الإطار القانوني للأمن المعلوماتي

Legal Framework for information security

عبد الصدوق خيرة♦
كلية الحقوق والعلوم السياسية -جامعة ابن خلدون تيارت/ الجزائر
مخبر بحث تشريعات حماية النظام البيئي
kheira.abdelsadok@univ-tiaret.dz

بولغاب أمال
كلية الحقوق جامعة الأصالة/ السعودية
amal.bolgab@alasala.edu.sa

تاريخ الإرسال: 2021/10/10 تاريخ القبول: 2021/11/02 تاريخ النشر: 2021/12/28

الملخص:

يعتبر الأمن ألمعلوماتي من أهم المحاور التي تطورت مع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة لا تعد ولا تحصى أو بالأحرى نقل البيانات عبر الشبكة من موقع لآخر و بالتالي يصبح الأمن ألمعلوماتي هاجسا بالنسبة للمتعاملين حيث يعتبر على حسب العديد من الخبراء المعلوماتيين على انه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفرها وتفعيلها لحماية المعلومات إلى أشخاص غير مرغوب فيهم أو غير مخولين عبر شبكات الاتصال فحماية المعلومات من شان القواعد القانونية الإجرائية لتامين أنظمة حماية نظم التشغيل وأنظمة حماية البرامج والتطبيقات وأنظمة حماية قواعد البيانات وأنظمة حماية الولوج أو الدخول إلى الأنظمة المعلوماتية.

الكلمات المفتاحية: الأمن ألمعلوماتي؛ الانترنت الجرائم المعلوماتية؛ التكنولوجيا؛ المعلوماتية

Abstract:

Information security is one of the most important axes that have developed with the development of technology and means of storing and exchanging information in countless different ways, or rather the transfer of data over the network from one site to another, and thus information security becomes an obsession for dealers, as it is considered according to many informational experts on It is the science that works to provide protection for information from the dangers that threaten it or the barrier that prevents it from being attacked by providing tools and means These are necessary to be available and activated to protect information to undesirable

♦ المؤلف المرسل

or unauthorized persons over communication networks, as the protection of information is the legal procedural rules for securing systems to protect operating systems, programs and applications protection systems, database protection systems, and systems to protect access or access to information systems.

Keywords: Information security; the internet; information crimes; technology; informatics

مقدمة:

يعد النظام ألمعلوماتي أهم قاطرة تعبر من خلالها كل المعاملات اليومية من أموال، صفقات اقتصادية، ومعطيات شخصية، إلا أنه لا يمكن التحدث عن نظام معلوماتي فعال وآمن إلا إذا تدخل المشرع الجزائري وأعطى ضمانات قانونية من أجل أمن معلوماتي، هذا الأخير يتجلى من خلال المرونة والثقة والأمل أثناء الاستخدام وفي أي وقت كان، بادر المشرع الجزائري بتأطير عدة استخدامات للتكنولوجيا الحديثة والتي أصبحت نوعا ما معقدة وغامضة لسرعتها واختلافها من بلد لآخر.

إن النظام ألمعلوماتي السائد في الجزائر لايزال في طور الإنجاز والتطوير فمن بين نتائج التطور التكنولوجي في الوقت الراهن، وجود ثمة علاقة ارتباط قوية بين استخدامات الحاسب الآلي، وارتكاب بعض الجرائم المستحدثة، أي استخدام الحاسب الآلي كأداة لارتكاب الأفعال غير مشروعة وسواء كان الحاسب الآلي محلا للجريمة الواقعة على النظام ألمعلوماتي أو وسيلة لها.

فجوهر الأمر في انتشار الوسائل المعلوماتية نتيجة لثورة المعلومات التي تنتشر بسرعة هائلة وتغزو مختلف مجالات الحياة الأمر الذي زاد من فرض انتشار هذا النوع من الجرائم المستحدثة.

إن انعكاسات تكنولوجيا المعلومات أثر بشكل كبير في سن القوانين لجعل هاته الأخيرة أقل خسارة وخطرا على المجتمع.

يهدف هذا البحث إلى تعريف جامع للأمن ألمعلوماتي وتحديد مستوياته والتعرف على الآليات الوطنية والدولية المقررة لمكافحة الجرائم المعلوماتية ومنه نطرح إشكالية هذه الدراسة كالتالي: ما هو الإطار القانوني للحد من الجرائم الواقعة على الأنظمة المعلوماتية وكيف واجهتها التشريعات الوطنية والدولية؟

تتجلى أهمية هذا الموضوع في انه متعلق بعالم افتراضي ويحفظ الأخلاق والمعلومات معا اللذان هم من قبيل كرامة الإنسان وإبراز جهود المشرع الجزائري والجهود الدولية في مكافحة الجرائم الماسة بالمعلوماتية والدعوة إلى التحسيس بهذا الموضوع خصوصا أن الإجرام المعلوماتي واقعة مستحدثة تتطلب مزيدا في البحث والإثراء مقارنة بالجرائم التقليدية.

المحور الأول: الطبيعة الخاصة للجريمة المعلوماتية

1-الطبيعة الخاصة للجرائم الواقعة على النظام المعلوماتي.

أ- نظم الحاسب الآلي والمجرم المعلوماتي.

