومة و التعريف بها ، ذلك أن المعلومة يجب أن تعبر عن شخصية من أوجدها و إبتدعها ، و إن لم يتحقق هذا تكون مجرد أفكار لا تستوجب الحماية ، و مما يجب ذكره أن الجدة يطلق عليها البعض مصطلح السرية (La Confidentialité) .

و على كل بالنسبة للمصطلحين فالمقصود منهما واحد ، و هذا يمثل شرط لازم لحصر حركة المعلومات في دائرة محددة من الأشخاص ، فلا يمكن تصور الحماية لها بدون وجود هذا الشرط لأن المعلومات غير المحاطة به هي قابلة للتداول و من ثم بمنأى عن أي حيازة كالمعلومات المتعلقة بددرجة الحرارة في لحظة معينة أو الزلزال أو الفيضن الذي يظرب منطقة معينة فهي معلومات قابلة للنقل بسهولة بين كل الأشخاص و بسبب حرية تداولها المتعارضة مع الجدة أو السرية لا يمكن إعتبارها من قبيل المعلومات محل الحماية القانونية ، ففي الواقع المعلومات تكتسب وصفها إما بالنظر لطبيعتها كإكتشاف شيء جديد كان مجهولا من قبل أو بالنظر إلى إرادة الشخص كإكتشاف مجال حديث لتيير الإدارة بواسطة رئيس شركة ما و إرادته بالإحتفاظ بسريته أو بالنظر إلى الأمرين معا كما هو الحال بالنسبة للرقم السري لبطاقة الإئتمان .

2- أنواع المعلومات الإلكترونية :

يمكن أن تظهر المعلومات في أنواع مختلفة و متعددة و هذه الأنواع يمكننا حصرها وفق الطوائف التالية

- **المعلومات الإسمية Informations Nomintives** :و تنقسم بدورها إلى معلومات شخصية و أخرى موضوعية :

* **المعلومات الشخصية Informations Subjectives** :و يقصد بها تلك المعلومات المرتبطة بشخص المخاطب بها مثل إسمه ، موطنه ، صحيفة السوابق القضائية الخاصة به ، و حالته الإجتماعية فهي المعلومات اللصيقة بشخص صاحبها التي لا يجوز للغير الإطلاع عليها إلا بموافقة صاحبها شخصيا أو بأمر من السلطات المختصة .

* **المعلومات الموضوعية Informations Obgectives** : و هي تلك المعلومات المنسوبة إلى شخص قصد الإدلاء برأيه الشخصي فيها و التي تكون في شكل مقالات و الملفات الإدارية للعاملين لدى الجهات الإدارية إذن هي معلومات موجهة إلى الغير بحسب الأصل .

– **المعلومات الخاصة بالمصنفات الفكرية** :وهي عبارة عن معلومات متمثلة في مصنفات فكرية تخضع لقوانين الملكية الفكرية و التي قد تكون مصنفات أدبية أو فنية أو مصنفات صناعية .

– **المعلومات المباحة** :و يقصد بها المعلومات المتاح الحصول عليها للجميع لأنها بدون مالك و مثالها تقارير البورصة اليومية و النشرات الجوية ...الخ ، فإذا تم تجميعها بغرض معالجتها لتشغيلها على الكمبيوتر و إسترجاعها بقصد خلق معلومات جديدة و عليه هذه الطائفة ممكن ان نجدها في صورتين هي

* **المعلومات المعالجة Informations Traités** :هي المعلومات المعالجة للتشغيل على جهاز الكمبيوتر بقصد تخزينها و حفظها فيه بقصد إسترجاعها وقت الحاجة إليها .

***المعلومات المتحصلة Informations Résultats** : و هي تلك المعلومات الناتجة عن معالجة مجموعة معلومات و التي تقرر حق ملكيتها طبقا لقواعد حيازة المال المنقول . [1]

– **المعلومات على أساس صورتها التي تظهر بها :**

* **المعلومات المتحركة و الساكنة** :المعلومات الساكنة هي معلومات تكون في شكل معطيات أولية أو نتائج نهائية متواجدة داخل جهاز الحاسوب أما المتحركة فهي تلك المتنقلة و المتداوللة عبر شبكات الإتصال من حاسب آلي إلى آخر .

* **المعلومات المشفرة و غير المشفرة** : و يقصد بها المعلومات المحجوبة عن التداول العام عن طريق برنامج لمنعها عن الغير ممن ليس لهم الحق في الإطلاع عليها و التعامل معها ما لم يصرح لهم بذلك فالوصول إلى المعلومات المشفرة يكون أصعب بكثير من تلك غير المشفرة فالأمر يتطلب الحصول على الشفرة و الإذن بإستخدامها .

د – شبكة المعلومات (الأنترنت) مصطلح أنترنت إنجليزي الأصل مختصر و مركب من شقين الأول(Inter) يمثل الحروف الأولى لكلمة (International و ترجمتها دولي) ، أما الشق الثاني (Net)كذلك مأخوذ من الحروف الأولى لكلمة (Network و ترجمتها شبكة عمل) ، و بجمع المختصرات يتكون المصطلح الذي يعني الشبكة العالمية للمعلومات المشار إليها بالأحرف (w.w.w) ، و التي تعني (word wid web) أي الشبكة الدولية الإلكترونية المتعددة الأبعاد و الخدمات .

[1] نسرين عبد الحميد نبيه ، المرجع السابق، ص 52.

فالأنترنت تعتبر وسيلة تواصل و تبادل للمعلومات فهي نظام للتخاطب بين الحواسيب تسمح بنقل الملفات و البرامج و البيانات ، التي تكون مكتوبة أو أصوات أو صور المشكلة في مجموعها للمعلومات الإلكترونية بين حاسوب لآخر أو لحواسيب متعددة في أماكن متباعدة جغرافيا و في زمن ضئيل جدا من أجل الحصول و إستبيان المعلومات المتوفرة فيها و تبادل تلك المعلومات مهما كان حجمها أو بعد أو طريقة الإرتباط فهي تساعد على ربط الإتصالات بين الأفراد و الجماعات لتبادل الخبرات و إنجاز المهام عن بعد أو الإثراء و النقد و ذلك إعتمادا على توجيه المعلومات من المرسل إلى المستقبل .[1]

المطلب الثاني : خصوصية جرائم الإعتداء على النظام المعلوماتي

خصوصية تلك الجرائم تتعدد من حيث مميزاتها و من حيث مرتكبيها بالإضافة الى تميزها من حيث أخطارها الناجمة عنها هو ما سنعالجه وفق الفروع الثلاثة التاليين :

الفرع الأول : خصوصية جرائم الإعتداء على النظام المعلوماتي من حيث مميزاتها

تتميز هذه الجرائم عن الجرائم التقليدية بمجموعة من الخصائص الفريدة و المتميزة ، بحيث تكمن أهمية تبيان تلك الخصائص في تحديد طبيعتها الخاصة التي تميزها عن غيرها من الجرائم كما أنها تحدد آثارها التي تنسحب على التحقيق فيها و على أطرافها ، وهي كالآتي :

أولا : أنها متعدية أو عابرة للحدود: بالنظر لإرتباط المجتمع المعلوماتي بالشبكة المعلوماتية (خاصة شبكة الأنترنت) التي تعبر الأزمنة والأماكن من دون أن تخضع في ذلك للحراسة ونقاط التفتيش، فقد ترتب على ذلك عدم اعتراف هذا المجتمع بالحدود الجغرافية للدول.[2] وهذه الخاصية مكنت مجرمي المعلوماتية من ارتكاب جرائم عن بعد ، فهناك في الغالب تباعد كبير بين الجاني والمجني عليه في هذه الجرائم، وبالتالي بين الفعل الإجرامي والنتيجة الجرمية حيث تتحقق الأخيرة في الغالب خارج حدود الدولة التي وقع فيها الأول.

ثانيا : سهلة الإركاب : فهذه الجرائم يرتكبها الجاني في الغالب لوحده من دون ان يحتاج في ذلك للإستعانة بشخص أو أشخاص آخرين ، بعكس الجرائم التقليدية التي يحتاج الجاني في ارتكابها في الغالب لمثل هذه الإستعانة ، فالجرم المعلوماتي قادر على تنفيذ مخططه الإجرامي لوحده وهو جالس أمام

---

[1] محمد عبيد الكعبي ، المرجع السابق، ص 42.

[2] عبد الفتاح بيومي حجازي ، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي ، دار الكتب القانونية ، مصر ، المحلة الكبرى ، 2007 ، ص 25

الكمبيوتر في منزله أو مكتبه أو مقهى للأنترنت ضد ضحية موجودة في دولة أخرى تبعد عنه آلاف الأميال .

ثالثا : مكلفة للضحايا : فإذا كانت هذه الجرائم مربحة للجناة فإنها في ذات الوقت مكلفة للضحايا حيث أنها تتسبب عموما في الحاق أضرار مالية بليغة بضحاياها مقارنة بما يمكن أن تتسبب فيه الجرائم التقليدية. فبينما أن معدل خسائر البنوك من الجرائم التقليدية كالسطو المسلح هي (10000) دولار ، فإن معدل خسائرها المالية نتيجة هذه الجرائم المستحدثة تتراوح ما بين (100000) و (500000) دولار أمريكي . لذا فإن لهذه الجرائم خطورة كبيرة في اقتصاديات الدول ،

رابعا : قليلة المخاطرة : فنسبة مخاطرة الجاني الناجمة عن ارتكاب مثل هذه الجرائم ، قليلة نسبيا ، بالمقارنة مع تلك الناجمة عن ارتكابه للجرائم التقليدية ، فهو غير معرض لخطر المواجهة المباشرة مع المجني عليه او غيره ولا لخطر المواجهة المسلحة من الشرطة ، كما وأن نسبة اكتشافه وتعرضه للإدعاء في مثل هذه الجرائم هي فقط 1 من 22000 حالة. وذلك بالنظر إلى صعوبة تتبع اثره على شبكة الأنترنت ، خصوصا وان هذه الجرائم لا تكتشف في الغالب إلا بعد مرور زمن طويل على ارتكابها ، وكل هذا بدوره يشكل عائقا آخر أمام اكتشاف هذه الجرائم والتحري والتحقيق فيها.

خامسا : خفية عن الأنظار : هذه الجرائم ترتكب بخفة وفي خفة شديدة ، بحيث أنها ترتكب في العالب من دون أن يرى طرفا الجريمة (المجرم المعلوماتي والضحية المعلوماتية) بعضها البعض ، فهي نادرا ؤما تكتشف مباشرة من الضحية أو غيره ، وتقع في الغالب من دون أن يدرك المجني عليه نفسه بوقوعه ضحية للجريمة المرتكبة. ولعل مما يزيد من خفاء هذه الجرائم هو أن أغلب ضحاياها لا يتوسلون ببرامج وأنظمة الحماية الفنية لحماية انظمة المعلوماتية غالبا ما يتوسل في ارتكاب هذه الجرائم ببرامج وتقنيات تمكنهم من العمل في الخفاء من اختراق جدران الحماية الأمنية تلك ، وكل هذا بدوره يصعب في امكانية اكتشاف الضحايا لهذه الجرائم والتبليغ عنها ، وهذا بدوره يشكل عائقا آخر أمام اكتشاف هذه الجرائم والتحقيق فيها. . [1]

سادسا : وقوعها في بيئة الكترونية : فهذه الجرائم تقع في بيئة الكترونية ، وأن الأدلة التي تخلفها تكون في الغالب أدلة الكترونية ، وكل هذا بدوره يترتب عليه جملة من المشاكل والصعوبات التي تعوق

[1] محمود أحمد عبابنة ، جرائم الحاسوب وابعادها الدولية ، دار الثقافة ، عمان 2005 ، ص 15.

اكتشاف هذه الجرائم والتحقيق فيها ، على أننا سنؤجل الكلام عن هذه المشاكل والصعوبات للفصل الثاني لدى تطرقنا لصعوبات اكتشاف الجرائم المعلوماتية الراجعة إلى الجريمة المعلوماتية في ذاتها.

سابعا : أنها ترتكب من خلال الوسائل التقنية : فهذه الجرائم تقع في بيئة الكترونية يستلزم التعامل معها استعانة الجاني بوسائل أجهزة تقنية تتمثل في الغالب بالكمبيوتر وملحقاته الأساسية من مثل أجهزة الطبع والمسح الضوئي وكذلك أجهزة الربط بالشبكات وغيرها. ولكن مع ذلك يمكن ارتكاب مثل هذه الجرائم أيضا من خلال وسائل تقنية أخرى كأجهزة الهاتف (المحمول) المتطورة، وغيرها من الأجهزة والتقنيات التي يمكن أن تظهر إلى الوجود في أي لحظة.

وهذه الخاصية بدورها تصعب من مهمة اكتشاف هذه الجرائم والتحقيق فيها إذا ما أخذنا بنظر الإعتبار أن مجرمي المعلوماتية غالبا ما يكونون على دراية واسعة بكيفية التوسل بهذه التقنيات بعكس جهات الإستدلال والتحقيق ، خصوصا التقليدية منها ، التي تكون في الغالب جاهلة بكيفية التعامل معها. [1]

الفرع الثاني: خصوصية جرائم الإعتداء على النظام المعلوماتي من حيث مرتكبيها

ما من شك أن المدى الزمني لنشأة وتطور العلوم الجنائية وما نتج في نطاقها من دراسات وتحديدا في ميدان علم الإجرام أمكن في ظلها بلورة سمات عامة للمجريمين عموما ، وسمات خاصة يمكن استظهارها لطائفة معينة من المجرمين تبعا للجرائم التي يرتكبونها ، فعلى سبيل المثال : افرزت الجرائم الاقتصادية ما يعرف بإجرام ذوي الياقات البيضاء ، وبالتالي كان طبيعيا ان تحمل ظاهرة الاجرام عبر تكنولوجيا المعلومات الحديثة في جنباتها والدة طائفة جديدة من المجرمين ، اسطلح جانب من الفقه على تسمية من ينتمي إليها بالمجرم المعلوماتي.

ومن جهتنا يمكننا القول أن المجرم المعلوماتي "تعبير " ينطوي على قدر من التجاوز في القول ، فالصحيح أنه لا يوجد نموذج محدد للمجرم المعلوماتي ، بل هناك عدة نماذج للمجرمين قد يستخدمون نظام المعلومات الإلكتروني (أيا كان الجهاز الذي يحتوي مزايا هذا النظام) في جرائمهم ، وقد يوقومون بأفعال جرمية ضد نظام المعلومات الإلكتروني نفسه ، غهناك من يقتل أو يسرق عن طريق الإستعانة بالوسيط الإلكتروني ، وهناك من يعتدي على سمعة الآخرين أو على حرمة حياتهم الخاصة أو على الاخلاق والقيم عبر الوسيط الالكتروني ، وهناك من ريرتكب جريمة التزوير عن طريق الاستعانة بالوسيط الإلكتروني وهناك من يرتكب جريمة تزوير عن طريق الاستعانة بنظام المعلومات الالكتروني ، وهكذا

[1] محمود أحمد عبابنة ، جرائم الحاسوب وابعادها الدولية ، دار الثقافة ، عمان 2005 ، ص 15.

الأمر بالنسبة لصور أخرى من الجرائم ، وبالتالي فإن تعدد جرائم تكنولوجيا المعلومات الحديثة وتنوعها التي تغطي صورا عديدة من الانشطة ، أدى إلى عدم اتضاح الصورة بشكل جلي في شأن تحديد سمات مرتكبيها ، بحيث اختلف الباحثون في هذا الخصوص ، كما اختلفوا أيضا فيما اذا كان المجرم المعلوماتي ينتمي إلى الإجرام الطبيعي (المجرم بطبيعته أو ما يسمى بذي الياقات الزرقاء) أو إلى الاجرام الاصطناعي المكتسب (المجرم النظيف أو ما يسمى بذي الياقة البيضاء).[1]

الفرع الثالث : خصوصية جرائم الإعتداء على النظام المعلوماتي من حيث اخطارها

فيما يلي نسلط الضوء على مدى خطورة جرائم المعلوماتية من حيث الكم والنوع على مجالات الحياة الرئيسية (الإقتصادية والإجتماعية والنفسية والصحية والعسكرية والأمنية والسياسيةو أخيرا الجوانب الإدارية) لذا سنتناول هذا الأمر في خمسة نقاط نقاط ، ندرس في الأول منها الاخطار الإقتصادية لجرائم المعلوماتية فيما نبحث في النقطة الثانية أخطارها الاجتماعية في حين نناقش في النقطة الثالثة اخطارها النفسية والصحية واخيرا نتطرق في الرابعة إلى اخطارها العسكرية والأمنية والسياسية أما النقطة الأخيرة فمخصصة للأخطار في الجانب الإداري .

أولا : أخطارها الاقتصادية

للجرائم المعلوماتية اخطار لا توصف من الناحية الإقتصادية ، لوقوعها في معظم الأحوال على معلومات وبرامج ذات قيمة اقتصادية عالية ، سواء في ذاتها أو لإرتباطها بأموال قيمة ، مما يؤدي في الغالب إلى خسائر مالية فادحة ، إذ أنه وبمجرد حصول المجرم المعلوماتي على الوقت والوسيلة الكافيتين لتنفيذ جريمته فإنه قد لا يتردد في القضاء على أكبر المؤسسات الإقتصادية في العالم.[2] فالمجرم المعلوماتي يختلف عن المجرم العادي ، من حيث أنه يستخدم العقل والتقنية في عمليته الإجرامية بدلا من الأسلحة ليستولي في الغالب على مبالغ طائلة تفوق بكثير عما يستولي عليه المجرم الإعتيادي ، فمثلا أن معدل ما يسرق اللص العادي في الولايات المتحدة الامريكية هو ما دون الـ (10) آلاف دولار ، بينما أن معدل ما يسرق المجرم المعلوماتي هو حوالي (45) الف دولار.[3] وتعتبرالولايات المتحدة الامريكية الدولة الأكثر

---

[1] غنام محمد غنام – عدم ملاءمة القواعد التقليدية لقانون العقوبات لمكافحة جرائم الكمبيوتر – بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت ، كلية الشريعة والقانون ، جامعة الإمارات ، مايو ، 2004 ، ص 02.

[2] محمد حماد مرهج الهيتي ، التكنولوجيا الحديثة والقانون الجنائي ، دار الثقافة ، عمان ، 2004.

[3] قحطان محمد صالح الجميلي ، آلة العصر (الكمبيوتر) ، منشورات مكتبة الشعب ، بغداد ، 1985 ، ص 29.

تضررا من الجرائم المعلوماتية من الناحية الاقتصادية ، حيث أنها تخسر سنويا ما مقداره (67.2) مليار دولار من جراء هذه الجرائم.

أما على صعيد الدول الأخرى ، فإنه قد سبق وأن قدرت دراسة أجريت في بريطانيا عام 1990 حجم الخسائر المالية الناجمة عن هذه الجرائم في ذلك البلد بـ (400) مليون جنيه استرليني سنويا ، وفي فرنسا قدرت الخسائر المالية الناجمة عن هذه الجرائم فيها بـ (12.720) مليار فرنك فرنسي سنويا ، وذلك بمقتضى دراسة قامت بها الجمعية الفرنسية لأمن المعلومات عام 1996. واما على صعيد الدول العربيه فإنه وبمقتضى دراسة أجرتها منظمة (Softwar Alliance Business) في الشرق الأوسط تبين أن مجموع الخسائر المالية الناجمة عن هذه الجرائم في كل من المملكة العربية السعودية والإمارات العربية المتحدة معا تقدر بـ (30) مليون دولار سنويا ، وفي لبنان بـ (1.400.000) دولار سنويا.

ثانيا : أخطارها الاجتماعية

ان خطورة جرائم المعلوماتية لا تتوقف عند حدود الإقتصاد بل تتخطاها لتشمل أيضا النواحي الإجتماعية للأفراد والمجتمعات وكالآتي :

1- المساس بالآداب والأخلاق العامة للمجتمع من خلال نشر الصور واللقطات والأفلام الجنسية (الإباحية) على شبكة الأنترنت، فعالمنا المعاصر يعيش ثورة جنسية طاغية ، تجاوزت كل الحدود والقيود ، بحيث أصبحت تشكل تهديدا كبيرا للمجتمعات البشرية ، فهي كما يقول (جيمس ريستون) الصحفي في جريدة نيويورك تايمز سيكون في النهاية أشد فتكا من الطاقة النووية في خطورتها على المجتمعات البشرية "، وأبرز سبب لهذه الثورة هو ظهور شبكة الأنترنت التي ربطت العالم بأسره مع بعضه البعض ، وجعلته (بالأخص أمريكا وأروبا) يعيش جنونا جنسيا محموما في عالم الأزياء والافلام والصور الجنسية الفاضحة ، حتى أمسى الجنس هو الشغل الشاغل لعقول أغلب أفراد المجتمع البشري. فتمثل هذه الشبكة واحدة من أكثر الوسائل فعالية وجاذبية لصناعة ونشر الإباحية وبشكل يقتحم على الجميع بيوتهم ومكاتبهم ، ولذلك فقد لجأ مروجوا تجارة الجنس إليها بغية الحصول على ارباح طائلة بأقل قدر ممكن

من المخاطر ، حتى باتت توجد على هذه الشبكة اليوم طوفان من هذه الصور والأفلام ، بشكل لم يسبق له مثيل في تاريخ البشرية.[1]

2- المساس بخصوصات حياة الأفراد ، نتيجة اختراق اجهزة الكمبيوتر واختراق البريد الإلكتروني وغيرها ، فمثل هذه الجرائم تشكل بلا شك تهديدا جسميا لخصوصات وأسرار حياة الأفراد الشخصية والعائلية ، وسواء أحدث الاختراق من قبل الهاكرز أو الكراكرز. أم من قبل جهات حكومية ، فإنها بلا شك تعتبر خرقا لأحد المبادئ الدستورية الراسخة ، ألا وهي مبدأ حق الانسان في الخصوصية.

