جامعة أبو بكر بلقايد – تلمسان

كلية الحقوق والعلوم السياسية

الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني

- دراسة مقارنة -

رسالة لنيل شهادة الدكتوراه في القانون الخاص

إعداد الطالبة:

درار نسيمة

إشراف:

أ.د. ديدن بوعزة

لجنة المناقشة :

– د. بسعيد مراد	أستاذ محاضر "أ"	جامعة تلمسان	رئيسا
– أ.د. ديدن بوعزة	أستاذ	جامعة تلمسان	مشرفا ومقررا
– أ.د. بموسات عبد الوهاب	أستاذ	جامعة سيدي بلعباس	مناقشا
– د. كريم كريمة	أستاذة محاضرة "أ"	جامعة سيدي بلعباس	مناقشا

السنة الجامعية : 2015-2016

جامعة أبو بكر بلقايد – تلمسان

كلية الحقوق والعلوم السياسية

الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني

- دراسة مقارنة -

أطروحة الدكتوراه في القانون الخـــــاص

إشـــــــراف:

أ.د. ديـــــدن بـــــوعزة

إعـــداد:

درّار نســـــــيمة

نوقشـــــت يوم : 2017.01.25

بسم الله الرحمن الرحيم

﴿ نَرۡفَعُ دَرَجَٰتٖ مَّن نَّشَآءُۗ وَفَوۡقَ كُلِّ ذِي عِلۡمٍ عَلِيمٞ ﴾

سورة يوسف، الآية 76

شكر وعرفان

الحمد لله الذي علم الإنسان ما لم يعلم ،و أسدى عليه من العلوم و فهم، و زاده من نعائمه بإسلامه خير مغنم، وحفه بعنايته و حفظه و سلم، و جعله سراجا منيرا في الليل و قد أظلم، ووفى بأحكامه و قواعده ما استجد و ادلهم، والصلاة و السلام على صاحب الوجه الأنوار، و الرأي الأزهر، و الخلق الأكبر محمد بن عبد الله و على اله و صحبه ما أقبل نهار و أدبر.

أما بعد . . .

كان من فضل الله علي أن تولى أستاذنا الكبير "الدكتور ديدن بوعزة" الإشراف على هذا العمل المتواضع وإني لأرجو الله أن يتولى عنا جزاء أستاذنا بقدر ما بذل من جهده و ما ضحى من وقته على عظم تبعاته و تنوع مسؤولياته.

و أتقدم له بجزيل الشكر و عظيم التقدير على توجيهاته و نصائحه العلمية ، فجعله الله ذخرا للعلم و سندا لطلابه

كما و أتقدم بعظيم الامتنان إلى كل من :

أستاذي الدكتور " بموسات عبد الوهاب"

الأستاذة الدكتورة "كريم كريمة "

الأستاذ الدكتور " بسعيد مراد"

و ذلك لقبولهم متكرمين مناقشة رسالتي ، ما زادني فخرا و تكريما .

سائلة المولى عز و جل قبول هذا العمل المتواضع ،معترفة بفضل كل من كان له دور في انجاز هذه الرسالة، داعية المولى عز و جل أن يكون جهدهم في ميزان حسناتهم يوم القيامة.

الإهداء

إلى من كان سببا في وجودي ، و اردعاني بمزيد جود والداي الكريمين

إلى من تحمل معي الكثير ، و عان معي جهد المسير أخي عبد الهادي

إلى منبع الإخلاص ،حنان و محمد و أسماء

إلى صديقة عمري الأستاذة بلخثير نجية

ثم إلى كل من علمني حرفاً أصبح سنا برقه يضيء الطريق أمامي.

بسمة دراجي

قائمة أهم المختصرات

أهم المختصرات العامة :

- ج.ر.ج.ج : الجريدة الرسمية للجمهورية الجزائرية
- د.م.ج. : ديوان المطبوعات الجامعية
- ص : صفحة
- ط: طبعة
- ق.م .ج : القانون المدني الجزائري
- ق.ت.ج : القانون التجاري الجزائري
- ق.ع.ج : القانون العقوبات الجزائري
- ق.إ.ج.ج:قانون الإجراءات الجزائية الجزائري
- ق.ت.ت.إ.ج: قانوني حدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين في الجزائر
- م.ت.إ.خ.إ: مرسوم التنفيذي يحدد شروط وكيفيات وضع واستغلال خدمة الإنترنت.
- ق.ح.م.ح.م : القانون المتعلق بحقوق المؤلف والحقوق المجاورة
- ق.و.ج.ت.إ.م: القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها
- م.س : مرجع سابق