ب-نظم الحاسب الآلي وعلاقته بالجريمة المعلوماتية.

ج-تصنيفات المجرم المعلوماتي.

2- الأساليب الغير مشروعة في ارتكاب الجريمة المعلوماتية.

أ- الاعتداء على المعدات المادية لأنظمة المعلوماتية.

ب- التقنيات المستخدمة في تدمير المعلوماتية.

المحور الثاني: الحماية القانونية للنظام ألمعلوماتي.

1-أوجه الحماية المختلفة لنظم المعلوماتية في إطار القوانين الخاصة.

أ- صور الحماية القانونية الخاصة لنظم المعلوماتية.

ب- إنشاء الوكالة المختصة في أمن الأنظمة المعلوماتية:

2-الجهود الدولية في مجال حماية الأنظمة المعلوماتية.

أ- التدابير الواجب مباشرتها على المستوى الدولي:

ب-دور الاتفاقيات في مجال التعاون الدولي.

المحور الأول: الطبيعة الخاصة للجرائم الواقعة على النظام المعلوماتي:

إن النظام المعلوماتي بما أنه يمثل كتلة مجموعة ضخمة من البيانات والمعطيات المخزنة وفقا لنظام[1] ، يعجز القانون عن وصفه وكأننا بمجرد البحث في مجال التكنولوجيا، يتقلص دور القضاء، لأنها عبارة عن وحدات حسابية، معطيات، بيانات حيث أفرزت تكنولوجيا المعلومات العديد من المعطيات الإيجابية والسلبية على حد سواء، لعل الإيجابيات ينتفع منها الناس دون معرفتهم أحيانا، بيد أن السلبيات هي التي يجب التنويه عنها لكي يأخذ الناس حذرهم منها، وفي مقدمة تلك السلبيات والتي يجب إظهارها الجرائم التي تتعلق بتكنولوجيا المعلومات، ولكي لا تبقى الرؤية ضبابية أمامنا وأمام كل مهتم، لابد من الإفصاح من تلك الجرائم.

1-الطبيعة الخاصة للجرائم الواقعة على النظام المعلوماتي :

أ-نظم الحاسب الآلي والمجرم المعلوماتي:

لتحدد "دون باركر "الخبير بجرائم الحاسوب[2]، مواصفات مرتكب جريمة الحاسوب وحددها في ثلاثة شروط، يجب أن تتوافر جميعها في الشخص الواحد، ويتزايد أعداد الذين يمتلكون هذه المواصفات، والتي تمكنهم من اختراق الحاسوب وارتكاب جريمتهم في التزوير، وحسب "باركر" هذه الصفات تكمن كالتالي:

1.المعرفة: مع تزايد مستخدمي الحاسوب الشخصي، وازدياد ذوي العلم والمعرفة، خاصة المعرفة بنقاط الضعف المتعلقة بالأنظمة المعلوماتية.

[1] - سلام منعم مشعل محمد سمير صالح، "جرائم تكنولوجيا المعلومات"- رؤية جديدة للجريمة الحديثة، "المجلة الأكاديمية للبحث القانوني، 2017، ص12

[2] - جعفر حسن، جاسم الطائي، "جرائم تكنولوجيا المعلومات"- رؤية جديدة للجريمة الحديثة، ، دار البداية- الطبعة الأولى، عمان، 2017، ص151

2.**القدرة على اختراق وسائل التخزين**، تتميز المعالجة بواسطة الحاسوب باللامركزية الأمر الذي أدى إلى ازدياد استخدام الشبكات ووسائل الاتصال، ونظرا لمستوى المعرفة، لن يجد المستخدم صعوبة في الولوج إلى مواقع خزن البيانات.

3.**القابلية على استخدام الوسائل**، إن زيادة معرفة الأشخاص بالمعلوماتية والحاسوب الأمر الذي هيأ لهذه الفئة أي لأصحاب النوايا السيئة[1] في استغلال وسائل الاتصال وغيرها من مصادر الحاسوب، سواء ما يتعلق منها بالخزن أو المعالجة لتنفيذ الجريمة.

-فالسؤال المهم في هذه النقطة هل الجريمة الواقعة على محتوى الحاسوب تكون من داخل البلد أو خارج أسوار الوطن، هذا يعني أن المجرم قد يكون من البلد أو أجنبي وهل المشرع الجزائري.

ب-نظم الحاسب الآلي وعلاقته بالجريمة المعلوماتية:

إن الجريمة المعلوماتية ترتكب عادة من مجرم محترف يدعى بالمجرم ألمعلوماتي" Delinquan informatique" فكرة جديدة على الفقه الجنائي حيث نترك المجرمين البؤساء وندخل عالم مجرمي المهارات المعلوماتية[2]، أي أن هذا النوع الجديد من الإجرام ألمعلوماتي يعتمد على مستوى عالي من المهارات والتقنية العالية، تمكن المجرم من الاعتداء على المكونات غير المادية كالبيانات والبرامج، لذلك هل النصوص القانونية التقليدية وضعت في حسبانها مواجهة المجرم الحديث.