3- المساس بسمعة وشرف وإعتبار الأفراد ، عن طريق نشر صور مشينة لسمعتهم وشرفهم ، سواء اكانت تلك الصور حقيقية أم مزيفة ومعدلة من خلال برامج تعديل الصور أو عن طريق السب والقذف والتشهير عبر الأنترنت ونشر الأقوال والتهم الملفقة ضد الافراد وبالأخص الذين يمثلون رموزا دينية أو سياسية في مجتمعهم.[2]وكثيرا ما تتسبب مثل هذه الجرائم في حدوث نتائج خطيرة كارثية تهدد استقرار الاسر والمجتمع ، فكم هي حلالت الطلاق والضرب والقتل التي وقعت على ضحايا أبرياء نتيجة مثل هذه التهم الملفقة وبالأخص قذف النساء بتهمة الزنا .

ثالثا : أخطارها النفسية والصحية

ان للجرائم عموما أثارها السلبية على نفسية الضحاليا ، إلا أن الآثار السليبة التي توقعها الجرائم المعلوماتية على نفسية ضحاياها تكون في الغالب أشد وقعا من تلك التي توقعها الجرائم التقليدية ، وبصورة عامة يمكن اجمال هذه الاثار بما يلي :

1- ان المجني عليه في مثل هذه الجرائم ، يشعر بصورة مستمرة بعدم الارتياح النفسي لشعوره الدائم بضياع حقوقه وعدم امكانية استرجاعها ، لان الجاني في الغالب يكون مجهولا ، ويصعب اكتشافه ، كما ويشعر دوما بعدم الأمان والطمأنينة النفسية لا في حاضره ولا مستقبله ، حيث يشعر دوما بأنه معرض

[1] حسن طاهر داود ، جرائم نظم المعلومات ، الطبعة الأولى ، مركز الدراسات والبحوث ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2000 ، ص 93.

[2] علي بن عبد الله العسيري ، الآثار الأمنية لإستخدام الشاب للأنترنت ، ط1 ، مركز الدراسات والبحوث ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2004 ، ص 47-48.

لخطر هذه الجرائم الخفية ، وأن خصوصياه واسرار حياته الشخصية والعائلية ومستوراته عموما معرضة للخطر الافشاء والانكشاف للملايين من مستخدمي الشبكة العنكبوتية

2- إن اغلب ضحايا الجرائم المعلوماتية وبالاخص جرائم المواقع الإباحية يعانون في كثير من الأحيان من الإدمان على ارتياد هذه المواقع ، وبلا شك فإن مثل هذا الادمان لا يقل خطرا على الادمان على أقوى أنواع المخدرات ، بل انه قد يكون أشد منه خطرا وفتكا.

3- ان خطورة هذه الجرائم ، لا تقف عند الحدود النفسية ، بل تتعداها لتنتج عنها أخطار صحية قد تؤدي أحيانا بحياة الأبرياء ، ولعل أبرز مثال على ذلك هو ما حدث وان قام به أحد المجرمين المعلوماتيين (الكراكرز) لدى إختراق النظام المعلوماتي لإحدى المستشفيات في الولايات المتحدة الامريكية ، حيث أنه أقدم على العبث بملفات النظام ، مما أدى بالنتيجة إلى وفاة احد المرضى الراقدين في المستشفى

رابعا : أخطارها العسكرية والأمنية والسياسية

اذا كانت الدول فيما مضى تقاوم الجرائم التقليدية التي تقع على مصالحها العسكريةو الامنية والسياسية ، فإن عليها اليوم ان تواجه الجرائم لمعلوماتية الاكثر خطورة في هذا الصدد من اجرائم القليدية ، نظرا لصعوبة اكتشافها ، فهذه الجرائم تعتبر كالشبح بالنسبة للدول وبالأخص الدول النامية التي لا تملك ما يكفي من التقنية لمواجهتها وإكتشافها ، وأهم المرخاطر في هذه المجالات يمكن اجازها بما يلي :

1- على صعيد المخاطر العسكرية ، فإن الخطر الحقيقي لهذه الجرائم يتمثل في جرائم التجسس المعلوماتي ، حيث باتت بإمكان الكثير من الدول التي تملك التكنولوجيا ان توم بالتجسس على المواقع المنشآت العسكرية (السرية وغير السرية) للدول الأخرى من خلال أقمار صناعية وأجهزة تقنية متطورة ومعدة خصيصا لذلك ، واضحى بإمكان هذه الدول الوصول لإى معلومات ما كان ليصل إليها الجاسوس الاعتيادي إلا بطريقة مميزة.

2- على صعيد المخاطر الأمنية ، فإن بعضا من الجرائم المعلوماتية كالإرهاب الإلكتروني وجرائم غسيل الاموال عبر الانترنت وغيرها من الجرائم المنظمة امست تشكل تهديدا حقيقيا للأمن القومي للدول المعاصرة، خصوصا بعد أن أصبح هناك نوع من الإرتباط الطبيعي ما بين الجريمة المنظمة وشبكة الانترنت ، والذي هو ارتباط قابل للإزدهار والتطور يوما بعد يوم ، ذلك أن هذه الشبكة توفر للجريمة

المنظمة القنوات والاهداف في آن واحد ، وكذلك توفر لها أيضا أفظل الفرص لإستغلال هذه القنوات والاهداف ، في سبيل تحقيق أكبر قدر ممكن من الأرباح ، بأقل قدر ممكن من الخسائر والمخاطرة ، وهذا ما تربو إليه دجماعات الجريمة المنظمة دوما.[1]

خامسا: أخطارها الإدارية

لم يعد أمام أي دولة سوى الاتجاه نحو المجتمع الإلكتروني والتكنولوجيا الرقمية فقد جعلت وسائل الإتصال الحديثة العالم يشبه المدينة الواحدة في تقارب أجزائه.

ولقد أدت التقنيات الحديثة للمعلومات والاتصالات إلى إحداث تطورات هائلة في الحياة العامة سواءا على مستوى الأفراد الذين يرغبون في الحصول على خدماتهم بصورة أكثر تطورا وسرعة ودقة عالية، أو على مستوى الهيئات والمؤسسات القائمة على تقديم تلك الخدمات.

ولقد أصبح إدخال تكنولوجيا المعلومات في كافة الأعمال الحكومية هو هدف العديد من الدول التي تسعى للتقدم والرقي والتي منها الجزائر بحيث سعت إلى إستخدام تكنولوجيا المعلومات في الأجهزة الحكومية .

أدى إرتباط إستخدام تكنولوجيا المعلومات في الأجهزة الحكومية لظهور مصطلح جديد أطلق عليه الحكومة الإلكترونية الذي من خلاله تسعى الإدارة إلى تبسيط وتسهيل التعاون بينها وبين الأفراد وتوفير المعلومات بشكل متكامل وسريع للجميع لتحسين أداء الإدارة وتسهيل حصول المواطن على الخدمة بأقل تكلفة .

في وقتنا هذا طرح في ميدان الفكر مصطلح الحكومة الإلكترونية[2] الذي يشد الإنتباه باعتباره مصطلح حديث مرتبط بالمعلوماتية وتقنياتها المرتبطة بتكنولوجيا المعلومات.

فمع تطور تكنولوجيا المعلوماتية سارعت الحكومات الرشيدة إلى بحث تنفيذ نظام يغير من أسلوب تقديم وكيفية الحصول على الخدمات التي تقدمها الإدارات الحكومية والمجالس البلدية والإقليمية وأجهزة الحكم عموما بصورة أمثل تختصر الوقت والجهد والمال أيضا مع تحسين الأداء والكفاءة و الفعالية.

---

[1] عبد الله عبد الكريم عبد الله ، جرائم المعلومات والنترنت (الجرائم الإلكترونية) ، ط1 ، منشورات الحلبي الحقوقية ، بيروت ، 2007 ، ص 42.

[2] لفظ الحكومة الإلكترونية متعلق بالصفات و المعاني التي توصف بها من حيث كونها سلطة عامة وركن في الدولة او الوزارة أو الهيئة التي تقوم بتنفيذ القوانين وإدارة المرافق العامة وغير ذلك.

بحيث يرى أنصار الإتجاه العام في تعريف الحكومة الإلكترونية أنها تعني إستخدام وسائل الإتصال التكنولوجية المتنوعة والمعلومات في تسيير سبل أداء الإدارات الحكومية خدماتها العامة الإلكترونية ذات القيمة، والتواصل مع طالبي إستخدام وسائل الإتصال الإلكترونية عبر بوابة واحدة وكذلك إستخدام المعلومات بطرق تعتمد على الآلية الالكترونية.

وبعبارة أخرى فإن الحكومة الإلكترونية تشير إلى استخدام المعلومات ووسائل اتصال التكنولوجي كالشبكات المتكاملة بعيدة المدى، والانترنت والكمبيوتر من قبل الإدارات الحكومية.

وهذا يعني أن الحكومة الإلكترونية تتبنى التغيير أو التعديل في العلاقات الأساسية بين الحكومة من ناحية، ولجمهور المواطنين ورجال الأعمال من ناحية أخرى من خلال طريقتين:

المبحث الثاني: إنعكاس إستقلالية جرائم الإعتداء على النظام المعلوماتي على النصوص التشريعية التقليدية

على ضوء ما سبق و بعد أن توضحت لنا إستقلالية تلك الجرائم و تفردها عن غيرها من الجرائم نتجه الآن لتوضيح إنعكاس تلك الإستقلالية على النصوص التشريعية التقليدية إنطلاقا من المبدأ الأساسي الذي يقوم عليه القانون الجنائي و هو مبدأ الشرعية الجنائية في الشقين التجريمي و العقابي فلا يجوز القول عن أي سلوك أنه مجرم ما لم ينص المشرع الجنائي على تلك الصفة بنص صريح واضح يزيل اللبس و الغموض حيث أن تزايد مضاهر الإعتداء على نظم المعلومات و ما تحتويه من معلومات جعل القانون الجنائي يشوبه الثغرات و هو ما أطلق عليه بأزمة مبدأ الشرعية في نطاق جرائم الإعتداء على نظم المعلومات و هو ما سنتطرق إليه في المطلب الأول من هذا المبحث بينما نخصص المطلب الثاني منه لمدى عجز المواجهة الجنائية التقليدية ضد الإعتداءات على النظام المعلوماتي .

المطلب الأول : مبدأ الشرعية الجنائية و أزمته في جرائم الإعتداء على النظام المعلوماتي

لا تختلف جرائم الإعتداء على النظام المعلوماتي عن أية جريمة أخرى تقليدية مقررة عن طريق قانون العقوبات من حيث أنها تتطلب لتحقيقها الأركان المتفق على ضرورة تحقيقها في أية جريمة أخرى للتواجد على أرض الواقع ، فبالإضافة إلى ضرورة تواجد الشرط المبدئي في كل جريمة ونقصد هنا الركن الشرعي ، فإنه لابد من وجود ركن مادي ملموس يعبر عن ارادة الفاعل بشكل جلي يمكن اثباته ، ومن ثم لابد

أيضا من ركن معنوي يعبر عن ارادة مجرم تقنية المعلومات الحديثة ، فالجريمة بشكل عام ، ليست ظاهرة مادية خالصة ، قوامها الفعل وأثاره ، ولكنها كذلك كيان نفسي ، ومن ثم استقر في القانون الجنائي الحديث ذلك المبدأ الذي يقضي بأن ماديات الجريمة تنشيء مسؤولية ولا تستوجب عقاب ، ما لم تتوافر إلى جانبها العناصر النفسية التي يتطبها كيان الجريمة. [1] ،

وبلا شك ، فإن هذا المنطق يسري أيضا على الجرائم محل الدراسة ، بمعنى أنها لا تختلف عن أية جريمة يحتويها القانون العقابي ، فلابد و أن ترتكب من شخص قادر على تحمل تبعات أعماله ، فلا يسأل عن هذه الجريمة من لا يعترف لهم قانون العقوبات بهذه الصفة كالمجنون والمعتوه أو المصاب بمرض عقلي.

فالفقه يرى بأن الركن الشرعي لا يعدو كونه علاقة تربط بين ماديات الجريمة ، وشخصية الجاني ، وهذه العلاقة تتمثل في سيطرة الجاني على الفعل وآثاره ، وجوهرها الإرادة ، ومن ثم كانت ذات طبيعة نفسية ولاشك أن هناك تقسيم للجرائم بشكل عام يستند على أساس الركن المعنوي فتقسم إلى جرائم عمدية وأخرى غير عمدية ، ويعتمد هذا التقسيم على أن الفاعل في الجرائم العمدية قد قام بإقتراف فعله قاصدا ارتكاب السلوك المجرم وتحقيق النتيجة المجرمة ، بينما نجد أن الفاعل في الجريمة غير العمدية لم يقصد سوى ارتكاب السلوك دون ارادة تحقيق النتيجة المجرمة عن طريق النص الجزائي ، وإذا كان من المتصور غالبا أن لا تقع جريمة التقنية الحديثة إلا بصورة جريمة عمدية سبقها التفكير في الحصول على المعلومة أو اختراق شبكة نظام حاسب آخر من أجل الحصول على المنفعة أو تحقيق الهدف المرسوم له ، إلا أن هذا لا يعني أنها لا تحقق إلا عن طريق عمدي ، بل أنه من الممكن أيضا أن نتصور امكانية ارتكابها أيضا بشكل جريمة غير عمدية في بعض الأحوال المحتملة الحدوث.

وكون الجريمة عمدية هو الأصل إلا ما استثنى المشرع بنص على أنها غير عمدية ، فقد استقر في غالبية قوانين الجزاء تلك القاعدة التي تقضي بأنه إذا سكت الشارع عن بيان صورة الركن المعنوي في جريمة من الجرائم ، كان معنى ذلك أنه يتطلب القصد الجنائي العمدي فيها.

أما الركن المادي للجريمة فيعرف بأنه يتمثل في سلوك اجرامي معين يتطلب القانون كمناط للعقاب على هذه الجريمة ، على أن تحقق نتيجة ضارة لهذا السلوك الإجرامي كشرط بذاته يتعين قيامه حتى يعاقب

[1] – محمود نجيب حسني – النظرية العامة للقصد الجنائي (دراسة تأصيلية مقارنة في الجرائم العمدية) – الطبعة الثالثة 1988 ، – دار النهضة العربية – ص 08.

على الجريمة ، وفضلا عن ذلك يجب أن يرتبط النشاط أو السلوك الإجرامي ونتيجته الضارة بعلاقة سببية ، وهو ما يطلق عليه "الإسناد المادي"[1]،وعليه فالركن المادي في الجريمة التامة يقوم على ثلاثة عناصر هي السلوك الاجرامي الذي يقع من الجاني ، والنتيجة الضارة أو الخطورة المترتبة على هذا السلوك سواء كان مقصود أم لا ، وأخيرا علاقة السببية بين سلوك الجاني والنتيجة التي تحققت.

ويقصد بالسلوك الاجرامي (النشاط الخارجي الذي يقوم به الجاني ، ويبرز في العالم الخارجي مكونا لماديات الجريمة ومسببا لما قد يترتب عليها من ضرر أو خطر ، وسواء قصد الجاني من هذا السلوك الإجرامي تحقيق نتيجة معينة أم تحققت النتيجة دون أن تنصرف ارادته إليها". أي أن السلوك الإجرامي لابد أن يخرج الجريمة من كونها مجرد فكرة تجيش في نفس الجاني إللى فعل يضهر أثره في العالم الخارجي ويدركه الغير بإستخدام حواس الإدراك.

ويحدد السلوك الإجرامي في كل جريمة من قبل المشرع ضيقا واتساعا على نحو يمكن القاضي من تكييف السلوك الإجرامي أو فعل الجريمة ورده إلى القاعدة القانونية أو النص التجريمي الذي يحكمه، معنى ذلك أنه للعقاب على الجريمة لابد أن يتطابق السلوك الإجرامي للجاني مع ذات النموذج الإجرامي الوارد في قاعدة قانون العقوبات على نحو من الدقة والوضوح ، بحيث لا يدع مجالا لإختلاف الرأي في مضمونه.

وبالكلام عن طبيعة السلوك الإجرامي في جريمة الإعتداء على النظام المعلوماتي ، فإن هذا السلوك يرتكب عن طريق إستخدام الأساليب الفنية ، و هو الأمر الذي إقتضي تدخل القانون الجنائي لمواجهتها ، لسد الفراغ او النقص التشريعي ، حيث لا يمكن أن تبقى بدون عقاب أفعال اجرامية جديدة رغم خطورتها.

ولكن حتى يتدخل المشرع فلا مناص سوى تطبيق النصوص القائمة على قانون العقوبات ، حتى لا تترك أفعال الإعتداء دون عقاب ، ولكن حتما دونما المساس بمدأ الشرعية الجنائية ، بحيث تفسر النصوص القائمة على نحو أوسع من الذي وضعت لأجله ، كما من المتصور أيضا تطبيق النصوص القائمة في أية قوانين خاصة أخرى معمول بها ، الأمر الذي يبرر الحاجة للحماية الجنائية ، وعليه سنتعرض لمبررات الحماية من خلال التطرق لمبدأ الشرعية الجنائية (أولا) ، ثم ابراز قصور الجزاءات الجنائية التي تقررها التشريعات المدنية ذات الصلة (ثانيا). [2]

[1] رؤوف عبيد ، مبادئ القسم العام من التشريع العقابي، طبعة ثالثة ، 1966 ،دار الفكر العربي ،ص 188.

[2] أحمد عبد العزيز الألفي ، شرح قانون العقوبات (القسم العام) ، مكتبة النصر الزقازيق ،1995 ، ص 256.

أولا : مبدأ الشرعية الجنائية

أ – مقتضى مبدأ الشرعية الجنائية

من المبادئ الأساسية في اغلب التشريعات أنه لتشريع مظهر من مظاهر النشاط الإنساني (فعلا كان أم امتناعا)، أي لإعتبار تصرف ما بأنه جريمة معاقبا عليها ، لابد من تدخل المشرع بالنص و الذي يوضح لنا أن هذا التصرف أو ذلك المظهر أنه غير مشروع بما يفيد النهي عن فعل ، وتقرير جزاء لمن يخالف النهي (بالإرتكاب) أو لمن يخالف الأمر (بالإمتناع). وذلك ما يعرف بأنه مبدأ شرعية الجرائم و العقوبات أو مبدأ الشرعية الجنائية ((Principe de légalité des délites et des peines ، حيث :

ان التجريم لا يكون إلا من قبل الشارع أي بنص قانوني صادر عن سلطة ممثلة للشعب ومختصة بالتشريع ، بيد أن استقلال المشرع بسلطة التجريم لا يمنعه من تفويض هذه السلطة في حدود معلومة للسلطة التنفيذية ، وغالبية الدساتير تجيز هذا التفويض، ويترتب على هذا المعنى أن القاضي محروم من سلطة التجريم ، وأيضا يمتنع عن القاضي الخروج عن نصوص التجريم والعقاب عند نفسيرها وتطبيقها، خلافا لما كانت عليه الحال في تشريعات العصور الماضية . كما أن الشخص يتمتع بحرية كاملة في تصرفاته فله أن يقوم بكل ما يشاء من تصرفات دون مساءلة أو متابعة من أي شخص إلا اذا قام بالتصرفات المحددة التي جرّمها القانون، لذلك نلاحظ أن القوانين الجنائية ألزمت القاضي على ذكر النص القانوني الذي يطبقه على المسائل المطروحة أمامه ، كما لا يمكن له أن ينطق بعقوبة غير محددة بطبيعتها ومقدارها بنص القانون، الأمر الذي يلزم القاضي بالإمتثال لنص عند النطق بالعقوبة ويبعده عن خطر خلق العقوبات.

انه يتعين على المشرع – أو من يفوض من السلطات التنفيذية – أن ينص مقدما على ما يعده من الأفعال أو التصرفات جرائم معاقبا عليها ، وأن يجهد في جعل ما يصوغه من هذه النصوص موضحا لخصائص أو مميزات كل جريمة ، فلا يكفي صدور نص التجريم فقط ، بل لابد من تحديد الجريمة تحديدا دقيقا وذكر عناصرها ماهية العقوبات المقررة لها ومقدارها أو كيفية تقديرها. وإذا ركان تدخل الشارع لازما على هذا الوجه ، فالمعنى الذي يستفاد من ذلك هو أن التجريم لا يكون إلا بنصوص مكتوبة ، وينبني على هذا أن النصوص المكتوبة هي المصدر الوحيد في تحديد الجرائم وتقرير العقوبات ، وبهذا

يتميز القانون الجنائي في الكثير من فروع القانون الأخرى التي لا تقتصر مصادرها على القانون المكتوب بل قد تستمد من غير ذلك المعرفة مثلا. [1]

ان التجريم لا يكون إلا للمستقبل ، أي أن القوانين التي تصدر بتجريم التصرفات لا تسري على ما وقع من هذه التصرفات سابقا على تاريخ صدورها ونفاذها. وهذا مفهوم بداهة ، إذ أن العقاب على افعال أو تصرفات وقعت قبل نفاذ القانون وهو في حقيقة الأمر تجريم لها بغير قانون ، ما دام الغرض أنه وقت وقوعها لم يكن هناك قانون ينص على عقابها أي تجريمها. ذلك هو مقتضى قاعدة (عدم رجعية القوانين الجنائية) ، و هي في هذا المعنى ليست نتيجة فحسب لمبدأ الشرعية الجنائية بل انها أصل هذا المبدأ و مقتضاه. على أن مفهوم مبدأ الشرعية لا يتوقف على ما سلف ذكره بل يتجاوز ذلك لكي يشمل الإجراءات الجنائية التي يتطلبها القانون بالنسبة للمتابعة من يوم ارتكاب الجريمة لحين المحاكمة. لذلك يطلق الفقه على هذا مبدا (لا جريمة ولا عقوبة ولا تدابير أمن و لا إجراءات إلا بنص قانوني) ، ولكن هذه الصيغة غير لازمة لان الإجراءات مسألة مفترضة ، إذ هي تسبق دائما النطق بالعقوبة فهي مندمجة بصفة ضمنية في عنصر شرعية العقوبة.