ج-تصنيفات المجرم ألمعلوماتي:

إن الاختلاف الوحيد بين الإجرام المعلوماتي والإجرام التقليدي، هو وجود التقنية المعلوماتية وأحيانا يمكن للمجرم المعلوماتي الولوج الغير مشروع لذاكرة الآلي لكي يلتقط المعلومات المخزنة، تعديلها أو إتلافها، هنا لابد أن يكون بحوزته حاسا مصغرا ولكمة السر- أو الشيفرة، شرط أن يكون الجهاز مزودا "بمودم" حتى يستطيع استقبال المعلومات ونقلها بواسطة وسيط تيليفوني وبالتالي يمكن القول التغلب على وسائل الأمان والحماية للحاسوب الآلي.

ينقسم المجرمون المعلوماتيون إلى نوعين وفقا لثورة المعلومات:

***-الشباب حديثي العهد بالمعلوماتية:**

نقصد بهذه الفئة الشباب الذين انبهروا بالثورة المعلوماتية فئة لها قدر لابأس به من الخبرة المعلوماتية، ومن ثم هم يمارسون مواهبهم في استخدام الحاسب الآلي بغرض اللهو أو هواية اللعب من أجل الوصول إلى نظم المعلوماتية والعبث بها كما هو الحال اليوم بنظم المعلومات التابعة للمؤسسات العملاقة والوزارات.

فالأمر بالنسبة لهم مجرد تسلية وليس لديهم النية أبدا لارتكاب أفعال الجريمة المعلوماتية، ومع ذلك خطر إنزلاق هاته الفئة إلى احتراف الأفعال الغير المشروعة قد يمس الامن المعلوماتي للدولة.

---

[1]- منير محمد , الجنبيهي محمد وح محمد الجنبيهي، جرائم الإنترنيت والحاسب الآلي ووسائل مكافحتها .الاسكندرية :دار الفكر الجامعي، 2014، ص23.

[2]- محمد , علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الاسكندرية، 2006، ص23.

*الأشخاص المحترفون ارتكاب الجريمة المعلوماتية هو أشخاص تتراوح أعمارهم ما بين 25 إلى 35 سنة، يمثلون نموذجا محترفا في مجال الرسائل المعلوماتية والتكنولوجية وفي إرتكاب الأفعال الغير مشروعة، غالبا ما يكونون موظفون داخل المؤسسة ولديهم العلم الكافي في مجال التقنية[1] للتلاعب بالحاسب الآلي فهذا علم موجه للمعلوماتية بالدرجة الأولى، إما لسرقة المال بدون بذل جهد، أو الحصول على معلومات سرية للإبتزاز أو التشهير، أو لضرب المنافسة ما بين المؤسسات.

من خلال تفحص المادة 394 مكرر وما بعدها المستحدثة لتجريم هذا النوع من الجرائم نلاحظ أن المشرع الجزائري ساير المشرع الفرنسي، إذ لم يعيضها تعريفا دقيقا لنظام المعالجة الآلية للمعطيات كون هذا المفهوم متغير بسرعة وتقني محض ومستمر حسب التطور الهائل للمعلوماتية، واكتفى المشرع بوجوب توافر نظام معالجة الآلية للمعطيات بصفة عامة[2] إلا انه بالرجوع إلى نص المادة من الاتفاقية الدولية للإجرام المعلوماتي الموقع في 23 جوان 2001 نجد أنها قد عرفت نظام المعالجة للمعطيات كالتالي:

كل مركب يتكون من واحدة أو مجموعة وحدات معالجة مرتبطة فيما بينها او مستقلة ليضمن فيها عنصر- أو عدة عناصر لتنفيذ برنامج المعالجة الآلية لمعطيات أن القانون العربي النموذجي الموحد

2-الأساليب الغير مشروعة في إرتكاب الجريمة المعلوماتية:

إن الجرائم المعلوماتية أساسا تنصب على المعلومات، لذا فهو محبب للمجرم ألمعلوماتي بيع أو مقايضة وحتى إتلافها، أما إذا تعلق الأمر بالاعتداء على المعلومات العسكرية فهنا نكون بصدد الاعتداء على أسرار الدولة[3]، ضف إلى ذلك المشروعات النووية ووضع الأسلحة المتطورة وكل ما يمس الأمن القومي جراء تسرب المعلومات، من خلال ذلك يمكن حصر- بعض الصور المتعلقة بالأساليب الغير مشروعة في إرتكاب الجريمة المعلوماتية فيما يلي:

أ-صور الاعتداءات على المعدات المادية للأنظمة المعلوماتية:

إن النظام ألمعلوماتي يتكون من عدة عناصر مادية، وأجهزة تابعة للحساب الآلي عن طريق الكابلات التي كانت فيما مضى معدات كبيرة الحجم، أما اليوم فالتكنولوجيا تعمل على تطوير المعدات بأصغر حجم ولا يزداد في التقلص إلى حد كبير[4] ، هذا ما يسهل أحيانا سرقتها لصغر حجمها، عن طريق أفعال النصب وحتى أن هاته السرقة إلى تجارة دولية غير مشروعة بين أكثر من دولة أو عبر الوطنية والقارات.

[1]- جعفر حسن جاسم الطائي، " جرائم تكنولوجيا المعلومات"، رؤية جديدة للجريمة الحديثة، دار البداية، الطبعة الأولى، عمان، 2017، ص23

[2]- جعفر حسن , جاسم الطائي، المرجع نفسه، ص8.

[3]- غزلان , بوعبدلي، "دور الإدارة الالكترونية في تيسير الحصول على المعلومات "، مجلة المنارة للدراسات القانونية و الادارية عدد خاص حول الثورة الرقمية و اشكالاتها – الرباط، أفريل، 2020، ص20.

[4]- دلال صادق الجود حميد ناصر الفتال، " أمن المعلومات"، اليازوري، 2010، ص76

في هذا الشأن يرى بعض العمال في مجال المعلوماتية ضرورة اتخاذ الاحتياطات المادية، الفنية والأمنية من خلال اللجوء إلى الأنظمة الحديثة لحماية نظم المعلومات سواء عن طريق المخازن المزودة بمراقبة أو حراسة خاصة ضرورة توفير أنظمة الإنذار المبكر[1] وأجهزة المراقبة التلقائية للأشياء المخزنة.

ب-التقنيات المستخدمة في تدمير النظام المعلوماتي:

المقصود بالتقنيات هي التي من شأنها إتلاف أو محو تعليمات البرامج أو البيانات التي يتم معالجتها آليا والهدف من وراء التدمير ينجر من وراءه تحقيق منافع شخصية سواء الاستيلاء على النقود أو مجرد الاطلاع عبر شبكة الأنترنيت وقد تصل الرغبة أحيانا إلى إصابة الحاسب الآلي بالشلل التام وإعاقته عن القيام بأداء وظائفه الطبيعية، هناك عدة وسائل وطرق لتدمير النظام المعلوماتي:

*.الفيروسات: يمكن تعريف الفيروسات على أنها مجموعة من العمليات التي تتكاثر بمعدل سريع وتصيب النظام المعلوماتي بشلل تام، هناك عدة تعريفات للفيروس منها:

*عبارة عن خلية مغناطيسية نائمة ومبرمجة، تنشط في وقت محدد لتخريب البرنامج الأصلي ومنتشرة في الأجهزة الأخرى التي تضمها الشبك بحيث تفسر- ما تحويه من معلومات[2] البعض الأخر يعرفه على أنه " برنامج يصممه بعض المختصين بهدف تخريبي مع إعطاءه القدرة على ربط نفسه ببرامج أخرى ثم يتكاثر وينتشر- داخل النظام حتى يتسبب في تدميره تماما.

من بين خصائص الفيروسات، أنها تضع من طرف فئة مريضة من خبراء البرامج، أما لإثبات الذات أو مجرد الدعاية، أو إلحاق الضرر والأذى، فهاته الفيروسات تتمتع بقدرة فائقة في مهاجمة البرامج وأجهزة الحاسبات، المعطيات، البيانات، والمعلومات وكأن الفيروس الحاسوبي يتشابه مع الفيروس العضوي[3] من حيث عدم جدواه إلا أن الأول يمكن له أن ينتشر- عبر الشبكات ويعبر الدول والقارات وهذه سمة أساسية للجرائم المعلوماتية.

*.أنواع الفيروسات: هناك عدة تسميات لهاته الفيروسات أهمها:

- بوت سكتور"boot sector" يصيب هذا الفيروس جزء من قسم البرنامج، الذي يحتوي على نظام التشغيل والملفات والمعلومات ويتميز بالإنتشار السريع.
- -فايل "file": يصيب هذا الفيروس ملفات Eve، com، ثم يقوم بنسخ نفسه كلما جرى تشغيل البرنامج المصاب.
- فيروس حصان طروادة : هذا الفيروس بالذات حصل نصرا عسكريا وأسطوريا[4] في العصور الوسطى هاته الأخيرة، تمكنت من إختراق أجهزة الحاسبات في أرع دول أوروبية هي إنجلترا، السويد الدانمارك، النرويج.

---

[1]- أمير فرج , يوسف، "التجارة الإلكترونية"، الطبعة الأولى، مصر، 2005، ص62.

[2]- محمد, سامي الشواء، "ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1993، ص45.

[3]- فيروس في اللغة اللاتينية، "سم" عرف هذا المصطلح في مادة العلوم البيولوجية

[4]- إبراهيم , عبد السلام إبراهيم، " فيروس الحاسب الآلي"، مجلة الإدارة العامة معهد الإدارة العامة، الرياض، نوفمبر، 1949، ص125.

■ فيروس الكريسماس: يظهر هذا الفيروس في شكل رسالة بريدية إلكترونية تعرض فيها بطاقة تهنئة للكريسماس على شاشة الحاسب الآلي ومما يترتب عن قبول التهنئة، توقف النظام كليا.

المحور الثاني: الحماية القانونية للنظام ألمعلوماتي:

إن قضية الأمن ألمعلوماتي أصبحت تشغل الكثير من الدول ، لأهميته الأمني ولاستقرار البلدان على برامج معلوماتية ذات ثقة وجودة عالية.