ومن الواضح أن الغرض الاول من مبدأ الشرعية هو كفالة لحرية الأفراد في افعالهم وتصرفاتهم ، لأنه لو ترك أمر التجريم للقاضي كما كان الحال في تشريعات العصور الماضية ، لأضحى الأفراد في حيرة من أمرهم لا يدرون بصفة قاطعة ما هو مباح لهم وما هو محظور عليهم ، فتتعطل بذلك حرياتهم ويشل نشاطهم بفعل الخوف والحذر تارة وبفعل ما يحتمل من تعسف القاضي واستبداده تارة أخرى.

و المبدأ فوق ذلك مما تقتضيه العدالة والمنطق ، اذ أن العقاب أخطر ما تملكه الدولة من الحقوق في مواجهة الأفراد لما يتهددهم من انواع الإيذاء في حرياتهم وأموالهم بل وفي أرواحهم تبعا لما تقتضيه مختلف العقوبات ، ومن ثم فإن الأمر يتطلب عدالة ومنطقا انذار الأفراد مقدما وفي صورة واضحة لا لبس فيها بما يتعرضون له إذا ما صدرت عنهم أفعال أو تصرفات معينة ، أي أن الأمر يتطلب النص مقدما على الجرائم وعقوباتها ، واخيرا فإنه مبدأ تقتضيه المصلحة العامة أو مصلحة الجماعة ، وذلك بإعتبار أن فيه ضمانا لوحدة القضاء الجنائي وعدم أو تفاوته تفاوتا يذهب بهذه الوحدة. [2]

---

[1] أحمد عبد العزيز الألفي ، المرجع السابق، ص 261.

[2] عبد الرحمان جلهم حمزة ، جرائم الانترنت من منضور شرعي وقانوني ، ظافرة للتصميم والطباعة ، بغداد ، بلا سنة نشر ، ص 22.

ب – نتائج مبدأ الشرعية الجنائية

لا نزاع في ان مهمة القاضي الجنائي هي تطبيق القانون ، لأن هذا هو عمل القاضي بصفة عامة ولما كان مقتضى مبدأ شرعية الجرائم والعقوبات قصر سلطة التجريم على المشرع أو ما يفوضه من الهيئات التنفيذية أو الإدارية ، وحرمان القاضي الجنائي من تلك السلطة ، فإنه يجب على هذا الأخير أن يمتنع في تطبيقه للقانون الجنائي عن كل ما من شأنه أن يوصله إلى التجريم في صورة ما ، فلا ينبغي له انشاء جرائم جديدة لم ينص عليها ، أو توقيع عقوبات غير مقررة قانونا ، او الزيادة في العقوبات المقررة ، أو الحكم في جريمة لعقوبة مقررة لجريمة أخرى.

ومعنى كل ذلك أن القاضي ملزم بتطبيق القانون الجنائي كما هو ، أو كما وضعه أو أراده الشارع ، وهذا المعنى هو ما يعبر عنه بقاعدة التفسير الضيق (Interpretetion étroite ou restrictive). وإذا كان مبدأ قانونية الجرائم والعقوبات يقتضي من جهة أخرى تقييد سلطة المشرع نفسه بقصر التجريم على المستقبل دون الماضي ، فلا شك في أن هذا القيد يجد صداه في عمل القاضي كذلك ، فيحتم عليه الإمتناع عن تطبيق النصوص الجنائية المتضمنة للتجريم تطبيقا من شأنه أن يجعلها تسري على الماضي و عليه نستخلص نتائج هذا المبدأ و هي :

حالة انعدام النص : اذا عرض على القاضي الجنائي أمر لا جريمة فيه ، أي لم يرد نص قانوني بتجريمه ، فإنه يتعين عليه أن يقضي بالبراءة مهما كان ذلك الأمر مستهجنا أو معيبا ، بل مهما كان فيه من اعتداء على حق فردي أو على مصلحة الجماعة.

وأبرز النتائج المترتبة على ضرورة التزام التفسير الضيق تتلخص في أن القاضي الجنائي لا يملك أن يطبق القانون بطريقة القياس (raisonnement par analogique) ، كان يوقع العقوبة المقررة لفعل معين على متهم بفعل آخر مشابه ، ولكن لا عقاب عليه بنص صريح ، قياسا لهذه الحالة الأخيرة على الحالة الأولى. وهذه القاعدة هي نتيجة مباشرة لمبدأ الشرعية الجنائية ، لأن اباحة تطبيق القانون الجنائي بطريق القياس يعني تخويل القاضي الجنائي سلطة التشريع في بعض الاحوال مادام يستطيع عن طريق القياس أن يعاقب على أفعال لم يرد نص صريح بتجريمها. وفي هذا يختلف القاضي الجنائي بطبيعة

الحال عن القاضي المدني الذي يستطيع أن يحكم بمقتضى قواعد العدل في حالة انعدام النص ، ويملك من باب أولى اللجوء إلى طريق القياس في تطبيقه للقانون. [1].

واذا كان انعدام النص جزئيا ، بأن كان القانون يوجب فعلا معينا دون أن يقرر عقوبة يجازي بها من يمتنع عن آدائه ، فلا يعتبر هذا النص تجريما للفعل المذكور ومن ثم فإن القاضي لا يملك أن يحكم بعقوبة ما على من يمتنع القيام به. كذلك الشأن اذا كان القانون ينص على عقوبة دون أن يعرف الجريمة المستوجبة لها ، فلا يحق للقاضي أن يوقع هذه العقوبة حتى على من يبدوا له أنه ارتكب عملا يستأهلها ، ذلك بأن مبدأ قانونية الجرائم والعقوبات يقتضي أن التجريم لا يكون إلا بتدخل الشارع لتحديد الجريمة وعقوبتها على السواء ، فإذا نص على أحد هذين الامرين دون الآخر لا يقوم التجريم لنص أحد عنصريه ، وهو نقص لا يملك القاضي الجنائي أن يكمله لأنه لا يملك التجريم كما نقول.

حالة وجود النص : واذا وجد النص الجنائي الذي يجرم سلوكا ، فإما أن يكون واضحا وإما أن لا يكون ، فإن كان النص واضحا ، بأن كانت عبارة مفصحة بذاتها عن غرض الشارع بغير تأويل ، التزم القاضي بتطبيقه كما هو أي وفقا لمدلوله وبغير تجاوز لما تحتمله عبارته.

الفرع الثاني : أزمة مبدأ الشرعية الجنائية سبب في تجريم الإعتداءات على النظام المعلوماتي

تعتبر جرائم الإعتداء على النظام المعلوماتي من الجرائم حديثة النشأة ، لذلك اعتراها نوع من الغموض في تكييف افعال الإعتداء غير المشروعة المصاحبة لها ، لدرجة أنها أعتبرت في بادئ الأمر مجرد جرائم عادية تقنية متطورة ، تستوعبها النصوص التقليدية.

إلا أن التسليم بتطبيق النصوص التقليدية على تلك الجرائم يثير العديد من النقاط القانونية الهامة ، أولها أن نصوص قوانين العقوبات التقليدية وضعت في وقت لم تكن تكنولوجيا المعلومات موجودة ، وبالتالي كانت مستندة إلى مفاهيم فقهية تقليدية ، تأخذ مادية المال او وسيطه المادي بعين الإعتبار لإيقاع

[1] – فريد منعم جبور : حماية المستهلك عبر الأنترنت ومكافحة الجرائم الإلكترونية دراسة مقارنة ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، بيروت ، لبنان ، 2010 ، ص 216.

التجريم بينما غيرت المعلوماتية بشكل كبير المفاهيم القانونية نظرا لظهور قيم حديثة ذات طبيعة خاصة ، محلها بيانات ومعطيات ذات طبيعة غير مادية.[1]

ثانيها إختلاف المواقف الفقهية والقضائية في معالجتها لهذه الجرائم ، ففي حين وجدت اجتهادات فقهية وأحكام قضائية حاولت تفعيل القواعد العقابية الكلاسيكية ، وجعلها مرنة و متوافقة والطبيعة الخاصة للمعلوماتية ، اعتبرتها أحكام أخرى سلوكا مباحا لم يرد بشأنه نص تجريمي ، التزاما بمبدأ الشرعية الجنائية والذي يقضي بأن لا جريمة ولا عقوبة بغير قانون .

و من جانب آخر يصعب التسليم بتخلف القانون الجنائي عن مواكبة الاستعمال الغير مشروع للمعلوماتية في ظل عدم تنظيم أحكام تلك الجرائم ، مما قد يترتب عنه افلات الجاني من العقاب عملا بمبدأ الشرعية الجنائية ، وهو ما يدفع بشكل أو بآخر إلى تطور النصوص التقليدية التي يعرفها قانون العقوبات ، ولكن دونما المساس بإحدى المبادئ المستقرة في القانون الجنائي وهو مبدأ شرعية التجريم والعقاب ، فجهد القاضي يجب أن لا يضع النصوص الكلاسيكية خارج اطارها ، كما لن يتعدى إلى مرتبة التفسير الذي يتجاوز حدود النص وغايته ولا يصل إلى حد إعماله القياس.

مما سيق يتضح أن الحاجة إلى حماية جنائية خاصة بجرائم الإعتداء على النظام المعلوماتي ، خلقتها بالدرجة الأولى دواعي مبدأ الشرعية الجنائية ، كون تلك الجرائم نوع متفرد من الفعل الجرمي ، وهو ما برر بضرورة التدخل وإصدار نصوص قانونية مصاغة بدقة لمعالجة هذه الظاهرة الإجرانية.

المطلب الثاني : مدى عجز المواجهة الجنائية التقليدية ضد الإعتداءات على النظام المعلوماتي

أثرت الرؤى المتعددة و المختلفة في تحديد لطبيعة القانونية للمعلومات الإلكترونية في ضمان حماية في ظل النصوص القائمة هذا من جهة و من جهة أخرى عجزت تلك النصوص في مواجهة الجرائم المستحدثة و هذا ما سنتطرق إليه وفق الفرعين التاليين :

الفرع الأول : تباين الرؤى في تحديد الطبيعة القانونية للمعلومات الإلكترونية :

إنقسم الفقه في تحديد الطبيعة القانونية للمعلومات الإلكترونية كي يمكن حمايتها ، مما إنجر عليه تأثيرا على التشريعات المتعلقة بها ، و هذا ما سنتطرق إليه وفق ما يلي :

[1] – بشرى النية ، مرجع سابق ، ص 96.

أ ولا: الإتجاه التقليدي القائل بأن المعلومات ذات طبيعة من نوع خاص :

و يرى أصحابه أن المعلومات ليس لها طبيعة مادية كونها ليست من قبيل الأشياء المحسوسة ، و لغياب الكيان المادي لها ، فهو لا يجعلها محلا لحق مالي من بين الحقوق المالية المتعارف عليها قانونا ، و التي ترد على الكيانات المادية ، و هو ما يستلزم إستبعادها من طائفة الأموال .

و يرتكز أصحاب هذا الإتجاه على بديهية مسلم بها ، مؤداها أن الأشياء الموصوفة بالقيم (biens أو المال) ، هي تلك الأشياء القابلة للتملك و يمكن حيازتها و الإستئثار بها ، و نضرا لكون المعلومات طبيعة معنوية فمن غير المعقول أن تكون قابلة للحيازة و الإستئثار و فقا لهذا الإتجاه إلا عن طريق حقوق الملكية (الفكرية أو الصناعية) ، مما ينتج عنه أن المعلومات التي لا تنتمي إلى المواد الفكرية أو الصناعية لا يمكن إدراجها في مجموعة القيم المحمية .

و ما يجب إبداءه هنا أن هذا الإتجاه لا يستبعد الحماية القانونية للمعلومات ، فحسبه ما دام أن هناك خطأ موجود عند الإستيلاء غير المشروع على معلومات الغير فهذا مبرر و يسمح برفع دعوى المنافسة غير المشروعة ، فطالما أن الخطأ لا يجد أساسه في الإستيلاء على معلومة الغير فهو يجد أساسه في الظروف المقترنة به و هو تحليل يستند إلى المبدأ الذي تبنته محكمة النقض الفرنسية في حكمها القاضي بأن "الغاية من دعوى المنافسة غير المشروعة هي تأمين حماية الشخص الذي لا يمكنه أن ينتفع بأي حق إستئثاري"

(L'action en Concurrenence Deloyale Apour Objet D'assurer La Protection De Celui Qui Ne Peut Se Pre'valoir D'un Droit Privatif) .

إلا أن هذه الإحالة وفق المبدأ الذي إنتهجته محكمة النقض لم يعتمد من قبل غرفة التجارة الفرنسية و ذلك لعدم توافر الشروط التقليدية لدعوى المنافسة غير المشروعة ، و هذا ما أدى لبلورة تأسيس جديد للخطأ المعترف به من بعض الفقهاء الذين أسسوه وفق التطبيق الموسع لنظرية التصرفات الطفيلية (La Théorie Des Agissment Parasitois) .

و محاولة للتوفيق بين الرأيين السابقين بإعتبارهما يتجهان لنتيجة واحدة مع إختلاف التصور (منافسة غير مشروعة و تصرف طفيلي) ، طرح الفقيه لوكاس (Lucas) فكرة إسناد الخطاء إلى نظرية الإثراء بلا سبب (La Théorie Des Enrichissement Sand Cause) بوصف الخطاء هنا تطبيقا خاصا لها.

و لأجل الوصول إلى تبرير دقيق للخطاء في هذه الحالة انتهى الفقيه ديبوا (Desbois) على الرغم من عدائه لفكرة الإقرار بوجود الحق الإستئثاري للمعلومات إلا أنه من المقبول على حدّ رأيه الإعتراف كذلك بوجود خطاء على أساس دعوى المسؤولية المدنية عقدية كانت أو تقصيرية وفقا لما نص عليه القانون المدني الفرنسي .

هذا الرأي كان أكثر واقعية في تبرير الحماية القانونية للمعلومات بوجود الخطاء على أساس المسؤولية المدنية ، الذي كان له الأثر الواضح في ظهور الإتجاه الفقهي الحديث الذي يرى بأن المعلومات في مصاف القيم .

ثانيا : الإتجاه الحديث القائل بأن المعلومات مجموعة مستحدثة من القيم :

يتزعم هذا الإتجاه كلا من الفقيهين كاتالا (Catala) و فيفانت (Vivant) و لكل منهما منهجه الخاص لكن للوصول إلى نفس النتيجة . فالفقيه كاتالا يعتبر المعلومات مشتقة عن دعامتها المادية (أي الشيء الذي يحتويها) ، و بكونها قيمة قابلة للإستحواذ مستقلة عن دعامتها المادية (Un Bien Susceptible D'appropriation) و يوضح رأيه قائلا "أن المعلومة تقوم وفقا لسعر السوق متى كانت غير محظورة تجاريا و أنها ترتبط بمؤلفها عن طريق علاقة قانونية تتمثل في علاقة المالك بالشيء الذي يملكه و هي تخص مؤلفها بسبب علاقة التبني التي تجمع بينهما". و هنا يستند الفقيه كاتالا في رأيه على حجتين لإضفاء وصف القيمة على المعلومة : الحجة الأولى ترتكز على القيمة الإقتصادية للمعلومة و ذلك لما إعتبرها منتوج تجاري قائم على سعر السوق متى كان غير محظور ، و الحجة الثانية متمثلة في وجود علاقة تبني تجمع بين المعلومة و بين مؤلفها .

و مع صحة هاتين الحجتين إلا أنهما لا تعدان من قبيل الحجج المألوف إستعمالها لتبرير الإعتراف بقيمة من القيم العلمية أو الفكرية...الخ .

أما الفقيه فيفانت الذي يعتمد نفس الإتجاه الذي ذهب إليه الفقيه كاتالا ، إلا أنه أسس رأيه و موقفه على حجتين الأولى مستوحات من الفقيهين بلانيول و روديبير المتمثلة في "أن فكرة الشيء أو القيمة لها صورة معنوية ، و أن نوع محل الحق يمكن أن ينتمي إلى قيمة معنوية ذات طابع إقتصادي و أن تكون جديرة بحماية قانونية" . أما الحجة الثانية قدمها الأستاذ فيفانت نفسه الذي رأى " أن كل الأشياء المملوكة ملكية معنوية ، و التي يعترف بها القانون ، و ترتكز على الإعتراف بأن للمعلومة قيمة ، عندما تكون من قبيل البراءات أو الرسومات أو النماذج أو التحصيلات الضرورية أو حق المؤلف و الإنسان الذي يقدم و

يكتشف و يطلع الجماعة على شيء ما بصرف النظر عن الشكل أو الفكرة ، فهو يقدم لهم معلومة بالمعنى الواسع و لكنها خاصة به ، و يجب أن تعامل هذه الأخيرة بوصفها قيمة تصبح محلا لحق ، فلا توجد ملكية معنوية بدون الإقرار بالقيمة المعلوماتية". و لذلك فهو يرى أن القيمة المعلوماتية ليست بالشيء المستحدث إذ أنها موجودة من قبل في مجموعة ما . [1] .

و عليه مما تقدم تعتبر المعلومات مالا قابلا للتملك أو الإستغلال و ذلك على أساس قيمته الإقتصادية و ليس على كيانه المادي و بذلك و لأجله فهي تستحق حمايتها القانونية . و تتمثل أهمية هذا الوصف أن المعلومات تدخل في عداد الأموال التي يحميها القانون الجنائي من الإعتداء عليها .

و نجد أن المشرع الجزائري قد أدرج في تعديله لقانون العقوبات بموجب القانون 15/04 المؤرخ في 10 نوفمبر 2004 و ذلك من خلال إدراجه للقسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات(من المادة 394 مكرر إلى المادة 394 مكرر 7) تحت الفصل الثالث المعنون ب "الجنايات و الجنح ضد الأموال" ، و هذا دلالة على أن المشرع الجزائري تفادى النقاش الفقهي الدائر حول الطبيعة القانونية للمعلومات و فصل في أمرها مباشرة لما أدرجها تحت الفصل الثالث السابق الذكر و من هنا سهل الأمر على الجهات القضائية و الباحثين متفاديا بذلك إيقاعهم في اللبس و الغموض حول موقفه من تكييف و تحديد طبيعة المعلومات الإلكترونية ، و من هنا نخلص أن المشرع أنه فصل في الأمر تسهيلا لعمل الجهات المختصة غالقا لباب التأويل .

الفرع الثاني : إعتبار البرنامج المعلوماتي حق من حقوق المؤلف

لا شك أن أولى بوادر الإهتمام بالحماية القانونية للمعلوماتية في بادئ الامر في محاولة لسد الفراغ كان في قوانين ذات طبيعة غير جنائية ، عن طريق يالاستعانة بالقواعد المتوفرة التي تراعي طبيعتها كمصنف معلوماتي قوانين حماية حقوق المؤلف.

وتظهر العلاقة بين حماية المعلوماتية عن طريق قوانين حقوق المؤلف ، في كون النظام المعلوماتي ماهو إلا ابتكار جديد لإحدى تطبيقات برامج الحاسب الآلي ومعطياته وبياناته واعتباره من قبيل المصنفات الفكرية.

أولا : فكرة عامة عن الملكية الأدبية و الفنية

[1] نواف كنعان : حق المؤلف –النماذج المعاصرة لحق المؤلف ووسائل حمايته : الطبعة الثالثة 2000 ص.47 وما بعدها

تعتبر الملكية الأدبية والفنية الصورة الثالثة من صور الملكية الفكرية، وبالرغم من اعتبار البعض أن تعبير الملكية الفكرية يشتمل على نوعين من الملكية الفكرية هما: الملكية الصناعية والملكية الأدبية والفنية، وإدخال ما يتعلق بالملكية التجارية ضمن الملكية الصناعية .

إلا أن الواقع أن هناك استغلال نسبي و لو أن هناك حقيقة صعوبة في الفصل لكل من الملكية الصناعية عن الملكية التجارية وكذلك الشأن بالنسبة للملكية الأدبية و الفنية

وتشمل الملكية الأدبية و الفنية القصص و الكتابات العملية و غيرها ، و النصوص المسرحية والأفلام والتأليف الموسيقي والرسوم وأعمال النحت والنجارة وما أشبه ذلك، ويستخدم اصطلاح حق المؤلف للدلالة على الملكية الأدبية والفنية ، حيث جاءت تحت طائلة حق المؤلف لتجعل له نطاق واسع يشمل كل المفردات والابتكارات الذهنية والفكرية التى تشكل كل واحدة منها مصفا فكريا يمنح الحماية المقررة للمصنفات الفكرية وفقا لما جاء في ظل الاتفاقات الدولية والقوانين الداخلية لحماية حق المؤلف[1] .

ثانيا : إعتماد برامج الحاسوب كمصنف محل حماية فكرية:

تعتبر برامج الحاسوب ابداعات فكرية ذات طبيعة تقنية، هذه الطبيعة المزدوجة هي ما جعلت المشرع في العديد من الدول يستند إلى قانون حماية حق المؤلف كسبيل لحماية برامج الحاسب الآلي .

ويقصد بحق المؤلف ، حقه في حماية القانون لإبتكاره الذهني ، بحيث يستطيع استعمال حقه هذا في مصنفه والاستئثار به واستغلاله كما هو مخول له بمقتضى القانون ، والوقوف في وجه كل معتد عليه ، بإلزام الغير بإحترام حقه.[2]

وعلى غرار التشريعات التي نصت على شمول برامج الحاسب الآلي بالحماية القانونية التي تقررها قوانين حماية حق المؤلف ، أدمج المشرع الجزائري برنامج الإعلام الآلي ضمن المصفات الأصلية بموجب الأمر رقم 10/97 المؤرخ في 1997/03/06 المتعلق بحق المؤلف والحقوق المجاورة.[3]وكذا بموجب الأمر 05/03 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 2003/07/19 المتعلق بحق المؤلف

---

[1] عامر محمود الكسواني – الملكية الفكرية –ماهيتها– مفردتها –طرق حمايتها –مرجع سابق ص.224.

[2] –عامر محمود الكسواني ،المرجع السابق ، ص 150.

[3] – نص المادة 04 من الأمر 10/07 المؤرخ في 1997/03/06 المتعلق بحق المؤلف والحقوق المجاورة على أنه :" تعتبر على الخصوص كمؤلفات فيه أو فنية محمية ما يأتي ، المصنفات الأدبية المكتوبة مثل المحاولات الادبية والبحوث العلمية التقنية والروايات والقصص والقصائد الشعرية ومصنفات وقواعد البيانات".

والحقوق المجاورة ، حيث نصت المادة الرابعة منه الفقرة أ على أن : "تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يأتي :

أ –المصنفات الأدبية المكتوبة مثل : المحاولات الأدبية والبحوث العلمية والتقنية ، والروايات والقصص والقصائد الشعرية و برامج الحاسوب و المصنفات الشفوية مثل المحاضرات والخطب والمواعظ وباقي المصنفات التي تماثلها".

ب –وعلى إثر النص السابق يدخل البرنامج ضمن نطاق الحماية التي توفرها النصوص للمؤلفات ، فبات الاعتداء على برامج الحاسب الآلي بمثابة الإعتداء على مصنف أو مؤلف ، ومنه وبشكل طردي يعتبر الموقع الإلكتروني من المصنفات المحمية بموجب قانون حماية المؤلف.

ثالثا : مدى ملاءمة الجزاءات لحماية البرامج في قانون حماية المؤلف

على ضوء نصوص قانون حماية حق المؤلف ، فلهذا الاخير حقه الخالص على المصنف ، يمكنه استعماله واستغلاله والتصرف فيه وقتما يشاء وكيفما يشاء دون اعتداء أو تعرض من أحد.

أ) فلصاحب هذه المصنفات الحق في نسب المصنف إليه ووضع اسمه على مصنفه ، أو وضع اسم مستعار وله الحق في أن يقرر هل سينشر مصنفه أم لا ، ومتى وكيف سينشر المصنف وله الحق في تعديل مصنفه متى راى الحاجة في ذلك ، وبناء على حقه في نشر مصنفه فيمكنه كذلك سحب المصنف من التداول إن كان في ذلك مصلحة له. ومن أهم الحقوق المخول للمؤلف حقه في دفع الاعتداء على المصنف واتخاذ الإجراءات التي وضعها القانون لحماية مصنفه.[1]

تبعا لذلك وبوصف النظام المعلوماتي أحد عناصره برامج الحاسب الآلي ، وبإدارج البرامج المعلوماتية ضمن المصنفات المحمية ، فلصاحب النظام المعلوماتي كامل الحق في تقرير نشر وتحميل وتخزين المعلومات على الحاسوب ، كما له الحق في نسبتها إليه ، والحق في دفع أي اعتداء قد يقع عليها ، وله كذلك الحق في سحبها وشطبها من التداول عبر الحاسوب وعبر شبكة الأنترنت ، أو منح الآخرين رخصا بإستعمالها أو استغلالها.

إلا أن الحماية التي يعطيها القانون المتقدم لبرامج الحاسب بإعتبارها كبقية المصنفات التي يحميها ، لم تسلم من أن ينسب إليها الفقه بعضا من مظاهر القصور :

[1] – د أمجد حسان : الفيروسات ارهابا اهدد انظمة المعلومات ، ملتقى الإرهاب في العصر الرقمي ، جامعة الحسين بن طلال ، 10–12 يوليو 2008 ، عمان ، ص 199.

- فطبيعة المؤلف تختلف عن طبيعة البرامج المعلوماتية ، الأمر الذي يستوجب التمييز بينها لا المساواة. من جانب آخر جرائم الإعتداء على حق المؤلف تختلف عن جرائم الإعتداء على برامج الحاسب الآلي كون الجرائم الأخيرة تفضي إلى خسائر أكثر بكثير من الخسائر الناجمة عن جرائم الاعتداء على حق المؤلف.

- كما أن خوارزميات برنامج الحاسوب وأفكاره لا تتمتع بالحماية القانونية بمقتضى قانون حق المؤلف بإعتبارها ملكا عاما ، يمكن للجميع استعمالها واستخدامها ولو بدون ترخيص من مؤلفها ، حيث يمكن إعادة استخدام الخوارزم ذاته في عدد لا محدود من البرامج. فالخوارزميات على أساس أنها مجرد اجراءات منطقية تأخذ حكم الفكرة التي تخرج بطبيعتها عن نطاق الحماية التشريعية.

- اضافة إلى ما سبق وبشكل عام فإن النصوص التي يتضمنها قانون حماية المؤلف ، لا تحمي البرامج المعلوماتية بإعتبارها من المصنفات إلا من صور الاعتداءات التي تشكل اعتداء على حق المؤلف دون الإعتداءات الأخرى التي قد تتعرض لها البرامج المعلوماتية.

- واذا كان القانون المتقدم قد منح الحماية المدنية لأصحاب الحقوق ، من خلال التعويض المدني عن أي صورة من صور الاعتداء على حق المؤلف الأدبي او المالي[1] فمتى أثبت المؤلف وقوع الاعتداء فيمكن الحكم له بالتعويض المناسب والعادل ، فإن هذه الحماية المدنية غير كاقية لوحدها لردع المعتدين فلابد أن تقرن المسؤولية الجزائية. وأكثر الأوصاف قربا من هذه الإعتداءات هي جريمة التقليد ، والتي تعرف بأنها " كل اعتداء مباشر أو غير مباشر على حقوق المؤلف في المصنفات الواجبة حمايتها أيا كانت طريقة الاعتداء أو صورته.

ومادام المشرع الجزائري قد أدمج برامج الحاسب الآلي ضمن قائمة المصنفات المحمية عن طريق القانون المتعلق بحماية المؤلف ، فإن أي اعتداء على الحق المالي أو الأدبي لمؤلف البرنامج يشكل فعلا من أفعال التقليد، وهو ما تضمنه نص المادة 151 من الأمر 05/03 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة.

[1] – تنص المادة 142 من الامر 05/03 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة على أنه:" تكون الدعوى القضائية لتعويض الضرر الناتج عن الإستغلال الغير مرخص به لمصنف المؤلف والآداء لمالك الحقوق المجاورة من اختصاص القضاء المدني".

وعليه فالإستعمال غير المشروع للبرنامج المعلوماتي يشكل اعتداء تتبعه المسؤولية القانونية ، فكل من يقوم بإستيراد مصنفات محمية أو تصديرها دون اذن صاحبها ، يكون معتدى وتتشكل جريمة التقليد ويدخل في اطار هذه الجريمة كل من يقوم بالكشف الغير مشروع عن المصنف أو المساس بسلامته ، كما يعد مرتكبا لجنحة التقليد تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف أو آداء.

ولا تقتصر جرمية التقليد على من يعتدي على الحقوق الأدبية للمؤلف ، بل يشمل كذلك كل من يعتدي على حقوق المؤلف المالية ، حيث اعتبر المشرع الجزائري أن كل استنساخ للمصنف مهما كان نوعه أو طريقة آدائه ومهما كانت الوسيلة المعتمدة في النسخ ، يعتبر اعتداء على حقوق المؤلف.[1]خذا الصنف من جرائم التقليد هو أكثر شيوعا في المجال المعلوماتي أي عملية استنساخ البرامج النسخ غير الشرعي.

- إضافة إلى ما سبق ، ومن أجل استضهار قانون حماية حق المؤلف في حماية المصنف وبالتالي البرنامج المعلوماتي الذي تثبت له تلك الصفة و الذي يعتبر أحد مكونات النظام المعلوماتي ، عن طريق بيان ما أقره من جزاءات على الإعتداءات التي يمكن أن يتعرض لها البرنامج بإعتباره مصنفا حاله حال أي مصنف آخر ، فللقاضي أن يطبق كعقوبة أصلية الحبس في ستة أشهر إلى ثلاث سنوات وغرامة قدرها حمسمائة الف دينار جزائري إلى مليوم دينار جزائري سواءء تمت عملية النشر في الجزائر أو في الخارج.

- وله سلطة تقرير عقوبات تكميلية ، تتمثل في مصادرة المبالغ المساوية لأقساط الإيرادات المحصلة من الاستغلال غير المشروع للمصنف (البرنامج وبالتالي الموقع) وكل النسخ المقلدة والمصادرة .

- كما للقاضي أن يضاف العقوبات المقررة وذلك في حالة العود ، مع امكانية غلق المؤسسة التي يستغلها المقلد أو شريكه مدة لا تتعدى ستة اشهر ، واذا اقتضى الحال تقرير الغلق النهائي.

ويمكن من جهة أخرى لمؤلف البرنامج المحمي أو ذوي حقوقه المطالبة بحجز الوثائق والنسخ الناتجة عن الاستنساخ غير المشروع أو التقليد ، وذلك حتى في غياب ترخيص قضائي ، وقد يتم عن طريق الحجز الناتج عن التقليد ايقاف لأية عملية جارية ترمي إلى الاستنساخ الغير مشروع للبرنامج أو حجز الدعائم المقلدة والإيرادات المتولدة عن الاستغلال غير المشروع للمصنفات.[2]

[1] – د أمجد حسان : مرجع سابق ، ص 11.

[2] – آمال قارة : مرجع سابق ، ص 66.

من خلال استقراء النصوص السابقة يتضح أن الحماية الجنائية التي تقررها لا تتوافق مع خطورة الإعتداءات التي يتعرض لها النظام المعلوماتي. فهذه النصوص لا تنال بالتجريم جميع الاعتداءات التي لا تمس البرامج بل فقط تلك التي تتعرض لها المصنفات كون البرنامج جزءا منها. فالمعايير التقليدية التي تحدد حصول الإعتداء لا تحمي البرنامج إلا بصورة الإعتداء المباشر الذي يتمثل بالنسخ المجرد ، فيجري التحقيق من الإعتداءات في مدى التشابه الظاهر بين العمل الأصلي والعمل المنسوخ. لكن برامج الحاسب قد تكون بصورة قد تضهر تظهر متطابقة تمام التطابق ، ولكنها تؤدي إلى نتائج تختلف عن بعضها كما أن هناك برامج تكتب بصورة قد تظهر أنها مختلفة تماما ولكنها تأتي بنفس النتائج.

إلا أن الحماية الجزائية للبرامج وبالتالي للنظام المعلوماتي من خلال حق المؤلف تنصب بصفة أساسية على شكل البرنامج أو مضمونه الإبتكاري فقط دون أن تغطي تلك الحماية كل مضمون البرنامج ، مما يجعلها قاصرة على مد الحماية القانونية المأمولة.

مما سبق نجد أنه من اللازم إضافة نصوص قانونية جديدة لجرائم الإعتداء على النظام المعلوماتي شريطة أن تصاغ النصوص وفقا لمبدأ الشرعية الجنائية ، بحيث تكون نصوص وافية تنطبق على الصور والوقائع الجديدة التي تفرزها ثورات التقنية المتسارعة ، تتماشى مع الواقع الحالي والمستقبل ، بحيث تكون النصوص المجرمة للإعتداء على النظام المعلوماتي تتسم ببعد النضر والأخذ بمعياري التوقع والإحتمال.

الفصل الثاني

الواقع القانوني لمواجهة الاعتداءات الواقعة على النظام المعلوماتي

المبحث الأول : إشكالية الحماية الفنية –التقنية– لأمن النظام المعلوماتي في مواجهة الإعتداءات الواقعة عليها

شكلت الإعتداءات الواقعة على نظم المعلومات معظلة قانونية على أساس أن الحماية الفنية أو التقنية لم تعد كافية في إطار أمن المعلومات الإلكترونية و لهذا سنتطرق في هذا المبحث للإجراءات التقنية لأمن المعلومات الإلكترونية من مخاطر الإعتداء عليها و هذا كمطلب أول بينما نخصص المطلب الثاني لتسوية المشاكل القانونية المتعلقة بالحماية من مخاطر الفيروسات.

المطلب الأول: الإجراءات التقنية لأمن المعلومات الإلكترونية من مخاطر الإعتداء عليها

نخصص هذا المبحث لدراسة التهديدات الأمنية للمعلومات الإلكترونية في النظام المعلوماتي كفرع أول بينما الفرع الثاني فنخصصه للوسائل الفنية الوقائية من التهديدات الأمنية للمعلومات الإلكترونية .

الفرع الأول : التهديدات الأمنية للمعلومات الإلكترونية في النظام المعلوماتي

يمكن تعريف التهديدات بطرق مختلفة تنطوي جميعها على بعض القواسم المشتركة التي تجسد الإطار العام للتهديد بمفهومه الواسع، وفيما يأتي نستعرض نماذج هذه التعريفات:

– هو الشخص، المنظمة، الآلية، أو الحدث الذي يمكن أن يلحق الضرر بالموارد المعلوماتية للمنظمة.

– أي ظرف أو حدث من المحتمل أن يؤثر سلبا على العمليات التنظيمية (بما في ذلك مهمة، وظيفة، صورة أو سمعة)، الأصول التنظيمية والأفراد والمنظمات الأخرى، أو للأمة من خلال تعديل المعلومات، و/أو الحرمان من الخدمة.[1]

– أنه "الخطر المحتمل الذي يمكن أن يتعرض له نظام المعلومات وقد يكون شخصيا كالمتجسس أو المجرم المحترف والقرصان المخترق أو شيئا يهدد الأجهزة والبرامج والمعطيات أو حدثا كالحريق وانقطاع التيار الكهربائي والكوارث الطبيعية".

وفقا للتعاريف أعلاه يمكننا تحديد أهم أبعاد مفهوم التهديدات لأمن المعلومات على النحو التالي:

[1] شوان عمر خضر ، الاختصاص القانوني والقضائي في الجرائم المعلوماتية ، رسالة ماجستير / كلية القانون – جامعة كويه ، 2008 ، ص 11.

- توجد التهديدات متى وجدت نقاط الضعف ويمكن أن يكون هناك عدد من التهديدات لكل نقطة ضعف.
- تتبع التهديدات من الأفعال والتصرفات المقصودة وغير المقصودة على السواء والتي قد تأتي من مصادر داخلية أو خارجية، كما أنها قد تتراوح من أحداث مفاجئة أو أحداث ثانوية تؤدي إلى عدم الكفاءة اليومية المتوقعة. وقد تتبع أخطاء النظام من سوء استخدام الأجهزة والبرمجيات، التحميل الزائد أو المشكلات التشغيلية وغير ذلك.
- قد تتسبب المشكلات الفنية نتيجة للهجمات المختلفة التي يتعرض لها النظام، فغالبا تدخل الفيروسات في النظام من خلال البرمجيات المصابة، المتطفلين، الديدان، أو القنابل المنطقية،...الخ. والتي تمثل بعض الوسائل الفنية المستخدمة لتعطيل النظام وتشويهه وعرقلة وظائفه المختلفة، إتلاف أو تحريف بياناته.
- يمكن تصنيف التهديدات في أنواع مختلفة بطرق مختلفة مثل التهديدات البشرية / غير البشرية، التهديدات المعتمدة / غير المعتمدة، تهديدات المهرة / غير المهرة، التهديدات الداخلية / الخارجية. الفيروس على سبيل المثال، هو تهديد غير بشري متعمد، عموما (في البداية على الأقل) وخارجي، ويمكن أن يكون تهديد المهرة أو غير المهرة (اعتمادا على مطور الفيروس). من ناحية أخرى، يوصف تهديد مدير النظم الساخط بأنه بشري، متعمد، ومهرة، وداخلي.
- التهديدات هي الأشياء التي يمكن أن تسبب الضرر، أو هي الأشياء السيئة المحتملة التي يمكن أن تحدث لأحد الأصول، ومن ثم يمثل خطرا ممكنا على النظام. وقد يكون هذا الخطر شخص يقوم بالتجسس أو التخريب، أو شيء يحدث مشكلة في الحاسب وملحقاته، أو حدثا مثل الحريق أو الفيضان، أو يستغل به نقطة ضعف النظام.[1]

أولا : أنواع التهديدات الأمنية للمعلومات الإلكترونية

تتجسد أهمية تحديد أنواع التهديدات في أنه يساعدنا في رسم ما يصطلح عليها "خارطة التهديدات لأمن المعلومات و من ثم تقييم مصادر التهديد، حيث أن المهم النظر في جميع مصادر التهديدات المحتملة التي يمكن أن تسبب ضررا لموارد المعلومات في النظام المعلوماتي وفي كيفية التعامل معها خاصة في الجوانب التي تخدم دراستنا للموضوع محل

[1] نهلا عبد القادر المومني ، الجرائم المعلوماتية ، ط1 ، دار الثقافة ، عمان ، 2008 ، ص 50

البحث ، على النحو الذي يسهل معرفة وتحديد أي التهديدات الأكثر خطورة وبالتالي تركيز الرقابة على النشاط المرتبط به ومن ثم السعي إلى تقليل الآثار السلبية المحتملة له. حيث يمكن استخدام أسس مختلفة في تصنيف التهديدات، وأهم هذه الأسس هي:

- نوع الهجوم المحتمل: يصنف الخبراء المختصين بالقضايا الأمنية عبر الشبكات والانترنت التهديدات لأمن المعلومات إلى نوعين من أنواع الهجوم المحتملة وهما: الهجوم التقني والهجوم غير التقني.
- حسب المصادر التي تنبع منها التهديدات تصنف التهديدات حسب المصادر التي تتبع منها إلى نوعين وهما: مصادر تهديدات داخلية ومصادر تهديدات خارجية.
- حسب طبيعة التهديدات يتم تصنيف التهديدات حسب طبيعتها إلى ثلاث أنواع " تهديدات طبيعية، تهديدات بشرية، تهديدات بيئية".[1]

–نوع الحدث الحاصل تقسيم أنواع التهديدات على أساس ما الذي يحدث مباشرة لأنظمة المعلومات و هي: الفضح و الكشف ، الوصول غير المصرح له للمعلومات ، الخداع ، التحكم غير الشرعي لأجزاء من النظام .

و عليه سنوضح بإيجاز أهم أنواع التهديدات المحتملة لأمن المعلومات من خلال تصنيفها إلى تهديدات ، داخلية و أخرى خارجية ، و هي تهديدات بشرية صرفة فلا يهمنا التصنيفات الأخرى لها لأنها لا تمس بصلة لبحثنا هذا فالتهديدات البشرية نعرفها بأنها: أي أحداث تتم عن طريف أخطاء البشر، مثل أعمال غير مقصودة (إدخال بيانات غير مقصودة) أو إجراءات متعمدة مثل (الهجوم على الشبكة، تحميل البرمجيات الخبيثة، الوصول غير المصرح به إلى المعلومات السرية) وبالتالي يكون هذا التهديد هو محل دراستنا و يمكن تصنيف التهديدات البشرية إلى نوعين رئيسيين هما:

أ– المهاجمون من الداخل: إن المتسبب للتهديدات الأمنية هو الخطأ البشري، و المعني بذلك هم الموظفون والعاملون في إطار المنظومة المعلوماتية ، إذ يشكل الموظفون ما نسبته (75_80%) من مصادر التهديدات الداخلية في المنظومة وتشمل هذه الفئة الموظفين الحاليين

[1] محمد بن حميد المزمومي ، جريمة الإعتداء على الأموال عن طريق الحاسب الآلي ، رسالة ماجستير / كلية الإقتصاد والإدارة (قسم الأنظمة) – جامعة الملك عبد العزيز ، جدة ، 2007 ، ص 19

والسابقين. المهاجمون من الداخل هم "أولائك الأفراد الذين ينتمون للجهة المستهدفة، غير أنهم يقومون بأعمال تصادم جهود الجهة الرامية إلى حماية أنظمة المعلومات التي تستخدمها تلك الجهة".

فالتهديدات الداخلية يمكن أن تكون بقصود أو غير قصود، من أشخاص معتمدين للوصول إلى نظم المعلومات ، و هم دوما "الخطر الذي تواجهه أي جهة"، مهما كانت سواء كانت تلك الجهة شركة أو منظمة أو حتى دولة. ومع استخدام الحاسوب والتقنيات زاد الخطر الناجم عن الهجمات التي يقوم بها المهاجمون من الداخل ضد الجهة التي ينتمي إليها.