يتسع مفهوم أمن المعلومات ليشمل الإجراءات والتدابير المستخدمة في المجالين الإداري والفني لحماية المصادر البيانية من أجهزة وبرمجيات وبيانات وأفراد، من التجاوزات والتداخلات غير المشروعة[1] التي تقع عن طريق الصنعة أو عمدا عن طريق التسلل أو نتيجة لإجراءات خاطئة أو غير الواقعية المستخدمة من إدارة هذه المصادر فالأمن المعلوماتي يمكن عرقلته عن طريق الخطوات التالية:

– الأخطاء العفوية غير المتعمدة أثناء تجهيز البيانات لإداخلها على الحاسبة.

– حوادث فقدان أو تغير المعلومات بسبب تعطيل الأجهزة أو حصول خلل في البرامج.

– -سرقة المعلومات أو التقاطها وتغييرها بشكل غير مأذون وما ينتج عن هذا من سوء استخدام هذه المصادر.

– -فقدان قدرات إدارة المعلومات نتيجة وقوع بعض الكوارث الطبيعية مثل الفيضانات والكوارث غير الطبيعية مثل الحرائق وحوادث التفجير، رغم أنه هناك أنظمة إحترازية[2] قبل الوقوع في بعض المشاكل كالحريق، أو انتشار الغاز، أو الفيضانات.

في الحقيقة من الصعب جدا اكتشاف أو تتبع التغيرات التي تطرأ على المصادر البيانية بسبب تشعب وتعقد النظم[3] وبالتالي فإن إقامة الأدلة على القائمين بهذه الأعمال يعتبر في غاية الصعوبة.

1-أوجه الحماية المختلفة لنظم المعلوماتية في إطار القوانين الخاصة:

إن الاستخدام المتزايد لتقنية المعلومات في مختلف نواحي الحياة، قد أدى بالمجرمين المعلوماتيين بالتلاعب في البيانات التي يتم تحويلها عن بعد، حيث أن وسائل الاتصالات الدولية ساهمت بشكل كبير في خلق الجريمة المعلوماتية المتعدية للحدود، في هذا الصدد قد راعى الظروف المحيطة بالمعاملات الإلكترونية والمساس بمعطيات بأنظمة المعالجة[4] وذهب إلى سن مجموعة من القوانين كالتالي:

---

[1]- نادر عبدالكريم , الغزواني، "الحماية الجنائية من جرائم الأنترنيت" –دراسة مقارنة، 2009، ص63.

[2]- علي عدنان الفيل، " الإجرام الإلكتروني" –دراسة مقارنة، منشورات زين الحقوقية، الموصل، 2011، ص25.

[3]- عبد الله , حسين علي محمود، " سرقة المعلومات المخزنة في الحاسب الآلي"، دار النهضة العربية، القاهرة، 2002، ص225.

[4]- قانون رقم 09-04 مؤرخ في 05 اوت 2005,متضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها , ج ر العدد 47 صادر بتاريخ 16 اوت 2009.

أ- صور الحماية القانونية الخاصة لنظم المعلوماتية:

– إن القانون رقم 04-15 المتعلق بتجريم المساس بأنظمة المعالجة الأوتوماتيكية للمعطيات مفاده تحديد الجرائم الماسة بالأنظمة المعالجة أوتوماتيكيا للمعطيات في أجهزة الدولة القانون.

– ولعل أهم القوانين الصادرة في هاته السنة بالمرسوم الرئاسي رقم 05/20 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، حيث يؤكد هذا المرسوم أن هاته المنظومة تشكل أداة للدولة في مجال أمن الأنظمة المعلوماتية، وتشكل الإطار التنظيمي لإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها وذلك بإنشاء :

أولا: إنشاء المجلس الوطني لأمن الأنظمة المعلوماتية يتولى هذا المجلس مهام حددها القانون كالآتي:

– البث في عناصر الإستراتيجية الوطنية لأمن الأنظمة من قبل الوكالة وتحديدها.

– دراسة مخطط عمل الوكالة وتقرير نشاطاتها والموافقة عليها.

– دراسة التقارير المتعلقة بتنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والموافقة عليها.

– الموافقة على اتفاقات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال الأنظمة المعلوماتية.

– الموافقة على سياسة التصديق الإلكتروني للسلطة الوطنية للتصديق الإلكتروني[1].

– اقتراح سلامة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية عند الحاجة، ويبدي المجلس رأيه في أي مشروع بنص تشريعي، أو تنظيمي ذي صلة بأمن الأنظمة المعلوماتية، يترأس المجلس الوطني، ووزير الدفاع أو ممثله من رئاسة الجمهورية ممثل عن الوزير الأول، المكلف بالشؤون الخارجية، الوزير المكلف بالطاقة، الوزير المكلف بالتعليم العالي، ضف إلى الاستعانة بأي شخص أو مؤسسة من شأنه تنوير المجلس في أعماله.

– لم يجد المشرع الجزائري يدا من تعديل قانون العقوبات لسد ما كان من فراغ قانوني في هذا المجال، وكان من ذلك بموجب القانون رقم 04-15 المؤرخ في 10-11-2004 المتمم والمعدل للأمر 66-156 المتضمن قانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات، ولقد جاء في عرض أسباب هذا التعديل أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة الإجرام، مما دفع بالكثير من الدول إلى النص على معاقبتها، وأن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، وأن هذه التعديلات من شانها سد الفراغ القانوني[2]

---

[1]- التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية على الموقع: m p u- edition @yahoo.fr.