ويؤكد المتخصصون أن الهجوم الداخلي لا يحصل دون أسباب حقيقية، حيث أن هناك أسباب مختلفة للهجوم ضد نظم المعلومات، وهذه الأسباب يمكن إيجازها كالآتي:

- حالة عدم الرضا التي تظهر عندما يشعر الموظف بعدم الرضا ومن ثم يقوم بمهاجمة نظم المعلومات للانتقام.
- إثبات الشخص مهاراته الفنية وقدراته على تنفيذ هجوم إلكتروني، حيث هناك بعض الأفراد يشعرون بالفخر والاعتزاز بنفسهم.
- تحقيق مكاسب مالية، حيث يهاجم شخص ما أنظمة معلومات الجهة التي يعمل فيها لسرقة معلومات سرية يستخدمها لاحقا لابتزاز الجهة لدفع فدية مالية.[1]

و هناك العديد من تلك الأخطاء التي تشكل تهديدا كبيرا على أمن المعلومات، وتشكل الأخطاء التقنية والتي حظيت بأكبر حصة، من بين أسوأ الأخطاء التي يرتكبها المستخدمون لأنظمة المعلومات ومنها:

- عدم الاحتفاظ بنسخ احتياطية واختبارها.
- التصريح بكلمات مرور المستخدمين عبر الهاتف أو تغيير كلمات المرور بناء على طلب الأفراد عبر الهاتف ومن قبل أفراد لا يتم التحقق من هويتهم.

[1] هشام محمد فريد رستم ، الجرائم المعلوماتية – أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي ، بحيث مقدم لمؤتمر القانون والكمبيوتر والأنترنت الذي نظمته كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة في الفترة (1-3/مايو/2000) ، بحوث مؤتمر القانون والكمبيوتر والأنترنت ، المجلد الثاني ، كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة ، 2004 ، ص 405 و 406.

- عدم القيام بتحديث الأنظمة عند اكتشاف فجوات (ثغرات) أمنية فيها.
- ربط الأنظمة بالإنترنت قبل تشغيل أنظمة الحماية.

فالإستهانة بالمخلفات التقنية أمر بالغ الخطورة، إذ يقوم المهاجم بتفتيش المخلفات التقنية بحثا عن أي شيء يساعده في اختراق النظام، مثل الأقراص الصلبة بعد استبدالها، أو الأوراق التي دون عليها كلمات السر أو أسماء الملفات والبرامج. وتشمل في المقام الأول الخروقات الأمنية العرضية الحاصلة من قبل الموظفين بسبب الإهمال أو غير المطابقة وسوء سلوك الموظف . فالتهديدات الداخلية المحتملة تحتوي على اختراق بيانات النظام المعلوماتي ، و الاستخدام غير المشروع لها . [1]

ب- المهاجمون من الخارج

وهم الأشخاص من خارج النظام المعلوماتي والذين يطلق عليهم "القراصنة Haker" والذين لديهم بواعث مختلفة للهجوم على الأنظمة، وهم اكثر خطورة من الموظفين الساخطين كما رأينا سابقا من خلال تطرقنا للمجرم المعلوماتي و دوافعه أو بواعثه . ففي المقام الأول نجد أن العملية تتم وفق تهديدات الفيروسات، وهجمات القراصنة ، والهجمات الإرهابية، هجمات الحرمان من الخدمة الموزعة، هجمات الاحتيال والبريد المزعج.

فالتهديدات الخارجية غالبا ما تلقى الكثير من الاهتمام عند إثارتها من قبل وسائل الإعلام وتصبح معروفة جيدا، مما يجعل من السهل التركيز عليها والتعامل معها . و تم تصنيف حصان طروادة وديدان الانترنت كأكبر التهديدات. وجاء بالمرتبة الثانية التهديد المرتبط بسوء سلوك الموظف.

ثانيا : أساليب التهديدات الأمنية للمعلومات الإلكترونية

أ -**القرصنة:** القرصان هو الشخص الذي يتجاوز عناصر التحكم في الوصول إلى النظام من خلال الاستفادة من نقاط الضعف الأمنية التي تركها مطوري الأنظمة في النظام. وبالإضافة إلى ذلك، العديد من المتسللين هم بارعون في اكتشاف كلمات السر للمستخدمين المرخص لهم الذين يفشلون في اختيار كلمات المرور التي يصعب تخمينها أو تلك غير المدرجة في القاموس. تمثل أنشطة القراصنة تهديدات خطيرة للمعلومات السرية في أنظمة

[1] – نائلة عادل فريد قورة ، مصدر سابق ، ص 91.

الحاسوب. حيث أنشأ العديد من المتسللين نسخ من الملفات ذات الحماية غير الكافية وتم وضعها في مجالات النظام والتي يمكن الوصول إليها من قبل الأشخاص غير مخولين.

ب – الإختفاء : المختفي أو المقنع هو المستخدم المصرح به للنظام والذي حصل على كلمة مرور مستخدم آخر، على النحو الذي يمكنه الوصول إلى الملفات المتاحة للمستخدم الآخر. وهؤلاء المتخفون غالبا ما يكونوا قادرين على قراءة ونسخ الملفات السرية. والتكرار أمر شائع في الشركات التي تسمح للمستخدمين لتبادل كلمات السر. [1]

ج – نشاط المستخدم غير المصرح : هذا النوع من النشاط يحدث عندما يحقق مستخدمي النظام المخولين للوصول إلى الملفات التي لا يحق لهم الوصول إليها. وضعف التحكم في الوصول غالبا ما يمكن من الوصول غير المصرح به، والتي يمكن أن تمس الملفات السرية.

د – التحميل للملفات دون حماية: يمكن تحميل الملفات السرية إذا تم في عملية التحميل، نقل الملفات من بيئة آمنة في الحاسبة المضيف إلى الحاسبات الصغيرة غير المحمية لغاية المعالجة المحلية. حيث يمكن الوصول إلى المعلومات السرية غير المراقبة من قبل المستخدمين المصرح لهم على الحاسابات الصغيرة.

هـ – شبكات المناطق المحلية: تشكل الشبكات المحلية تهديدا خاصا للسرية بسبب أن البيانات التي تتدفق من خلال LAN يمكن مشاهدتها في أي عقدة في الشبكة، بغض النظر عما إذا كانت هذه البيانات معنونة أم لا إلى تلك العقدة. وهذا أمر بشكل خاص لأن معرفات المستخدمين غير المشفرة وكلمات المرور السرية للمستخدمين الذين يسجلون الدخول إلى المضيف تخض لتقديم تنازلات كلما تحولت هذه البيانات من عقدة المستخدم ومن خلال LAN إلى المضيف. أي معلومات سرية غير مخصصة للعرض في كل عقدة يجب أن تكون محمية من خلال التشفير.

و – أحصنة طروادة: يمكن برمجة أحصنة طروادة لنسخ الملفات السرية إلى المناطق غير المحمية من النظام عندما يتم تنفيذ أية عملية من قبل المستخدمين الذين يؤذن لهم بالوصول إلى تلك الملفات. وحالما يتم التنفيذ، يصبح حصان طروادة مقيما في نظام المستخدم، ويمكن نسخ الملفات السرية بشكل روتيني على الموارد غير المحمية .

[1] – نسرين عبد الحميد نبيه ، مصدر سابق ، ص 59 و 60.

ي –الأجهزة المحمولة: و هذا من التحديات الجديدة التي تتزايد خطورتها يوما بعد يوم و هذا من خلال البرمجيات الضارة التي تستهدفه، وسرقة البيانات، وفقدان أو سرقة الأجهزة، وبشكل متزايد، وقضايا أخرى تظهر في كل وقت، مثل القدرة على تحديد الموقع الجغرافي للفرد من خلال أجهزتهم بحيث يخلق أنواع من المخاطر التي لا تزال غير مفهومة

الفرع الثاني : الوسائل الفنية الوقائية من التهديدات الأمنية للمعلومات الإلكترونية

ما من وشك أن للوسائل الفنية –التي تعمل على الوقاية من اثار التهديدات الأمنية– أثر بالغ الأهمية في تحديد موقع ونوع الفيروس وتعقب آثاره وبالتالي الوقاية من الأخطار الممكن وقوعها في حال غياب هاته الإجراءات.

ويمكن تلخيص هاته الإجراءات الواجب العمل بها من طرف مالك البرنامج أو من طرف الجهات المنتجة أو غيرها من الجهات الصلة بالنقاط التالية:

أولا: أن تكون النسخة التي يحصل عليها مقتني البرنامج مغلفة بغلاف الشركة المنتجة تغليفا محكما وهذا لا يعني أن البرامج المغلفة مؤداه خلوها تماما من الفيروس، لكن هذا الاجراء يقلل من احتمالات الإصابة بالفيروس بدرجة كبيرة.

ثانيا: عمل نسخة احتياطية باستخدام القرص الاصلي برنامج ثم حماية القرص الاحتياطي أيضا[1].

وتجدر الإشارة إلى أن مسألة عمل نسخة احتياطية للبرنامج لاقت اعتراضا واسع النطاق من طرف المبرمجين والشركات المنتجة بحجة أن العديد من الأفراد غالبا من يلجئون إلى قرصنة البرامج تحت ذريعة أن هذه النسخة لا تمثل سوى نسخة احتياطية لبرنامج هذا فضلا عن أن أغلب الأشخاص الذين يحصلون على هاته النسخ غالبا ما يتواجدون في أماكن خاص بهم يصعب الوصول إليها أو معرفة أنهم قاموا –مثلا– بعملية قرصنة لبرامج الحاسب الالي.

لذا برزت معارضة حادة لمسألة عمل نسخة احتياطية للبرنامج إلا أن هاته المعارضة لم ترق –في الواقع– إلى مستوى منع الأفراد أو الجهات من الاحتفاظ بنسخة احتياطية كإجراء وقائي يتم اللجوء في حال تعرض برامجهم لهجمات فيروسية.

ثالثا: تحميل البرنامج على القرص الصلب من القرص الأصلي للبرنامج.

[1] د. محمد فهمي طلبة وآخرون: فيروسات الحاسب وأمن البيانات، مرجع سابق، ص98.

رابعا: العمل على مقارنة الملفات المخزنة على القرص الأصلي بنفس الملفات المخزنة على القرص الاحتياطي.

إذ أنه في حال تواجد أي اختلاف، يصبح هناك شك في تواجد الفيروس[1].

خامسا: العمل على اختبار كل برنامج موجود على القرص والتأكد من أنه يؤدي وظائفه بصورة طبيعة، وملاحظة أي أشياء غريبة قد تحدث من أي برنامج.

سادسا: العمل على اختبار البرامج المخزنة مع تغيير التاريخ في ساعة النظام **(SYSTEM CIOCK)** إدخال التواريخ التي تستخدمها بعض الفيروسات والتي تبدأ عملها وفق تاريخ أو توقيت محدد، إذ يتم بهذه الطريقة الكشف عن هذه الفيروسات –إذا كانت موجودة– وبالتالي إمكانية التخلص منها[2].

سابعا: العمل على اختبار البرامج للبحث عن سلاسل حرفية معينة ترتبط بوجود أنواع معينة من أنواع الفيروسات، وبالتالي إمكانية التخلص منها.

ثامنا: مرقبة ملفات الأوامر المجمعة **(Batch Files)** ذات الامتداد **(BAT)** بين الفينة والأخرى، وكذلك ملف المواصفات **(Config. Sys)** وملاحظة أي تغيير يطرأ على الأوامر الموجودة فيها، حيث أن الفيروس يحتاج إلى الارتباط بأي ملفات منفذة حتى يتم تشغيله، لذلك فإنه في بعض الأحيان يكتب سطورا في ملف الأوامر المجمعة أو في المواصفات حتى يضمن تنفيذه

تاسعا: تعقب آثار الفيروس، وذلك باستخدام أسلوب التوقيع الرقمي.

حيث يمكن –عن طريق أسلوب التوقيع الرقمي– تعقب آثار الفيروس إلى مصدره–وذلك عندما يكون الفيروس موجها عبر شبكات الاتصال– إذ يمكن عن طريق استخدام **(Audit Trail)** أن يتم تتبع هذا الفيروس، الشيء الذي يمكن عن طريقه أن يحجم مروجو الفيروسات عن الإنتاج لها وترويجها عبر الشبكات[3].

عاشرا: إتاحة الإمكانية للبرامج للقيام بعملية الدفاع الذاتي.

حيث يستطيع كل مبرمج تصميم نظام دفاعي ضد الفيروسات، وهناك أبحاث تقترح أن تضاف هذه الإمكانية لمترجمات البرامج وذلك حتى تقوم بتزويد البرامج في مرحلة الترجمة بهذا النظام الدفاعي.

---

[1] تتم المقارنة باستخدام الأمر (Disk comp) أو الأمر (Comp) في نظام التشغيل (DOS).

[2] فهمي محمد طلبة: مرجع سابق، ص98.

[3] د. حسن طاهر داود: الحاسب وأمن المعلومات، مرجع سابق، ص79.

وتكمن ميزة هذا الأسلوب في سهولة وسرعة تطبيقه، إلا أنه يعاب عليه أنه لا يستطيع اتخاذ إجراء ضد الفيروس المهاجم إلا بعد تعرقه عليه، وربما يكون الوقت عندئذ قد فات وبدأ الفيروس نشاطه الهدام.

الحادي عشر: استخدام أحد البرامج المساعدة في عرض أسماء الملفات المختفية (hidden Files)، وعند ملاحظة أي أسماء جديدة أكثر من أسماء الملفات المستخدمة في نظام التشغيل يكون هناك شك في تواجد الفيروس الذي يجب العمل على التخلص منه.

الثاني عشر: العمل على تسجيل بيانات كل برنامج مثل طول الملف والتاريخ والوقت ومصدر البرنامج، وعند ظهور الفيروس في أي وقت، تصبح هذه البيانات في منتهى الأهمية.

حيث يمكن من خلال تاريخ اكتشاف هذا الفيروس استنساخ النسخ الاحتياطية التي تم عملها قبل هذا التاريخ خالية من الفيروس، ويكون هناك شك فقط في باقي النسخ التالية لهذا التاريخ.

كما أن هذه البيانات قد تقود المستخدم في النهاية إلى المجرم الذي قام بوضع هذا الفيروس[1].

الثالث عشر: وضع برنامج عازل للفيروسات في الجهاز الذي يصل بين الشبكات الداخلية والعالم الخارجي (مثل الوسيط Proxt) لمنع وصول الفيروسات إلى الشبكة المحلية أو إلى أجهزة المستفيدين.

الرابع عشر: التأكد من أن جميع الاتصالات التي تتم من خلال الحاسبات الشخصية للمستفيدين بخارج المؤسسة تتم عن طريق الشبكة وليس عن طريق "مودم" قد يتم تركيبه خلسة في أحد الحاسبات الشخصية للاتصال (بإنترنت) مثلا.

الخامس عشر: استخدام ما يطلق عليه "بالتوقيع الرقمي" (Digital Signature).

فلما كان تداول البيانات داخل الشبكات والبريد الالكتروني هما من المصادر الهامة للإصابة بالفيروسات، فلابد من التركيز على هذا القطاع للحد من تأثير الفيروسات وذلك بالعمل على اكتشاف وجوده قبل أن تبدأ عملها.

المطلب الثاني: تسوية المشاكل القانونية المتعلقة بالحماية من مخاطر الفيروسات

ما من شك أن تفعيل السبل القانونية وبناء النصوص الموضوعية في موضوع الحماية من مخاطر التهديدات الأمنية مؤداه تقليص حجم المخاطر وتقليص مستوى الجريمة المرتكبة بحق المعلومات عن طريق الإعتداء عليها .

الفرع الأول : المعوقات التطبيقية القانونية

[1] د. محمد فهمي طلبة وآخرون: فيروسات الحاسب وأمن البيانات، مرجع سابق، ص90.

في الواقع، يواجه تطبيق القانون في موضوع الفيروس عددا من الصعوبات والموانع التي يمكن تلخيصها فيما يلي:

1- في إطار الإعتداءات التي أساسها الفيروس نجد أنه-في الغالب- لا يتمكن الضحية من معرفة المجرم الذي صمم هذا الفيروس، وأنه في حال معرفته بذلك، فإنه غالبا ما يتحمل تكاليف باهظة للوصول إلى هاته الحقيقة ومتابعة الجاني[1].

2- رغبة العديد من ضحايا الفيروس وقد سبق الإشارة إلى ذلك من الشركات والقطاعات الاقتصادية الكبرى -وخصوصا في ميدان البنوك- في عدم الكشف عن إصابة نظامهم بالفيروس، وذلك حتى لا يتسبب ذلك في اهتزاز ثقة العملاء إذ يؤدي الكشف -مثلا- عن هاته الفيروسات -في قطاع البنوك- إلى قيام العديد من العملاء باللجوء إلى سحب أرصدتهم كإجراء حال علمهم بذلك.

3- جهل أو عدم معرفة الضحية أن نظامه قد أصيب بالفيروس لمدة طويلة وعندما يكتشف ذلك يصعب عليه تحديد وقت وسبب الإصابة

4- صعوبة قياس أو تقدير الخسائر -خصوصا عندما تكون مادية- ومثال ذلك أن بعض الفيروسات يتسبب في إتلاف أحد البرامج مما يؤدي إلى إصابة مخطط هذا البرنامج بكثير من الاحباط نتيجة ذلك دون حدوث خسائر مادية محددة مع العلم أن أهمية هاته المخططات قد تفوق بكثير التقديرات المادية المتوقعة[2].

5- قدرة الفيروس على إخفاء أي آثار وكذا إمكانية بعض الفيروسات مسح نفسها تماما من ذاكرة البرنامج بعد تنفيذها لأعمالها التدمرية وبالتالي صعوبة الوصول إلى المخرب الذي قام بتصميم هذه الفيروسات أو إدخالها إلى النظام.

6- جهل المستخدم للمعلومات الكافية عن الفيروس وبالتالي لا يعرف أن هناك مخربا وراء هذا الفيروس الذي يجب الإبلاغ عنه حتى يتم الوصول إلى مدبره ومعاقبته.

---

[1] د. محمد فهمي طلبة، مرجع سابق، ص206.

**- كذلك راجع:

Anderson J.p (1972) Informatino security in a multi_user Computer environnment .IN Advances in Computers, Vol.12 (ed M.Rubinoff) Academic press, New York. Deferance pages.

[2] د. محمد فهمي طلبة : فيروسات الحاسب وأمن البيانات، مرجع سابق، ص206.

الفرع الثاني : ضرورة صدور نظام تشريعي خاص بأمن المعلومات من الإعتداءات الواقعة عليها

لما كان النظام المعلوماتي و المسائل المتصلة به ، تسمح لمستخدميه الدخول إلى النظام من أي مكان في العالم، و هذا لكون بنية الانترنت التحتية المتمثلة بأنظمة الكمبيوتر والاتصالات تمتد إلى العديد الدول، وأن مكان ممارسة العمل الفعلي للشخص قد لا يكون هو المكان الذي تقدم من خلاله خدمة إطلاق الموقع على الشبكة، ولما كان الاعتماد على الانترنت أصبح يمثل محور حياة الفرد والجماعة، لذا فقد كان لظهور التحديات القانونية والتنظيمية الصفة المباشرة نتيجة هاته التطورات المتلاحقة.

وبالتالي فقد وجدنا أنه من المناسب الحديث عن بعض الحلول التي تهم موضوعنا والمتمثل في امن المعلومات الإلكترونية و النظم من الفيروسات –بالتحديد– التي تروج شبكات الاتصال وتمتد آثارها إلى أكثر من جهة أو أكثر من قطاع.

حيث يجمع الباحثون أن تحديد الموقف من مسائل القانون المتصلة بالأنترنت يجب أن ينطلق ابتداء من فهم الطبيعة التقنية لهذه الواسطة المعقدة من وسائط تكنولوجيا المعلومات، وأنه بدون إدراك هذه الطبيعة يتخلف الشرط الموضوعي لتقييم مدى ملائمة القواعد القانونية القائمة، ومدى الحاجة إلى إيجاد قوانين خاصة تنظم مسائل عصر المعلومات، بما فيه الإنترنت

وعليه فإن أولى المقترحات والحلول التي نوليها اهتمامنا هي تلك التي تهم الكيفية التي يتوجب من خلالها تسوية الإجراءات الشكلية المتعلقة بتنازع القوانين والاختصاص التي تحكم جرائم الحاسب الآلي – وتحديدا– الفيروسات الالكترونية المروجة عبر شبكات الاتصال.

ولتوضيح الصورة الميدانية نسوق المثال التالي:

فلو فرضنا أن شخصا متواجد في الولايات المتحدة أو في الباكستان مثلا، وقام بزرع فيروس معلوماتي عبر الشبكة المعلوماتية (الإنترنت) الذي زار عددا من المواقع على هاته الشبكة، وعمل على اختراق مجموعة من الأنظمة على الشبكة، وأحدث إتلاف بياني معلوماتي في البرامج والنظم، وقد طال هذا الأثر عددا من البلدان منها الجزائر ومس الآلاف من الحاسبات الالكترونية، بحيث خلف خسائر يصعب حصرها، فما هو الإجراء الواجب إتباعه لتفادي هذا الإشكال ؟ وهنا –بالتحديد– نتساءل: ما هو القانون واجب التطبيق ؟ و فيما يخص موضوع حماية الأنظمة من مخاطر الإعتداءات كان لابد من وضع تشريع خاص بحماية الانظمة المعلوماتية من الإعتداءات الواقعة عليها يضمن الأتي توضيحه:

أولا: خلق أجهزة دولية متخصصة هدفها مراقبة شبكات الاتصال، ومهمتها الكشف عن الفيروسات التي تروج عبر الشبكات والعمل على ضبط المخالفات في هذا الميدان، وكذا –في حال انتشار فيروس عبر شبكات الاتصال– هذا الفيروس ومعرفة مصدره، والعمل على الكشف عن الشخص أو الجهة المروجة له وتقديمها للجهات المكلفة بالمحاكمة.

وعليه فإنه يمكن القول أن عمل هذه اللجان يشبه–إلى حد ما– عمل اللجان الدولية، إلا أن هاته اللجان تمتاز بكونها تشتمل على عناصر فنية متخصصة في ميدان النظم وتكنولوجيا المعلومات، الشيء الذي يتيح لها إمكانية العمل–وبحرية– للتمكن من حماية المعلومات الإلكترونية من الانتهاكات التي ترتكب عبر شبكات الاتصال، والتي يتم من خلالها تحقيق الاعتداء على الأنظمة.

ثانيا: إنشاء قانون خاص و مستقل، وذلك لتفادي الإشكالات الناجمة عن مشاكل الفيروسات المروجة عبر شبكات الاتصال.

ومما ينبغي الإشارة إليه هو أن التشريع المستقل الذي أشرنا إليه هنا المتعلق بالحماية من مخاطر الإعتداءات على المعلومات ، وليس كل صور الاعتداءات أو المشاكل الأخرى التي تثور –خصوصا– في إطار الإعتداءات على النظام المعلوماتي.

ومما ينبغي قوله أن القضاء في ميدان تكنولوجيا المعلومات والمتعلق بحماية أنظمة المعلومات وشبكات الاتصال، ينبغي أن يملك حجية الإلزام وآليات التنفيذ لأحكامه ضمانا للحفاظ على المكتسبات التي وصلت إليها الحياة البشرية، وكذا إتاحة الفرصة للإبداع والمبدعين لتقديم المزيد في عالم يسوده الأمن والاستقرار وليس في بيئة محفوفة بالمخاطر أخذت فيها معظم الشركات والقطاعات تعزل نفسها عن شبكات الاتصال مخافة الهجمات الفيروسية التي تتزايد حدتها يوما بعد يوم.

ثالثا: توضيح الأعمال التي تشكل جرائم نتيجة الأضرار التي يحدثها الإعتداء على النظام المعلوماتي.

حيث سبق وأن قلنا أن الفيروس –في الواقع– يحدث أضرارا مختلفة تبعا للهدف الموجه لأجله. وبالتالي فإنه لتحقيق مبدأ الشرعية، يستوجب التعاون بين رجال القانون لتجريم كافة مظاهر وأشكال الاعتداء التي يلجأ إليها الفيروس في تحقيق الضرر، هذا دون إغفال الإشارة إلى ضرورة الاستعانة بأصحاب الخبرة الفنية في هذا الميدان.

رابعا: العمل على ترتيب إجراءات هيكلية يكفل من خلالها المتضررون من الهجمات الفيروسية الحصول على تعويضات مالية في حال كان الضرر الذي لحق بهم مادي، حيث من المعلوم أن بعض

الفيروسات قد تطول الآلاف من الأفراد الذين تلحق بهم أضرار جسيمة من جراء هاته الفيروسات، ففي هاته الحالة هل من المعقول أن الشخص الذي تسبب في هذا الفيروس أو الجهة التي قامت بزرعه قادرة على تعويض هؤلاء المتضررين جميعا ؟

بالطبع لا يمكن تحقيق ذلك، لذا فإنه يتوجب على المجتمع الدولي إيجاد وسائل بديلة وذلك عن طريق إنشاء شركات تأمين عالمية متخصصة ترتبط مباشرة مع الأجهزة الدولية المكلفة بضبط ومتابعة مبرمجي الفيروسات الالكترونية، ووظيفتها هو التعويض للمتضررين عن الأضرار التي خلفها الفيروس ببرامجهم وأنظمتهم الالكترونية.

المبحث الثاني: الإطار التشريعي لمواجهة الإعتداءات الواقعة على النظام المعلوماتي

المطلب الأول : نماذج تشريعية دولية لجرائم الإعتداء على النظام المعلوماتي

أولا : قانون الأونستيرال النموذجي بشأن التجارة الإلكترونية

وضعت اللجنة الأممية للقانون التجاري – و هي التي يختصر في تسميتها بالأونسيترال – في اعتبارها أن هذا القانون سيكون أداة فعالة للدول المعنية بتحديث تشريعاتها في اطار التعاملات المرتبطة بتقنية الإتصالات الحديثة ، و لقد طرأ على هذا القانون عدة عمليات تشريعية لتكملته وفق المستجدات الواقعة و لكي يكون قانونا متكاملا ينصح به من طرف اللجنة الأممية للتجارة الإلكترونية للدول للأخذ به دون إلزام منها .

فالقانون الأول من حيث الصدور كان في 16 ديسمبر 1996 في الجلسة العامة رقم 85 ، و هو يحتوي على 17 مادة حيث عالجت تلك المواد الأتي توضيحه :

-نطاق تطبيق القانون النموذجي بحيث يغطي كل الحالات التي تنشأ فيها المعلومات أو تخزن أو تبلغ بوسائل إلكترونية أو ضوئية أو وسيلة مشابهة ، و المستخدمة في سياق الأنشطة التجارية[1]. كما تم كذلك التعريف بكل المصطلحات ذات الصلة بالموضوع الذي شرع لأجله هذا القانون ،[2]

و هي : رسائل البيانات ، و التبادل الإلكتروني لها[3] ، المنشئ و المرسل إليه ، الوسيط ، نظام المعلومات .

-التفسير بحيث يقصد منها أن تقوم المحاكم و غيرها من السلطات الوطنية أو المحلية توفير الإرشاد الى تفسير هذا القانون[4] .

-التغيير بالإتفاق و المقصود منه ألا تنطبق فقط بين المنشئ و المرسل إليهم رسائل البيانات لكن أيضا تشمل الوسطاء ، و عليه يمكن تغيير الفصل الثاني من الجزء الأول من هذا القانون بموجب اتفاقية

[1] المادة الأولى من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية .

[2] وائل أنور بندق ، موسوعة القانون الإلكتروني و تكنولوجيا الإتصال و المعلومات ، الطبعة الأولى (2007) ، دار المطبوعات الجامعية ، الإسكندرية ، ص ص (42-48)

[3] الفقرة ب من المادة الثانية من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص(133)

[4] المادة الثالثة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص(134)

ثنائية أو متعددة الأطراف ، و إما بموجب قواعد للنظم يتفق عليها الأطراف ، مع تقييد صراحة إستقلالية الأطراف بالحقوق و الإلتزامات الناشئة بينهم[1] .

-الإعتراف القانوني برسائل البيانات بحيث لا ينبغي التمييز بين رسائل البيانات و المستندات الورقية بصرف النظر عن أية إشتراطات قانونية تقتضي وجود "كتابة" أو "محرر أصلي" و هو يمثل مبدأ أساسي عام لا ينبغي قصره على الأدلة القانونية[2] .

-الكتابة التي تيسر الإطلاع على المعلومات أي بشكل مقروء و قابلة للتفسير كضمانة لوجود الدليل الملموس و الذي يؤكد نية الإلتزام لدى الأطراف ، و مساعدة الأطراف على إدراك تبعات إبرامهم للعقد ، فإمكانية قراءته للجميع تكفل بقاء المستند بلا تحريف بمرور الزمن و يوفر سجلا دائما للمعاملات كما أنه يتيح المجال للإستنساخه و لتوثيقه ، و بهذا يكفل أن يكون في شكل مقبول لدى السلطات العامة و المحاكم[3] .

-التوقيع المعترف به في بيئة قائمة على التعاملات الرقمية و هو يقوم مقام التوقيع في التعاملات الورقية و لهذا حددت وظائفه المتمثلة في : تحديد هوية الشخص ، تحديد ما يؤكد يقينا مشاركة ذلك الشخص بالذات في فعل التوقيع ، الربط بين الموقع و المستند . لهذا أعتمد للدلالة على نية الطرف الموقع في الإلتزام بمضمون العقد محل الإبرام ، و على نيته في الإقرار بتحرير النص ، و نية الشخص ربط نفسه بمضمون مستند قد كتبه شخص آخر ، واقعة و زمان وجود شخص في مكان معين[4] .

-الأصل بوصفه واسطة يتم فيها تثبيت المعلومات للمرة الأولى و هي ذات صلة بمستندت الملكية و الصكوك القابلة للتداول ، التي تتسم فكرة الطابع الفريد للأصل ، مع العلم ان مستندات الملكية و الصكوك القابلة للتداول ليست هي الوحيدة التي يتطلب فيها الأصل و من أمثلة الوثائق التي تتطلب

---

[1] المادة الرابعة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص(135)

[2] المادة الخامسة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص(135)

[3] المادة السادسة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص ص(135-136)

[4] المادة السابعة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص(136)

الأصل نجد الوثائق التجارية و التي منها وثائق التصديق على الوزن ، و الشهادات الزراعية ، و تقارير التفتيش ،و شهادات التأمين ، ...الخ ، حيث أن إرسالها دون تغيير أي في شكلها الأصلي أمر لابد منه لأطراف التجارة الدولية لتكون الثقة في محتوياتها للتقليل من إمكانية حدوث تغيير فيها[1] .

-قبول رسائل البيانات و حجيتها الإثباتية بحييث تعتبر كدليل إثبات في الإجراءات القانونية و أنها ذات قيمة بغض النظر عن شكلها الإلكتروني و هذا في مجال الإختصاص القضائي مع أنها تتميز بالتعقيد و هذا تبعا لما اذا كانت قد انشئت او خزنت أو ابلغت بطريقة يعول عليها[2].

-الإحتفاظ برسائل البيانات بواسطة مجموعة من القواعد البديلة للمقتضيات القائمة بشأن تخزين المعلومات لأغراض مثل المحاسبة أو الضرائب و التي قد تشكل عقبات أمام تطوير التبادل التجاري الحديث ، و هذا من خلال الكتابة[3] ، مع التأكيد على انه لا حاجة للاحتفاظ بالرسالة دون تعديل ما دامت المعلومات التي تم تخزينها تعكس بدقة رسالة البيانات على النحو الذي ارسلت به ، مع تناول جميع المعلومات التي تدعو الحاجة لتخزينها[4] .

-تكوين العقود و صحتها من خلال تشجيع التجارة الدولية بتوفير المزيد من اليقين القانوني في اطار ابرام العقود بالوسائل الالكترونية ، من خلال توافر العرض و القبول بالوسائل الالكترونية سواءا كانا مجتمعين في رسالة واحدة او منفصلين ، مع امكانية الدولة المشرعة استثناء تطبيق ذلك[5] .

-اعتراف الاطراف برسائل البيانات التي لا تتعلق بابرام العقود و مثالها الاشعار بالبضائع المعيبة و عروض الدفع و الاشعار بالمكان الذي سينفذ فيه العقد و الاعتراف بالدين ...الخ ، و هذا في اطار اثبات صحة استعمال الوسائل الالكترونية في هذا الصدد[1] .

---

[1] المادة الثامنة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص ص(136-137)

[2] المادة التاسعة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص ص(137-138)

[3] المادة العاشرة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص ص(138-139)

[4] المادة العاشرة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص ص(138-139)

[5] المادة الحادية عشرة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص(139)

-اسناد رسائل البيانات باقامة افتراض بان رسالة البيانات تعتبر في ظروفمعينة رسالة من المنشئ ، مع تقييد ذلك الافتراض في حالة ما اذا كان المرسل اليه قد علم او كان ينبغي ان يكون على علم ، بان الرسالة ليست رسالة المنشئ .

-الاقرار بالاستلام و هو قرار تجاري يتخذه مستعملوا وسائل التجارة الإلكترونية و هذا لاثبات استلام رسالة البيانات.

-زمان و مكان ارسال و تلقي رسائل البيانات عن طريق تحديد وقت الارسال بدخول الرسالة في النظام المعلوماتي و متى كانت متوفرة للمعالجة داخله و لا يهم ان كانت مفهومة او قابلة للاستعمال من جانب المرسل اليه ام لا . كما تم تناول مكان تلقي الرسالة كأن يكون مكان العمل الرئيسي او مكان اخر .

-الأفعال المتصلة بنقل البضائع و مستندات النقل .

ثانيا : قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية 2001

يطبق هذا القانون حيثما تستخدم التوقيعات الإلكترونية في سياق الأنشطة التجارية و هذا لا يلغي أي قاعدة قانونية يكون القصد منها حماية المستهلكين حيث عرفت المادة الأولى منه الفقرة أ، التوقيع الإلكتروني بأنه "بيانات في شكل الكتروني مدرجة في رسالة بيانات أو مضافة اليها أومرتبطة بها منطقيا و التي يجوز أن تستخدم لتعيين هوية الموقع بالنسبة الى رسالة البيانات و لبيان موقفه و لبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات ".

كما يعرف الشهادة بانها رسالة بيانات او سجلا اخر يؤكد ان الارتباط بين الموقع و بيانات انشاء التوقيع ، في حين تعرف رسالة البيانات بانها معلومات يتم انشاؤها او ارسالها او استلامها او تخزينها بوسائل الكترونية او ضوئية او بوسائل متشابهة ، بما في ذلك على سبيل المثال لا الحصر ، التبادل الالكتروني للبيانات او البريد الالكتروني او البرق او التلكس او النسخ البرق . أما الموقع فهو الشخص الحائز على بيانات انشاء التوقيع و يتصرف اما بالاصالة عن نفسه و اما بالنيابة عن من يمثله ، بينما مقدم خدمة التصديق هو الشخص المصدر للشهادات و يجوز ان يقدم خدمات اخرى ذات صلة

[1] المادة الثانية عشرة من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(الجمعية العامة للامم المتحدة) ، نفس المرجع السابق ، ص(139)

بالتوقيعات الالكترونية .و الطرف المعول هو الشخص الذي يجوز له ان يتصرف استنادا الى شهادة او الى توقيع الكتروني

ثالثا : الاتفاقية الدولية الخاصة بالإجرام المعلوماتي المبرمة ببودابست 2001

-تطرقت هذه الاتفاقية للتعاريف الخاصة بأغراض هذه الاتفاقية فعرفت منظومة الكمبيوتر بأنه أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو ذات الصلة بذلك ويقوم أحد أو أكثر منها عن طريق البرامج بعمل معالجة آلية للبيانات .

-بينما يقصد ببيانات الكمبيوتر أي عمليات عرض للوقائع أو المعلومات أو المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكمبيوتر بما في ذلك البرنامج الذي يؤدي لتأدية المهام داخل المنظومة .

-في حين يقصد بجهاز الخدمة أي كيان عام أو خاص للمستخدمي الخدمة الحاصة بهم والذي له القدرة على الاتصال بواسطة منظومة الكمبيوتر، أو أي كيان آخر يقوم بمعالجة أو تخزين بيانات الكمبيوتر نيابة عن خدمة الاتصالات أو مستخدمي هذه الخدمة.[1]

-كما تقوم كل دولة طرف في هذه الاتفاقية بإقرار الإجراءات التشريعية وغيرها من الإجراءات كلما كان ذلك ضروريا لإصدار نصا قانونيا أو تشريعيا الذي يشكل قاعدة لتجريم سلوكات الإعتداء على البيانات في إطار إذا ما تعلق بإتلافها أو إلغائها أو إفسادها أو تغييرها أو تدميرها دون وجه حق [2] .

-و تم تعريف التدخل غي المشروع في منظومة المعالجة الآلية للمعطيات بأنه أي سلوك من السلوكات السابقة الذي يرتكب عن قصد للإعاقة الخطية دون وجه حق لعمل منظومة الكمبيوتر[3].

-في حين تطرقت هاته الإتفاقية لإقرار الإجراءات التشريعية وغيرها من الإجراءات الاخرى كلما كان ذلك ضروريا من خلال النصوص التشريعية أو القانونية التي تصدر من طرف المشرعين الوطنيين وذلك في إطار تجريم الإنتاج أو البيع أو الحصول بغرض الإستخدام أو التوفير لجهاز يشمل برنامج كمبيوتر يتم تصممه أو تطويعه أساسا بغرض إرتكاب أية من الجرائم المنصوص عليها في إطار المادة الثانية من هاته الإتفاقية و المواد ثلاثة وأربعة وخمسة منها، كذلك كلمة السر الخاصة بالكمبيوتر أو الكود الشيفري

[1]– المادة 1 من الاتفاقية الدولية للإجرام المعلوماتي 2001

[2]– المادة 4 من الاتفاقية الدولية للإجرام المعلوماتي 2001

[3]– المادة 5 من الاتفاقية الدولية للإجرام المعلوماتي 2001

للدخول أو بيانات مماثلة تمكن الدخول لمنظومة المعلومات بأكملها أو أي جزء منها بقصد استخدام الجهاز في أغراض خاصة لارتكاب أية من الجرائم الواردة بالمواد من إثنان إلى خمسة، كذلك حيازة إحدى القطع المشار إليها سابقا بقصد استخدامها في أغراض الخاصة بارتكاب جرائم الواردة في المواد أعلاه [1] .

-و تقوم كل دولة طرف في هذه الاتفاقية بإقرار النصوص القانونية التي تشرع تجريم التزوير المتعلق بالكمبيوتر و تجريم التدليس المتعلق بالكمبيوتر كذلك الأعمال الإباحية وصور الأطفال الفاضحة، الإنتهاكات الخاصة بحقوق الطبع والنشر والحقوق المتعلقة بهما[2].

-وتقوم كل دولة طرف في هذه الاتفاقية كذلك بإقرار النصوص القانونية التي تجرم المساعدة أو التحريض أو الشروع في ارتكاب أية جريمة من الجرائم السابقة الذكر عن قصد، دون إغفال تجريم الشخص المعنوي الذي يرتكبها بموجب سلطة تفويض أو سلطة ممارسة السيطرة والتحكم طبقا للمبادئ والأسس القانونية الخاصة للدولة [3]

-وعليه تضمن كل دولة من خلال إقرارها للإجراءات التشريعية المعاقبة على الجرائم السابقة الذكر بموجب عقوبات فعالة ومتناسبة تدعو للعدول عنها والتي قد تشمل الحرمان من الحرية وأي إجراء جنائي أو غير جنائي يتوافق مع متطلبات الردع في إطار السياسة الجنائية الحكيمة والراشدة المنتهجة في كل دولة[4].

-وفي هذا الإطار تم النص على مجموعة من الإجراءات بما في ذلك تجميع الأدلة الخاصة بالجريمة في صورتها الإلكترونية من خلال ضبط الإجراءات التحقيقية وفق إمكانية كل دولة كما أنه تم الاعتماد على الإجراءات الوقائية[5]، كما تم التأكيد على سرعة المحافظة على بيانات الكمبيوتر المخزنة و إصدار الأوامر من خلال منح السلطات المختصة وحق التفويض في توجيه الأوامر التي يمكن من خلالها التوصل لنوعية خدمة الاتصال أو المراسلة المستخدمة والشروط الفنية التي يتم اتخاذها في ذلك والفترة

---

[1]– المادة 6 من الاتفاقية الدولية للإجرام المعلوماتي 2001، يجوز لكل دولة طرف في هذه الإتفاقية التحفظ على الفقرة 1 من هذه المادة ى بشرط ألا يكون هذا التحفظ متعلق بعمليات البيع أو التوزيع .

[2]– المواد 6،7،8،9،10 من الاتفاقية الدولية للإجرام المعلوماتي 2001

[3]– المادتين 11، 12 من الاتفاقية الدولية للإجرام المعلوماتي 2001

[4]– المادة 13 من الاتفاقية الدولية للإجرام المعلوماتي 2001

[5]– المادتين 14، 15 من الاتفاقية الدولية للإجرام المعلوماتي 2001

الزمنية للخدمة، بالإضافة إلى ذلك البيانات الشخصية للمشترك، عنوانه البريدي أو الجغرافي...الخ، وأي معلومات أخرى خاصة بموقع تركيب أجهزة ومعدات الإتصالات.