[2]- سعيداني , نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية، 2012-2013، ص41.

– وقد قدر المشرع في تدخله أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحول إلى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات من أوجه عدة، لك فقد آثر المشرع الجزائري استخدامه لمصطلح المساس بنظم المعالجة الآلية للمعطيات، ويتصرف هذا المصطلح وفقا لدلالة الكلمة إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكات المعلومات، ليخرج بذلك من نطاق تجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة لارتكابها وحصرها فقط في صورة الأفعال التي تشكل اعتداء على النظام المعلوماتي

ب-إنشاء الوكالة المختصة في أمن الأنظمة المعلوماتية:

– هي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية والتي مقرها الجزائر العاصمة[1].

تتميز الوكالة بمهام حددها القانون كالتالي:

– تحضير عناصر الإستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية وعرضها على المجلس.

– تنسيق تنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية المحددة من قبل المجلس.

– الاحترافية في مجال المعلوماتية من طرف قانونين وفئتين في نفس الوقت.

– توفير أكبر قدر من الدراية المعلوماتية والأمن المتعلق بها.

– محاولة تفادي الهفوات المتعلقة بالأمن المعلوماتي خاصة المواقع الحكومية.

– إدخال الطرق التقنية الحديثة في تثبيت الأمن المعلوماتي من خلال البرمجيات الحمائية لصد هجمات الهاكر.

– التطور السريع للتكنولوجيا يجعلنا نفطر في الأمر مرتين وذلك لتطور الفيروسات، ولذلك يجب تحديث الأمن المعلوماتي على حسب متطلبات تكنولوجية.

– نظرا لتعقيدات متعلقة بالأمن المعلوماتي على الدولة تكوي كوادر وإطارات فنية رفيعة المستوى لتغطية الأمن المعلوماتي.

2-الجهود الدولية في مجال حماية الأنظمة المعلوماتية:

لقد أدى ظهور المعلوماتية وتطبيقاتها المتعددة إلى ظهور مشاكل قانونية جديدة في نطاق القانون الدولي[2] وذلك باتفاق دولي ما بين عدة دول عن طريق المصادقة بروتوكولات دولية من بينها:

[1] - مرسوم رئاسي رقم 20-05 مؤرخ في 24 جمادى الاولى عام 1441 الموافق ل 20 جانفي 2020 يتعلق بوضع منظومة لأمن الأنظمة المعلوماتية.ج ر العدد04 ص 05 بتاريخ26 جانفي سنة 2020

[2] - هادي, مسلم يونس البشكاني، " التنظيم القانوني للتجارة الإلكترونية"-دراسة مقارنة، دار الكتب القانونية، مصر، 2005، ص72.

أ.التدابير الواجب مباشرتها على المستوى الدولي:

يمكن تقييم هذه التدابير إلى نوعين، الأولى تتعلق بالتسليم والثاني يتعلق بالتعاون الدولي المتبادل بالنسبة للأول يجب على الدول التعاون فيما بينها من خلال تطبيق المواثيق الدولية[1] ، ذات الصلة بشأن التعاون الدولي في المسائل الجنائية وعلى وجه الخصوص في مجال تسليم المجرم المعلوماتي، هذا الأخير يجب أن يكون وفقا للخطوات التالية:

التسليم: ان مبدأ تسليم المجرمين يقوم على أساس أن الدولة التي يتواجد على إقليمها المتهم بارتكاب إحدى الجرائم المعلوماتية العابرة للحدود مثل جرائم الإنترنت عليها أن تقوم بمحاكمته، إذا كان تشريعها يسمح بذلك،

–تناولت العديد من الاتفاقيات الدولية موضوع تسليم المجرمين، تدعو فيها إبرام معاهدة عالمية لتسليم المجرمين، أهمها المؤتمر الأول للشرطة القضائية في موناكو سنة 1924، والمؤتمر الدولي للعقاب في لندن سنة 1945 وتشكل كل من الاتفاقية الدولية الأوروبية لتسليم المجرمين، و معاهدة " renelux " لتسليم المجرمين سنة 1962 تقدماً ملحوظاً في تطوير قواعد تسليم المجرمين لحد الآن، كما أبرمت على ضوئها العديد من الاتفاقيات الثنائية، واستكمالا لها أصدرت الدول تشريعاتها الخاصة لتحكم نظام تسليم المجرمين من بينها القانون الفرنسي- الصادر في 1927/3/10، وهذا النظام هو في الأصل صياغة للقواعد الدولية المقررة في تسليم المجرمين عبر دول العالم.

ب- دور الاتفاقيات في مجال التعاون الدولي :

سارعت الدول إلى مجابهة إلى مجابهة جرائم الانترنت بصفة عامة لما لها من خطورة على أمنها و استقرارها من خلال إيجاد ترسانة قانونية كفيلة بمواجهتها و قد واجهت الدول جرائم المعلوماتية بعدة مناسبات و اتفاقيات دولية متعددة من بينها الاتفاقية الدولية حول الإجرام المعلوماتي في بودابست الموقعة في 23-11-2001 وهي الاتفاقية بشكل أساسي إلى سواءمة عناصر القانون الموضوعي الجنائي المحلي والأحكام المتصلة بالجرائم في مجال الجرائم الالكترونية والتنصيص على صلاحيات القانون الإجرائي الجنائي الداخلي اللازمة للتخفيف في هذه الجرائم ومتابعتها قضائيا علاوة على الجرائم الأخرى التي ترتكب عن طريق نظام الكومبيوتر والتي تكون الأدلة المتطلب بها في مشكل الكتروني، والى إنشاء نظام سريع وفعال للتعاون الدولي.