-كما أنه تم إقرار الصلاحيات القانونية للبحث ومصادرة بيانات الكمبيوتر المخزنة تجميعها في الوقت الصحيح.[1]

-ولتقوية مجال الإجراءات وتوضيحه لكي تكون كل دولة طرف في هاته الاتفاقية على بينة من أمرها تم إقرار حق كل دولة طرف في الاتفاقية بإصدار الإجراءات التشريعية ليشمل أي جريمة ترتكب على أراضيها أو على متن إحدى السفن التي تحمل تلك الدولة الطرف أو بإحدى الطائرات المسجلة بموجب قوانينها أو بمعرفة أحد مواطنيها.[2]

-في حين ختمت هاته الاتفاقية بمبادئ عامة تتعلق بالتعاون الدولي في إطار تسليم المجرمين والمساعدات المتطلبة في إطار الإجراءات.[3]

رابعا: القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها (2004/417)

بناء على مشروع قانون تقدمت به دولة الإمارات العربية المتحدة بخصوص مكافحة جرائم تقنية المعلومات الحديثة في نطاق الأمانة العامة الحديثة في نطاق الأمانة العامة لجامعة الدول العربية ، صدر القانون العربي النموذجي أو الإسترشادي لمكافحة تقنية أنظمة المعلومات وما في حكمها ، ، والذي إعتمده مجلس وزارة العدل العرب في دورته التاسعة عشر بالقرار رقم 495-د 19 -2003/10/8 ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين ، و على إثر ذلك صدر هذا القانون النموذجي و الذي يتضمن القانون العربي الإسترشادي (النموذجي) لمكافحة جرائم تقنية أنضمة المعلومات وما في حكمها ، تجريم الأفعال التالية :

1- الدخول العمد وبغير وجه حق إلى موقع أو نظام معلوماتي.[4]الدخول غير المشروع بقصد الغاء أو حذف أو تدمير أو انشاء أو اتلاف أو تغيير أو بإعادة نشر بيانات أو معلومات شخصية.[1]

---

[1]- المواد 16، 21 من الاتفاقية الدولية للإجرام المعلوماتي 2001

[2]- المادة 22 من الاتفاقية الدولية للإجرام المعلوماتي 2001

[3]- المواد 22- 48 من الاتفاقية الدولية للإجرام المعلوماتي 2001

[4] - المادة الثالثة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمه الصادر عن الأمانة العامة لجامعة الدول العربية (قرار رقم 2004/417) .ا .

2- الدخول غير المشروع بقصد الغاء أو حذف أو تدمير او انشاء أو اتلاف او تغيير أو بإعادة نشر بيانات أو معلومات شخصية.

3- تزوير في أحد المستندات المعالجة في نظام معلوماتي.[2]

4- الإدخال عن طريق شبكة معلومات أو أحد أجهزة الحاسب الآلي وما في حكمها وما من شأنه ايقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو اتلاف أو تعديل البرامج أو البيانات أو المعلومات.[3]

5- اعاقة أو تشويش أو تعطيل العمد وبأية وسيلة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها والوصول إلى الخدمة أو الدخول إلى أجهزة أو البرامج أو مصادر البيانات أو المعلومات.[4]

6- التنصت والإلتقاط أو الاعتراض بدون وجه حق لما هو مرسل عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الالي أو ما في حكمها.[5]

7- استعمال الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها من تهديد أو ابتزاز شخص آخر لحمله على القيام بفعل أو الامتناع عنه ، ولول كان هذا الفعل أو الإمتناع مشروعا.[6]

8- التوصل عن طريق الشبكة المعلوماتية أو أحد اجهزة الحاسب الآلي وما في حكمها إلى الإستيلاء على مال منقول أو على سند أو توقيع هذا السند وذلك بالإستعانة بطريقة احتيالية أو بإتخاذ إسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه.[7]

9- استخدام الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها في الوصول بدون وجه حق إلى ارقام أو بيانات بطاقة ائتمانية وما في حكمها بقصد استخدامها في الحصول على بيانات الغير أو أمواله.[1]

---

[1] – المادة الثالثة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[2] المادة الرابعة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[3] – المادة الثالثة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها .

[4] – المادة السابعة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[5] – المادة الثامنة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[6] – المادة التاسعة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها .

[7] – المادة العاشرة من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها

10- الانتفاع بدون وجه حق عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي في حكمها بخدمات الإتصالات.[2]

11- انتاج أو اعداد أو ارسال أو خزن ما من شأنه المساس بالنظام العام أو الآداب العامة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي.[3]

12- نشر أو نسخ مصنفات فكرية أو أدبية أو ابحاث علمية أو ما في حكمها بدون وجه حق عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها.[4]

13- الدخول بدون وجه حق إللى موقع ؤخاص لشركة أو مؤسسة أو غيرها لتغيير تصاميم هذا الموقع أو الغاء أو اتلاف أو تعديل أو شغل عنوانه.[5]

14- الإعتداء على أي من المبادئ ، أو القيم الدينية أو الاسرية أو حرمة الحياة الخاصة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها.[6]

15- انشاء أو نشر موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بقصد الاتجار بالجنس البشري أو تسهيل التعامل فيه.[7]

16- انشاء أو نشر موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بقصد الإتجار أو الترويج أو التعاطي بالمخدرات أو المؤثرات العقلية وما في حكمها أو تسهيل التعامل فيها.[8]

17- القيام بتحويل الأموال غير المشروعة أو نقلها أو تمويه يالمصدر غير المشروع لها أو اخفائه ، أو القيام بإستخدام أو اكتساب أو حيازة الأموال مع العلم بأنها مستمدة من مصدر غير مشروع أو تحويل الموارد أو الممتلكات مع العلم بمصدرها غير المشروع ، وذلك عن طريق استخدام الشبكة المعلوماتية أو

---

[1] – المادة الحادية عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها

[2] – المادة الثانية عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[3] – المادة الثالثة عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها .

[4] – المادة الرابعة عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها .

[5] – المادة الخامسة عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها .

[6] – المادة السادسة عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[7] – المادة السابعة عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[8] – المادة الثامنة عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حاكمها .

أحد أجهزة الحاسب الآلي وما في حكمها وبقصد اضفاء الصفة المشروعة على تلك الأموال أو انشاء أو نشر موقع لإرتكاب أي من هذه الأفعال.[1]

18- انشاء أو نشر موقع على الشبكة المعلوماتية أو أحد اجهزة الحاسب الآلي وما في حكمها لتسهيل وترويج برامج وأفكار مخالفة للنظام العام.[2]

19- انشاء أو نشر موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما فيحكمها لجماعة ارهابية تحت مسميات تمويهية لتسهيل الإتصالات ببقياداتها أو اعضائها او ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة او المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية.[3]

20- الدخول العمد بغير وجه حق إلى موقع أو نظام مباشر أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها بقصد الحصول على بيانات أو معلومات تمس الامن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو بث أفكار تمس ذلك.[4]

المطلب الثاني : نماذج تشريعية أجنبية داخلية في إطار جرائم الإعتداء على النظام المعلوماتي

أ : النظام القانوني الأمريكي لمكافحة جرائم المعلوماتية

ينظم جرائم المعلوماتية في الولايات المتحدة الأمريكية مجموعة من التشريعات على المستوى الفدرالي وكذلك على المستوى المحلي في مختلف الولايات.

1 - على المستوى الفدرالي

يمثل الفصل (18) من قانون الولايات المتحدة التشريع الرئيس لجرائم التقنية الحديثة ، فقد استجاب الكونغرس لمشكلة جرائم تقنية المعلومات من خلال سن العديد من القوانين الفدرالية كان أولها قانون الاحتيال واساءة استخدام الكمبيوتر ((Computer Fraud and Abuse Act)(CFAA عام 1984 وتم تعديله عام 1986 ومن ثم عدل عام 1994 من أجل التعامل مع مشكلة (الشيفرة الخبيثة) وغيرها من البرامج والتي تهدف إلى تغيير أو اتلاف أو تدمير البيانات على نظام الحاسب.

[1] – المادة التاسعة عشر من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[2] – المادة عشرين من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها .

[3] – المادة واحد وعشرون من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

[4] – المادة الثانية والعشرون من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها.

وينص القسم (1030) [1] من الفصل (18) من قانون الولايات المتحدة على اعتبار الافعال التالية مجرمة :

- التوصل غير المصرح به (الدخول) إلى أحد أنظمة الحاسب للحصول على معلومات أمنية وطنية مع وجود نية لضرر للولايات المتحدة أو لمنفعة دولة أجنبية.
- التوصل غير المصرح به (الدخول) إلى أحد انظمة الحاسب للحصول على معلومات خاصة بأموال محمية.
- التوصل غير المصرح به (الدخول) إلى نظام خاص بالحكومة الفدرالية الأمريكية.
- الدخول غير المصرح به إلى اي نظام مع نية الاحتيال.
- الدخول غير المصرح به إلى اي نظام محمي مع تعمد الحاق اضرار به.
- الاتجار الاحتيالي في كلمات السر الحاسوبية وغيرها من المعلومات التي يمكن استخدامها لإكتساب الوصول إلى نظام محمي.
- الاتجار الاحتيالي في كلمات السر الحاسوبية وغيرها من المعلومات التي يمكن استخدامها لإكتساب الوصول إلى نظام محمي.
- بث أو تهديد بإرتكاب ضرر لأي نظام محمي عبر الولايات أو للتجارة الأجنبية بغرض ابتزاز أموال أو منافع من أي شخص طبيعي أو معنوي.

ويحضر القسم (1462) من الفصل (18) من قانون الولايات المتحدة ، استخدام نظام الحاسب لإستيراد مواد مخلة بالآداب إلى داخل داخل الولايات المتحدة الامريكية، ويحضر القسم (1463) نقل أية مواد فاحشة عبر الولايات أو الجهات الخارجية.

ويجرم القسم (2251) من الفصل (18) توظيف أي قاصر أو اغرائه في المشاركة في أنشطة جنسية بما فيها خلق وتصوير مواد وبثها لجهات خارجية ، أو استخدام نظام الحاسب للإخلال برعاية قاصر بقبول استغلاله مع العلم في انتاج مواد تنطوي على استغلال جنسي . أما القسم (1028) من الفصل (18) من قانون الولايات المتحدة فإنه يعتبر انتاج أو نقل ادارة جهاز يتضمن نظام حاسب يقصد استخدامه بتزوير

[1] – Title 18 Section 1030 of the United States Federal Code.

الوثائق أو انتاج وثائق تعريف مزورة جريمة تعتبر المادة (2319) من ذات القسم الاخلال بحق المؤلف جريمة فدرالية.[1]

كما أصدر الكونغرس عام 2003 قانون مكافحة البريد الإلكتروني غير المرغوب فيه (Anti Spam Law) (The CAN-SPAM ACT of 2003) الذي دون في قسم (1037) من الفصل ((18) من قانون الولايات المتحدة. ويحظر هذا القانون ارسال الرسائل غير المرغوب فيها ، كما ينص على أنه يجب أن تشمل رسائل البريد الإلكتروني آلية تتيح للمتلقي الإشارة إلى أنه لا يريد استقبال هذه الرسائل من المستقبل ، ويهدف هذا القانون أيضا إلى القضاء على عادة الحصول على عناوين البريد الإلكتروني من مواقع الأنترنت.

2 - على مستوى الولايات

ان الاطار العام لتشريعات الولايات المتحدة في حقل جرائم المعلوماتية يمثل بما يلي :

- كل ولاية من الولايات الخمسين تملك حرية التشريع الخاص بها وليس هناك آلية على مستوى الولايات أو المستوى الفدرالي تتطلب تبني الولايات شكلا أو محتوى محددا لقوانينها بالرغم من وجود مشاريع توحيد ومحاولات تصريحات تهدف إلى توحيد التدابير التشريعية ، وقد سنت جميع الولايات قوانين خاصة أو عدلت قوانين العقوبات لديها بما يكفل النص على تجريم أنشطة جرائم تكنولوجيا المعلومات الحديثة ، مع تباين فيما بينها سواء من حيث صور النشاط المجرم ، أو من حيث آلية التعامل مع محل الاعتداء .

- ان الاطار العام لتوحيد قوانين جرائم تقنية المعلومات يعتمد على مشروع قانون نموذجي (Model state computer crimes code) تم وضعه من قبل هيئة أكاديمية عام 1998 ، وفي نطاقه تم تقسيم جرائم التقنية الحديثة إلى الجرائم الواقعة على الاشخاص ، والجرائم الواقعة على الاموال عدا السرقة ، وجرائم السرقة والاحتيال ، وجرائم التزوير ، وجرائم المقامرة والجرائم ضد الآداب عدا الجرائم الجنسية ، والجرائم ضد المصالح الحكومية ، وهذا التقسيم يقوم على فكرة الغرض النهائي أو المحل النهائي الذي يستهدف الاعتداء. وبإستعراض مواقف التشريعات القائمة والنافذة في الولايات الأمريكية ، نجد أن عددا قليلا من الولايات تعاملت مع الجرائم التي تستهدف الاشخاص من غير الجرائم المتعلقة بالمحتوى النفسي ، فلا يوجد أية ولاية نصت على جريمة تقنية حديثة تتعلق بقتل الاشخاص. أما ولايتا (فرجينيا)

---

[1] - James. R. Richards-Transnational Criminal Organisations Cyber Crime and Money Laundering-1999-p.71.

(وكاليفورنيا) فقد اعتبرا استخدام نظام المعلومات الإلكترونية بدون تصريح بنية الحاق الضرر المادي بالأفراد جريمة من بين جرائم التقنية الحديثة.[1]

وقد اعتبر 16 ولاية من بين الولايات الامريكية أن اكلاق التهديدات والمواد التي تثير الاحقاد من قيل الافعال الجرمية ومن معضمها تتطلب أن يكون الجاني قد نقل تهديدا ممكن تطبيقه وممكن تصديقه لإلحاق اصابة بشخص أو ضرر به أو بعائلته أو بأءي شخص آخر. وبعضها اعتبر من بين جرائم السلوك أو المساهمة في ارتكاب سلوك قد يؤدي بالشخص العادي (A reasonable Person) للمعاناة من التهديد أو التعرض لإزعاج حقيقي أو أي ضرر أخر وكذلك الخوف من الإصابة أو الموت على نفسه أو أي من أفراد عائلته. بعضها جرم الإتصالات التي تتضمن مواد بذيئة بأية واسطة الكترونية تستهدف تهديد شخص أو الحاق ضرر به أو بعائلته ويشمل ذلك استخدام لغة فاحشة ، وقد اعتبر محكمة نيويورك أن هذا النص ينطبق على رسائل التهديد والذم التي ترسل عبر الانترنت.

بالإضافة إلى الافعال الجرمية سابقة الذكر ، فإن معظم الولايات الأمريكية تضمنت قوانينها موادا تتعلق بالأفعال التي تستهدف استغلال أو اغواء القصر أو تتعلق بدعارة الأطفال.

وقد اهتمت كافة الولايات الامريكية بشكل أساسي بجرائم تقنية المعلومات المتصلة بالإختراق والحاق رالضرر بالنظم والشبكات والمعطيات جراء هذه الانشطة ، وتنقسم التدابير التشريعية المتصلة بالإختراق إللى طائفتين : طائفة تشريعات انتهاك الحرمة (Trespass) ، وطائفة الهاكرز (Hackers) التي تقوم بأنشطة اختراق وانتهاك الحرمة دون تصريح (Hacking) ، وطائفة الكريكرز (Crackers) التي تقوم بهجمات التدمير انطلاقا من دوافع الحقد (Cracking).

أما بالنسبة للأفعال الأخرى التي تستهدف الأخلاق والآداب العامة ، فإن ولاية أمريكية واحدة فقط جرمت المقامرة على الخط وهي ولاية (Louisiana) فقد اعتبرت هذه الولاية المقامرة بواسطة نظام الحسب جريمة ، ويتضمن ذلك القيام بأي سلوك أو المشاركة بسلوك يتضمن اللعب كالمضاربات بأنواعها تحت خطر خسارة ذلك الشخص أي قيمة ، وذلك بإستخدام أي من وسائط تقنية المعلومات الحديثة.

وبالنسبة للجرائم ضد الحكومة ، اعتبرت العديد من الولايات الأمريكية من قبيل جريمة تقنية المعلومات الحديثة استخدام أي من وسائط لتعطيل تطبيق القانون أو تعطيل خدمة حكومية ، فعلى سبيل المثال

[1] – المادة 15207 –1802 من قانون عقوبات ولاية فرجينيا (VA. CODE. ANN). والمادة 502 من قانون عقوبات ولاية كلفورنيا.

حظر استخدام نظام الحاسب للتسبب بتعطيل أو قطع أي خدمة أو أية عملية أو اجراءات حكومية محلية أو انشطة المؤسسات العامة. والعديد من الولايات جرمت استخدام نظام الحاسب لتعطيل أو قطع أي خدمة أساسية، ويشمل ذلك خدمات المؤسسات العامة والخاصة ذات النفع العام والخدمات الطبية وخدمات الاتصال وكافة خدمات الحكومية، ويشمل أيضا تعريض الأمن العام للخطر.

واعتبرت بعض الولايات استخدام نظام الحاسب للحصول على معلومات تعتبرها الدولة أو أي دائرة سياسية من قبيل المعلومات السرية ، جريمة من جرائم تقنية المعلومات الحديثة، والعديد من الولايات جرمت الدخول غير المصرح به إلى أية معلومات مخزنة داخل نظام حاسب مملوك أو متصل بجهات التشريع بالولاية. كذلك جرمت العديد من الولايات استخدام نظام الحاسب لتدمير أي دليل بقصد تعطيل أي تحقيق رسمي ، كما اعتبرت غالبية الولايات الأمريكية عدم ابلاغ عن جريمة تقنية المعلومات بمثابة جريمة.

ب : النظام القانوني الفرنسي لمكافحة جرائم المعلوماتية

ان التجربة الفرنسية في مجال مكافحة جرائم المعلوماتية ليست أقل نضجا من التجربة الامريكية بل هي كذلك تعتبر من أوائل الدول التي تعاملت مع جرائم تقنية المعلومات تعاملا واقعيا ، بحيث استجابت مبكرة لما تتطلبه مكافحة هذه الظاهرة من خلال التدابير التشريعية[1].

1 – الجرائم التي تقع مباشرة على تكنولوجيا المعلومات والاتصال

نص المشرع الفرنسي على الجرائم التي تقع مباشرة على تكنولوجيا المعلومات والاتصال ، وهي الجرائم المتعلقة بأنظمة المعالجة الآلية للبيانات وسرية وسلامة وتوافر البيانات والمعلومات المعالجة آليا. وبهذا الخصوص جرم المشرع الفرنسي الافعال التالية :

– **الهجمات على النظم المؤتمتة لمعالجة البيانات** :حيث جرم كل من :

* الدخول غير المشروع أو الوصول الاحتيالي إلى نظام آلي لمعالجة البيانات (المادة 323–1 من قانون العقوبات الفرنسي الجديد).

[1] عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية، 2004، ص19–20

* فعل عرقلة أوتشويه وظيفة النظام الآلي لمعالجة المعلومات. (المادة 323-2 من قانون العقوبات الفرنسي الجديد).

* ادخال أو حذف أو التعديل الاحتيالي للبيانات الموجودة في نظام آلي لمعاجلة البيانات. (المادة 323-3 من قانون العقوبات الفرنسي الجديد).

* المشاركة في مجموعة أو الاتفاق على ارتكاب فعل من الأفعال المعاقب عليها في المواد السابقة. (المادة 323-4 من قانون العقوبات الفرنسي الجديد).

* بالإظافة إلى ذلك نص قانون العقوبات على معاقبة محاولة ارتكاب فعل من الافعال سابقة الذكر (المادة 323-7 من قانون العقوبات الفرنسي الجديد) ، وعلى المسؤولية الجنائية للأشخاص الإعتباريين (المادة 323 -6 من قانون العقوبات الفرنسي الجديد).

- انتهاك حقوق الاشخاص الناشئة من الملفات أو البيانات الشخصية المعالجة معلوماتيا

حيث نجده جرم كل من الأفعال التالية :

* فعل معالجة بيانات شخصية آليا من دون أخذ الاحتياطات اللازمة للحفاظ على أمن هذه المعلومات (المادة 226-17 من قانون العقوبات الفرنسي الجديد).

* جمع البيانات الشخصية عن طريق الاحتيال أو باية وسيلة غير مشروعة (المادة – 18 من قانون العقوبات الفرنسي الجديد).

* فعل انشاء أو حفظ بيانات شخصية في شكل الكتروني دون موافقة صريحة من الشخص ؤالمعني ، بحيث أن هذه البيانات تكشف عن الأصول العرقية أو الآراء السياسية أو الفلسفية أو الدينية أو النقابية أو عادات الاشخاص . (المادة 226-19 من قانون العقوبات الفرنسي الجديد).

* الإبقاء على معلومات في شكل الكتروني لمدة تتجاوز المدة المستوجبة لطلب اذن أو تصريح مسبق لتنفيذ المعالجة الآلية. (المادة 226-20 من قانون العقوبات الفرنسي الجديد).

* اساءة استخدام المعلومات اثناء تسجيلها أو تصنيفها أونقلها أو أي شكل آخر من أشكال المعالجة الآلية. (المادة 226-21 من قانون العقوبات الفرنسي الجديد).

* الكشف عن البيانات الشخصية المعالجة آليا التي تؤثر على اعتبار الشخص أو خصوصيته.(المادة 226-22 من قانون العقوبات الفرنسي الجديد).

- خرق قواعد التشفير (قانون 29 كانون الأول 1990)

2- الجرائم الواقعة بإستخدام تكنولوجيا المعلومات والإتصالات :

نص المشرع الفرنسي على الجرائم الواقعة بإستخدام تكنولوجيا المعلومات والإتصال أي الجرائم التي تتم من خلال استخدام غير مشروع لتقنية المعلومات الحديثة.

- الجرائم الواقعة ضد الاشخاص :

* الإعتداء على القصر : أصدر المشرع الفرنسي بعض النصوص لمكافحة وضع الاعتداءات الجنسية وحماية القصر ضحايا هذه الجرائم ، وذلك عندما تستخدم في ارتكاب الجريمة وسائل تكنولوجيا المعلومات والإتصالات (تقنية المعلومات الحديثة) ، فنصت المادة 227-23 من قانون العقوبات الفرنسي الجديد على تجريم افعال نشر أو تثبيت أو تسجيل أو نقل الصور الإباحية للقاصرين.[1]

كما نصت المادة 225-7 من قانون العقوبات الفرنسي الجديد على تجريم فعل القوادة Proxenetisme المتعلقة بالقاصرين بإستخدام وسائل تكنولوجيا المعلومات والإتصالات.