يعرف خبراء منظمة التعاون الاقتصادي والتنمية جريمة الكمبيوتر بأنها "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو /ونقلها"، ويتبنى هذا التعريف الفقيه الألماني "ubichsiehr" يعتمد هذا التعريف على معيارين هما : وصف السلوك واتصال السلوك بالمعالجة الآلية للبيانات أو نقلها[2]

[1]- بشرى , النية، " المستهلك السيبيراني في فترة الحجر الصحي : أي حماية-مجلة القضاء و القانون –عدد خاص بفيروس كورونا كوفيد-19 جوان 2020.

[2]- جورج لبكي، المعاهدات الدولية للانترنت"حقائق و تحديات"، مجلة الدفاع الوطني،الموقع الرسمي للجيش اللبناني، 2013، ص10

عرف جريمة الكومبيوتر خبراء متخصصون من بلجيكا في معرض على استبيان منظمة التعاون الاقتصادي والتنميةOECD[1] بأنها "كل فعل أو امتناع عن شانه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[2]

عرفت المادة الأولى من الاتفاقية الدولية للإجرام المعلوماتي النظام المعلوماتي على أنه "يقصد بمنظومة الكومبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو ذات الصلة بذلك ويقدم إحداها أو أكثر من واحد منها تبعا للبرنامج يعمل معالجة آلية للبيانات ويقصد ببيانات الكومبيوتر أية عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكومبيوتر بما في ذلك البرنامج المناسب لجعل منظومة الكومبيوتر تؤدي وظائفها"

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

الخاتمة:

انعكست استخدامات الأنترنت والحاسب الآلي وانتشاره على نحو واسع في حياتنا ظهور فكرة التجارة الالكترونية، وهذه المعاملات تعتمد على وسائل الكترونية، حيث أغلب الجرائم المرتكبة على هاته العناصر لم تحض بتشريع خاص يجرمها وكذلك نسبة للتطور السريع والمتنامي في أساليب ارتكابها، ونظر لأن جريمة الأنترنت التي تمس الأنظمة المعلوماتية هي جريمة تتعدى الحدود الوطنية، أي أثرها يتعدى حدود الدولة المرتكب فيها الفعل الاجرامي، فإن مكافحتها لا يمكن أن تتحقق إلا بتكاتف الجهود الوطنية ووقوفها جنبا إلى جنب مع تلك الجهود الدولية لتدارك صحة الأمن المعلوماتي وملأ الفراغ القانونية حيث يمكن حصر المعوقات المتعلقة بالتعاون الدولي في مجال الأمن المعلوماتي بما يلي:

أولا: اختلاف صور النشاط الاجرامي ما بين دولة وأخرى.

ثانيا: عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة في التحقيق في الجرائم المعلوماتية

ثالثا: عدم وجود معاهدات ثنائية أو جماعية بين الدول في مجال مكافحة الجرائم الماسة بالأمن المعلوماتي

من خلال تسليط الضوء على الإطار القانوني للأمن المعلوماتي يمكن لنا طرح بعض النتائج التي يمكن لها أن تكون مجدية وفعالة مستقبلا:

أولا: تميز الجرائم الواقعة على الأنظمة المعلوماتية بعدم وجود حواجز لا للزمان ولا للمكان ولا حتى بالحدود الاقليمية للدول

ثانيا: إن الفعل المجرم على الأنظمة المعلوماتية صعب الإثبات ولا يترك أثرا

---

[1] -organisation économique de commerce et de développement

[2] - جورج , لبكي، المعاهدات الدولية للانترنت"حقائق و تحديات"، مجلة الدفاع الوطني،الموقع الرسمي للجيش اللبناني، 2013، ص11.

[3] - إعلان فينا بشأن الجريمة والعدالة، مواجهة تحديات القرن الحادي والعشرين صدر عن مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين المنعقد في فينا من 10-17 أفريل 2000.

ثالثا: افتقار كبير لمعظم التشريعات الدولية والوطنية لنصوص قانونية وإجرائية رادعة للجرائم الواقعة على الأمن المعلوماتي

رابعا: الجهل المعلوماتي من قبل الهيئات القضائية المكلفة بالتحقيق وانحصار عمليها على الطرق التقليدية.

خامسا: عدم استحداث معظم الدول لإدارة شرطية جديدة او ما يسمى بشرطة الأمن المعلوماتي.

سادسا: تعزيز اتفاقيات دولية في هذا المجال وتسطير برامج تعاون فيما يخص تسليم المجرمين وتبادل المعلومات مصادرة وتدمير الأثر الإلكترونية والمعلوماتية.