و هذا بالإضافة لما نصت عليه المادة 227-4 من قانون العقوبات الفرنسي الجديد على تجريم فعل تعريض القصر للخطر وعبر تصنيع أو نقل او تثبيت أو تداول اي محتوى ذو صفة عنيفة أو إباحية أو ذو طبيعة تسبب ضررا خطيرا لطرامة الانسان ، من المحتمل أن يشاهدها أو يتداولها قاصر بإستخدام تقنيةالمعلومات الحديثة.

* جرائم التهديد و الإعتداء على حرمة الحياة الخاصة .[2]

* الإعتداء على السمعة والتشهير ، القذف Diffamation غير العلني [3] ، السب Injure غير العلني .

* جريمة افشاء الاسرار (المادة 226-13 من قانون العقوبات الفرنسي الجديد).

- الجرائم الواقعة على الأموال :

* جرائم الاحتيال (المادة 313-1 وما يليها من قانون العقوبات الفرنسي الجديد)

* جريمة الإتلاف (المادة 322-12 من قانون العقوبات الفرنسي الجديد).

- الجرائم الواقعة بإنتهاك قانون الصحافة (قانون 29 تموز 1881 بصيغته المعدلة).

---

[1] - المادة 216-2/1 من قانون العقوبات الفرنسي الجديد .

[2] - المادة 7/217 من قانون العقوبات الفرنسي الجديد

[3] - المادتين 226-10 و 624-3 من قانون العقوبات الفرنسي الجديد

* التحريض على الجرائم والمخالفات (مادة 23 و 24)

* الدفاع عن ارتكاب جرائم ضد الإنسانية (مادة 24)

* التمجيد والتحريض على الإرهاب (مادة 24).

* التحريض على الكراهية العرقية (مادة 24).

* التشهير والإهانة (المواد 30 ، 31 ، 32).**4 – الواقعة بإنتهاك قانون الملكية الفكرية.**

* عمل الفكري بما في ذلك البرمجيات والصوت والضصورة (مادة 335-3/2).

* التعدي على تصميم أو نموذج (مادة 521-4)

* التعدي على العلاقات التجارية (مادة 716-9)

– هتك أو ادارة أو المشاركة في مشروع قمار عبر شبكة الأنترنت.

(مادة 1 من قانون 12 تموز 1983 المعدل بقانون 16 كانون الأول 1992).

– الجرائم المرتكبة بإنتهاك قانون الصحة العامة

* الإتجار بالمخدرات عبر وسائل تقنية المعلومات الحديثة.

* بيع الأدوية عبر وسائل تقنية المعلومات الحديثة دون الحصول على إذن.

الفرع الثاني : نماذج تشريعية عربية في إطار جرائم الإعتداء على النظام المعلوماتي

على المستوى العربي ، سنقتصر في دراسة الحركة التشريعية في شأن مواجهة جرائم المعلوماتية ، على نماذج تشريعية لكل من دولة الإمارات العربية المتحدة والمملكة العربية السعودية والسودان والأردن ، حيث أصدرت دولة الإمارات القانون الإتحادي رقم 2 لسنة 2006 الخاص بمكافحة جرائم تقنية المعلومات الحديثة ، وهذا القانون هو القانون الريادي الأول في العالم العربي الذي يعنى بجرائم المعلوماتية ، ، كذلك اصدار المملكة العربية السعودية بتاريخ 2008/01/24 نظامها الخاص بمكافحة جرائم تقنية المعلوماتن و نختمها بالتنظيم التشريعي الجزائري في إطار تجريم الإعتداء على المنظومة المعلوماتية

أولا: نظام مكافحة جرائم تقنية المعلومات الحديثة في دولة الإمارات العربية المتحدة

(القانون الإتحادي رقم 2 لسنة 2006)

نص القانون الإتحادي رقم 2 لسنة 2006 على تجريم الأفعال التالية :

- **إختراق المواقع والأنظمة الإلكترونية :**

عاقب هذا القانون على جريمة اختراق المواقع وأنظمة المعلومات ، وفرد لتلك الجريمة أنواعا من العقوبة تتدرج وفقا لحالات أربع : حالة القيام بفعل دون ترتب نتيجة ، حالة القيام بالفعل مع ترتب نتيجة متعلقة بإلغاء أو حذف أو تدمير معلومات ، حالة القيام بالفعل مع ترتب نتيجة متعلقة بإنتهاك معلومات شخصية ، حالة القيام بالفعل أثناء أو بسبب العمل أو تسهيل للغير مهمة القيام بهذا الفعل.[1]

– تزوير مستندات معترف بها في نظام معلوماتي :

حيث يعاقب هذا القانون كل من زور مستندا من مستندات الحكومة الإتحادية او المحلية أو االهيئات أو المؤسسات العامة الإتحادية والمحلية المعترف به قانونا في نظام معلوماتي.

– التعطيل او العبث :

من خلال تعطيل الوصل إلى الوسائل أو البرامج أو المعلومات أو الشبكات المتعلقة بتقنية المعلومات [2] أو العبث بالشبكة المعلوماتية أو احدى وسائل التقنية التي يترتب عليها ضرر موصوف .[3]العبث بالفحوص الطبية بإستخدام الانترنت أو احدى وسائل تقنية المعلومات.

– التنصت أو التهديد :

بإستخدام الأنترنت أو إحدى وسائل تقنية المعلومات . التهديد بإستخدام الإنترنت أو بإحدى وسائل تقنية المعلومات .

– السرقة و الاحتيال :

بإستخدام الانترنت أو احدة وسائل تقنية المعلومات والاستيلاء على البطاقات الإلكترونية بإستخدام الأنترنت أو احدى وسائل تقنية المعلومات .

– المساس بالآداب العامة والتحريض عليها و المساس بالأديان و انتهاك حرمة الحياة الخاصة و الاتجار بالبشر أو بالمخدرات و غسل الاموال و الأفعال الإرهابية و والحصول على معلومات حكومية او التحريض على ارتكاب اي جريمة من هذا القانون :

[1] – المادة الثانية من القانون الإتحادي رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات ، منشور في العدد رقم (442) من الجريدة الرسمية لدولة الإمارات العربية المتحدة.

[2] – المادة الخامسة من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات.

[3] – المادة السادسة من القانون الاتحاد رقم 2 في سنة 2006 في شان مكافحة جرائم تقنية المعلومات.

تجريم الدعارة بإستخدم الأنترنت أو احدى وسائل تقنية المعلومات ، أو العبث بالمواقع الإلكترونية على الانترنت ، أو المساس بالأديان بإستخدام الانترنت أو احدى وسائل تقنية المعلومات ، أو انتهاك حرمة الحياة الخاصة عن طريق الانترنت أو احدى وسائل تقنية المعلومات ، أو الاتجار بالبشر عبر الانترنت والاتجار بالمخدرات وغسل الاموال عبر الانترنت، أو انشاء مواقع الكترونية مخالفة للنظام العام والآداب أو استخدام وسائل تقنية المعلومات لهذه الغاية ، أو الأفعال الإرهابية عبر أو بإستخدام وسائل تقنية المعلومات والحصول على معلومات حكومية عبر أو بإستخدام وسائل تقنية المعلومات ، أو التحريض أو التدخل في الجرائم السابق ذكرها في هذا القانون.

ثانيا : نظام مكافحة جرائم تقنية جرائم المعلومات في المملكة العربية السعودية (القانون الصادر بتاريخ 2008/01/24)

نص قانون مكافحة جرائم تقنية المعلومات في المملكة العربية السعودية على تجريم الافعال التالية :

التنصت على ما هو مرسل عن طريق وسائط التقنية أو التقاطها أو اعتراضه .

الدخول غير المشروط لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو امتناع عنه والدخول غير المشروع إلى موقع إلكتروني لتغيير تصاميم هذا الموقع أو الغائه أو اتلافه أو تعديله أو شغل عنوانه والمساس بالحياة الخاصة بالإخرين أو التشهير بالأخرين والحاق الضرر بهم عبر وسائل تقنية المعلومات المختلفة .

- انشاء المواقع للمنظمات الإرهابية على الشبكة العنكبوتية والدخول إلى نظام معلوماتي للحصول على معلومات وبيانات تمس الامن الداخلي والخارجي للدولة أو اقتصادها الوطني.
- الإستيلاء على مال منقول أو على سند أو توقيع هذا السند عن طريق الاحتيال أو انتحال شخصية غير صحيحة ، أو الوصول إلى بيانات بنكية أوائترمانية أو بينات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات أو أموال ، عبر استخدام وسائل وتقنية المعلومات أو الدخول غير المشروع إلى نظام معلوماتي ، والدخول غير المشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو اعادة نشرها وايقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدمير او نسخ البرامج أو البيانات الموجودة

والمستخدمة فيها أو حذفها أو تسريبها أو اتلافها أو تعديلها أو اعاقة الوصول إلى الخدمة او تشويشها أو تعطيلها بأي وسيلة كانت من وسائل التقنية .[1]

- انتاج ما يمس بالنظام العام أو الآداب العامة أو حرمة الحياة الخاصة أو اعداده أو ارساله أو تخزينه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو انشاء موقع على السبكة المعلوماتية أونشره للإتجار في الحنس البشري أو تسهيل التعامل به ، أو انشاء المواد المتعلقة بالشبكات الاباحية أو انشطة الميسر المخلة بالأداب العامة ونشرها أو ترويجها أو انشاءء موقع للإتجار بالمخدرات او المؤثرات العقلية أو ترويجها أو طرق تعاطيها أو تسهيل العامل بها

ثالثا : الإطار القانوني الوطني المتعلق بجرائم الإعتداء على النظام المعلوماتي

و يشمل هذا الإطار نصوص قانونية مختلفة نحصرها فيما يلي :

أ: القانون رقم 15/04 المعدل و المتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات

بحيث احتوى على جرائم مختلفة تستهدف النظام المعلوماتي و هي :

1 – الجرائم المنصوص عليها بالمادة 394 مكرر :

– الدخول غير المشروع و عن طريق الغش للانظمة المعلوماتية .

– البقاء غير المشروع في الانظمة المعلوماتية .تعديل او حذف معطيات المنظومة نتيجة الدخول غير المشروع .

– الإضرار (الإتلاف او التخريب) بنظام التشغيل للمنظومة على اثر الدخول او البقاء غير المشروع .

2 – الجرائم المنصوص عليها في المادة 394مكرر 1:

– ادخال معطيات في منظومة معلوماتية خلسة .

– ازالة او تعدي معطيات في منظومة معلوماتية خلسة .

3 – الجرائم المنصوص عليها في المادة 394 مكرر 2 :

– القيام عمدا و خلسة بتصميم او تجميع او توفير او نشر او البحث عن معطيات تمكن من ارتكاب الجرائم السابقة الذكر .

[1] – المادة الرابعة والخامسة من نظام مكافحة جرائم تقنية المعلومات في المملكة العربية السعودية نفس المرجع، ص (103).

– حيازة او افشاء او نشر او استعمال معطيات متحصل عليها من جرائم المساس بانظمة المعالجة الالية للمعطيات .

4 – تجريم المساعدة و التحريض على ارتكاب الجرائم السابقة الذكر

ثانيا : القانون رقم 15-03 المتعلق بعصرنة العدالة

أ – حيث أنه جاء لعصرنة سير قطاع العدالة من خلال وضع منظومة معلوماتية مركزية لدى وزارة العدل تتعلق بنشاط الوزارة و المؤسسات التابعة لها و مختلف الجهات القضائية و التي تكون محمية بواسطة برنامج يرخص لاستعمال معطيات المنظومة المركزية ، الذي يسمح بتبادل المعلومات بطريقة الكترونية كتابة و قراءة ، و استخدام تقنية المحادثات المرئية عن بعد في الاجراءات القضائية

. – التصديق الإلكتروني

– ارسال الوثائق و الاجراءات القضائية بالطريق الالكتروني

– استعمال المحادثة المرئية عن بعد اثناء الاجراءات القضائية

– الاجراءات

– الاحكام الجزائية

ثالثا: القانون رقم 15-04 المحدد للقواعد العامة المتعلق بالتوقيع و التصديق الالكترونيين

أ – حيث يقصد في مفهوم هذا القانون بالتوقيع الالكتروني بانه بيانات في شكل الكتروني مرفقة او مرتبطة منطقيا ببيانات الكترونية اخرى تستعمل كالرموز او مفاتيح التشفير الخاصة كوسيلة توثيق عبر جهاز او برنامج معلوماتي معد لتطبيق بيانات انشائه من اجل التحقق منها و التي تمنح عبر وثيقة الكترونية تسمى شهادة التصديق الالكتروني تثبت الصلة بين الموقع و هو شخص طبيعي يحوز بيانات انشاء التوقيع الالكتروني و يتصرف لحسابه الخاص او لحساب الشخص الطبيعي او المعنوي الذي يمثله ، و بين البيانات . تلك الشهادة تمنح من مؤدي الخدمات في مجال الترخيص .

ب – مبادئ الممثالة و عدم التمييز اتجاه التوقيع الالكتروني

ج – اليات انشاء التوقيع الالكتروني الموصوف و التحقق منه

د – شهادة التصديق الالكتروني الموصوفة و سلطات التصديق

هـ– النظام القانوني لتادية خدمات التصديق الالكتروني

ي– العقوبات الادارية و المالية و الاحكام الجزائية

الخاتمة

الخاتمة

في ختام دراستنا للآليات القانونية للحماية الجنائية للبيئة الإلكترونية، يمكننا استخلاص عدة نتائج وتوصيات هامة:

أولاً، لقد أظهرت الدراسة أن البيئة الإلكترونية أصبحت جزءاً لا يتجزأ من حياتنا اليومية، مما يستدعي توفير حماية قانونية فعالة لها. وقد سعت التشريعات الوطنية والدولية إلى مواكبة هذا التطور من خلال سن قوانين وتشريعات تهدف إلى حماية الفضاء الإلكتروني وضمان أمن المعلومات.

ثانياً، رغم الجهود المبذولة، لا تزال هناك تحديات كبيرة تواجه الحماية الجنائية للبيئة الإلكترونية. فالطبيعة العابرة للحدود للجرائم الإلكترونية، وسرعة تطور التقنيات المستخدمة فيها، تجعل من الصعب أحياناً ملاحقة المجرمين وإثبات الجرائم.

ثالثاً، لوحظ أن فعالية الآليات القانونية للحماية الجنائية للبيئة الإلكترونية تعتمد بشكل كبير على التعاون الدولي وتبادل الخبرات بين الدول في مجال مكافحة الجرائم الإلكترونية.

رابعاً، أبرزت الدراسة أهمية التوازن بين حماية البيئة الإلكترونية وضمان حرية التعبير وحماية الخصوصية، وهو ما يشكل تحدياً كبيراً للمشرعين.

وعليه، نوصي بما يلي:

- ضرورة مراجعة وتحديث التشريعات المتعلقة بالحماية الجنائية للبيئة الإلكترونية بشكل دوري لضمان مواكبتها للتطورات التكنولوجية المتسارعة.
- تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، من خلال تفعيل الاتفاقيات الدولية وتبادل الخبرات والمعلومات.
- تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، من خلال تفعيل الاتفاقيات الدولية وتبادل الخبرات والمعلومات.

– تطوير قدرات الجهات القضائية والأمنية في مجال التحقيق في الجرائم الإلكترونية وجمع الأدلة الرقمية.

– إنشاء هيئات وطنية متخصصة في أمن المعلومات ومكافحة الجرائم الإلكترونية، تكون مسؤولة عن وضع استراتيجيات وطنية للأمن السيبراني.

– تعزيز التعاون بين القطاعين العام والخاص في مجال حماية البيئة الإلكترونية.

– تكثيف برامج التوعية والتثقيف للمواطنين حول مخاطر البيئة الإلكترونية وسبل الحماية منها.

ختاماً، إن توفير حماية جنائية فعالة للبيئة الإلكترونية يتطلب جهداً متكاملاً يجمع بين التشريع الفعال، التنفيذ الصارم، التعاون الدولي، والتوعية المجتمعية. ورغم التحديات الكبيرة التي تواجه هذا المجال، فإن تطوير وتفعيل الآليات القانونية للحماية الجنائية للبيئة الإلكترونية يبقى أمراً ضرورياً لضمان أمن وسلامة الفضاء الإلكتروني وحماية حقوق مستخدميه.

قائمة المصادر والمراجع

أولا: الكتب

1. نائلة عادل فريد قورة ، جرائم الحاسب الآلي الإقتصادية ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، بيوت 2005 ،
2. أيمن عبد الله فكري ، جرائم نظم المعلومات ، دار الجامعة الجديدة ، الإسطندرية ، 2007
3. هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنيةالمعلومات – مكتبة الألات الحديثة – 1992 –
4. محمد الأمين البشري ، التحقيق في الجرائم المستحدثة ، الطبعة الاولى ، مركز الدراسات والبحوث بجامعة نايف العربية للعلوم الأمنية ، الرياض ، 2004
5. علي حسين الخلف وسلطان عبد القادر الشاوي ، المبادئ العامة في قانون العقوبات ، مطابع الرسالة ، الكويت ، 1982
6. خالد ممدوح ابراهيم ، الجرائم المعلوماتية ، ط1 ، دار الفكر الجامعي ، الإسكندرية ، 2009
7. أسامة أحمد المناعسة وآخرون ، جرائم الحاسب الآلي والأنترنت ، ط1 ، دار وائل للطباعة والنشر ، عمان ، 2001
8. طارق ابراهيم الدسوقي عطية ، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية) ، دار الجامعة الجديدة ، الإسكندرية 2009
9. محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت ، ط2 ، دار النهضة العربية ، القاهرة ، 2009
10. نسرين عبد الحميد نبيه ، الجريمة المعلوماتية والمجرم المعلوماتي ، منشأة المعارف ، الغسكندرية ، 2008
11. عبد الفتاح بيومي حجازي ، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي ، دار الكتب القانونية ، مصر ، المحلة الكبرى ، 2007 ،

12. محمود أحمد عبابنة ، جرائم الحاسوب وابعادها الدولية ، دار الثقافة ، عمان ، 2005

13. محمود أحمد عبابنة ، جرائم الحاسوب وابعادها الدولية ، دار الثقافة ، عمان ، 2005

14. محمد حماد مرهج الهيتي ، التكنولوجيا الحديثة والقانون الجنائي ، دار الثقافة ، عمان ، 2004.

15. قحطان محمد صالح الجميلي ، آلة العصر (الكمبيوتر) ، منشورات مكتبة الشعب ، بغداد ، 1985 ،

16. حسن طاهر داود ، جرائم نظم المعلومات ، الطبعة الأولى ، مركز الدراسات والبحوث ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2000 ،

17. علي بن عبد الله العسيري ، الآثار الأمنية لإستخدام الشاب للأنترنت ، ط1 ، مركز الدراسات والبحوث ، جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2004 ،

18. عبد الله عبد الكريم عبد الله ، جرائم المعلومات والنترنت (الجرائم الإلكترونية) ، ط1 ، منشورات الحلبي الحقوقية ، بيروت ، 2007

19. محمود نجيب حسني – النظرية العامة للقصد الجنائي (دراسة تأصيلية مقارنة في الجرائم العمدية) – الطبعة الثالثة 1988 ، – دار النهضة العربية –

20. رؤوف عبيد ، مبادئ القسم العام من التشريع العقابي، طبعة ثالثة ، 1966 ،دار الفكر العربي

21. أحمد عبد العزيز الألفي ، شرح قانون العقوبات (القسم العام) ، مكتبة النصر الزقازيق ،1995

22. عبد الرحمان جلهم حمزة ، جرائم الانترنت من منضور شرعي وقانوني ، ظافرة للتصميم والطباعة ، بغداد ، بلا سنة نشر

23. فريد منعم جبور : حماية المستهلك عبر الأنترنت ومكافحة الجرائم الإلكترونية دراسة مقارنة ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، بيروت ، لبنان ، 2010

24. نواف كنعان : حق المؤلف –النماذج المعاصرة لحق المؤلف ووسائل حمايته : الطبعة الثالثة 2000

25. أمجد حسان : الفيروسات ارهابا اهدد انظمة المعلومات ، ملتقى الإرهاب في العصر الرقمي ، جامعة الحسين بن طلال ، 10–12 يوليو 2008 ، عمان

المجلات :

1. نائل عبد الرحمان صالح ،واقع جرائم الحاسب في التشريع الأردني ، بحيث مقدم لمؤتمر القانون والكمبيوتر والانترنت الذي نظمته كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة (2000) بحوث مؤتمر القانون والكمبيوتر والأنترنت ، المجلد الأول ، الطبعة الثالثة ، كلية الشريعة والقانون جامعة (الإمارات العربية المتحدة ، 2004 ،

2. غنام محمد غنام – عدم ملاءمة القواعد التقليدية لقانون العقوبات لمكافحة جرائم الكمبيوتر – بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت ، كلية الشريعة والقانون ، جامعة الإمارات ، مايو ، 2004

القوانين:

1. القانون رقم (04/09) ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها ، المؤرخ في 05 غشت 2009، الجريدة رسمية ، العدد 47

2. لأمر 10/07 المؤرخ في 1997/03/06 المتعلق بحق المؤلف والحقوق المجاورة

فهرس المحتويات

فهرس المحتويات