نظراً للتطور السريع في مجال تكنولوجيا الكمبيوتر والإنترنت وشهود الدولة الأوروبية بأهمية إعادة النظر في الإجراءات الجنائية في هذا المجال. فقد أصدر المجلس الأوروبي التوصية رقم 13195 في سبتمبر 1995م في شأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات لحث الدول الأعضاء بمراجعة القوانين الجنائية الوطنية لتلاءم التطور في هذا المجال.

–إن أهم ما ورد في توصية المجلس الأوروبي هو-:

* أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها المعلومات أثناء انتقالها.

* أن تسمح الإجراءات الجنائية لجهة التفتيش بضبط برامج الكمبيوتر والمعلومات الموجودة بالأجهزة وفقاً لذات الشروط الخاصة بالتفتيش العادي.

* تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات.

* يجب إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطات التحقيق لإجراء المراقبة والتسجيل.

* تعين تعديل القوانين الإجرائية بإصدار أوامر لمن يحوز معلومات (برامج – بيانات) تتعلق بأجهزة الكمبيوتر وتسليمها.

* يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة. يتعين عندئذ أن تسمح السلطة الأخيرة بإجراء التفتيش والضبط.

قائمة المراجع:

1. إبراهيم ,"ع " .(1949) .فيروس الحاسب الآلي . "الرياض، نوفمبر :مجلة الإدارة العامة معهد الإدارة العامة.
2. إعلان فينا بشأن الجريمة والعدالة، مواجهة تحديات القرن الحادي والعشرين صدر عن مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين المنعقد في فينا من 17-10أفريل .2000
3. أمير فرج ,يي" .(2005) .التجارة الإلكترونية ."مصر :طبعة أولى.
4. بشرى ,ا " .(2020) .المستهلك السيبيراني في فترة الحجر الصحي :أي حماية-مجلة القضاء و القانون –عدد خاص بفيروس كورونا كوفيد 19-جوان.
5. بشرى ,ا 19) .جوان " .(2020المستهلك السيبيراني في فترة الحجر الصحي :أي حماية -مجلة القضاء و القانون– .عدد خاص بفيروس كورونا كوفيد.19-
6. جعفر حسن ,ج" .(2017) .جرائم تكنولوجيا المعلومات -"رؤية جديدة للجريمة الحديثة .عمان :، دار البداية -الطبعة الأولى.

7. جعفر ,ح .ج " .(2007) .جرائم تكنولوجيا المعلومات"، رؤية جديدة للجريمة الحديثة،) .ا .الأولى (.Éd ,عمان :دار البداية، الطبعة الأولى.

8. جورج ,ل .(2013) .المعاهدات الدولية للانترنت"حقائق و تحديات) ."ا (.Éd ,83 .مجلة الدفاع الوطني،الموقع الرسمي للجيش اللبناني .

9. دلال ,ص .ح " .(2010) .أمن المعلومات ."اليازوري.

10. سعيداني ,ن .(2013-2012) .آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري .مذكرة ماجستير، جامعة الحاج لخضر، باتنة :كلية الحقوق والعلوم السياسية، قسم الحقوق.

11. سلام ,م .م" .(2017) .الحماية القانونية لحقوق الملكية الفكرية الرقمية .Vol)العدد) .(01ا" (.Éd ,15 .المجلة الأكاديمية للبحث القانوني.

12. عبد الله ,ح " .(2002) .سرقة المعلومات المخزنة في الحاسب الآلي ."القاهرة :دار النهضة العربية.

13. علي ,ع " .(2011) .الإجرام الإلكتروني– "دراسة مقارنة .الموصل :منشورات زين الحقوقية .

14. غزلان ,ب" .(2020) .دور الإدارة الالكترونية في تيسير الحصول على المعلومات . "الرباط افريل :مجلة المنارة للدراسات القانونية و الادارية عدد خاص حول الثورة الرقمية و اشكالاتها .–

15. فيروس في اللغة اللاتينية، "سم "عرف هذا المصطلح في مادة العلوم البيولوجية.(.s.d) .

16. قانون رقم .(.s.d) . 04-09مؤرخ في 05اوت ,2005متضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ,ج ر العدد 47صادر بتاريخ 16اوت .2009

17. محمد ,ع" .(2006) .الجرائم المعلوماتية . "الاسكندرية :دار الجامعة الجديدة للنشر .

18. محمد ,س" .(1993) .ثورة المعلومات وانعكاساتها على قانون العقوبات .القاهرة :دار النهضة العربية.

19. مرسوم رئاسي رقم .(.s.d) . 20-05مؤرخ في 24جمادى الاولى عام 1441الموافق ل 20جانفي 2020يتعلق بوضع منظومة لأمن الأنظمة المعلوماتية.ج ر العدد 04ص 05بتاريخ 26جانفي سنة .2020

20. منير محمد ,ا .م " .(2014) .جرائم الإنترنيت والحاسب الآلي ووسائل مكافحتها .الاسكندرية :دار الفكر الجامعي.

21. نادر ,ع" .(2015) .الحماية الجنائية من جرائم الانترنت-"دراسة مقارنة .-

22. نادر عبدالكريم ,ا" .(2009) .الحماية الجنائية من جرائم النترنيت– "دراسة مقارنة.

23. هادي ,م .ي " .(2005) .التنظيم القانوني للتجارة الإلكترونية-"دراسة مقارنة .مصر :دار الكتب القانونية.