Des abréviations:

- J.O.R.F : Journal officiel de la republiquefrancais
- Op.cit : ouvrage precite
- o.p.u.: office des publications universitaires
- p.u.f. : presses universitaires de France

General terms in information security

- GIAC : Global Information Assurance Certification
- IAB :Internet ActivitésBoard
- IRTF :Internet ResearchTask Force
- IETF : Internet Engineering Task Force
- RFC : Request For Comments
- NIC : Network Information Center
- ISP : Internet Service Providers.
- UCAID : UniversityCorporation for Advanced Internet Développen
- SQL : StructuredQueryLanguage

- DDL :Data DefinitionLanguage
- DML :Data Manipulation Language
- DB : Data Base
- DBA : Data Base Administrator
- DBMS : Data Base Management System
- RDMD : Relation Data Base Management
- ORDBMS : Object-Relational Data Base
- MS : Management System
- LOB : Large Object Binary
- GUI : Graphic User Interface
- PL : ProcedureLanguage
- OLAP : Online AnalyticalProcessing
- SGA : System Global Area
- PGA : Program Global Area
- SID : System Identifier
- ADO : ActiveX Data Objects
- DAO : Data Access Object
- DDE : Dynamic Data Exchange
- UBA : Visual Basic For Application
- RDO : Remote Data Objects
- VBS : Visual Basic Script
- www : World Wide Web
- Com : Commercial Businesses
- Edu: Higher Education
- Org: Organization
- Gov: Government
- Net : Network
- Mil : Military
- http : Hyper text Transfer Protocol
- HTML : HypertextMarkupLanguage
- FTP : File Transfer Protocol
- IP Address: Internet Protocol Address

- ISP : Internet Server Provider
- P.P.P : Point to point protocol
- TCP/IP : Protocol / Internet Protocol
- IIS : Internet Information Server
- PWS : Personal Web Server
- PGP : Pretty Good Privacy
- XML : Extensible Mark up Language
- ASP : Active Server Page
- SSL : Secure Socket Layer
- SET :Secure Electronic Transaction
- SMTP : Simple Mail Transfer Protocol
- FAQ : FrequentlyAsked Questions
- ISDN : Integrated Services Digital Network
- NNTP :Network News Transport Protocol
- POP : Post Office Protocol
- SLIP :Serial Line Internet Protocol
- URL : Uniform Recourse Locator
- IRC : Internet Relay Chat
- CERT : Computer Emergency Response Team
- CIX : Commercial Internet Exchange
- DDN : Defense Data Network
- POD : Department of Defense
- EFF : ElectronicFrontierFoundation
- ANSI : American National Standards Institute
- UCS : Unicode World Wide Character Standard

مـــقدمـــة

مقـــدمـــــــة.

فـــي خضم الصحوة الرقمية، التي تقيم مجدها على سهولة تدفق المعلومات من الشبكة المعلوماتية الكوكبية، وتوفير إنسيابية لمرور البيانات عبر قنواتها، بما يضمن الإستغلال الأقصى لهذه الموارد، عبر متاهة هائلة من مسالك التشعب، اللامتناهية، تسهيلا لمعاملاتنا اليومية.

لكن لكل عالم مثالي جهات ترفض مثاليته،[1] ذلك أن امتلاك زمرة من المستخدمين خبرة رصينة في المعرفةَ المعلوماتية خاصة في جنباتها الخفية السلبية، تسوغ لهم ممارسة أعمال القرصنة على الموجودات المعلوماتية، أو الموجودات التقليدية، وفكّ رموز شفراتها الأمنية، والوصول إلى بنوك المعلومات الوطنية، والعبث بها، بحيث يصعب تعقب الأنشطة غير المشروعة، أو التنبؤ بحدوثها.

هذه الأمور مجتمعة، باتت تحتم إلتماس النظر بمواضيع و قضايا الأمن المعلوماتي، من خلال استخدامات شبكة الإنترنت، فالبيئة المفتوحة التي تتيحها الشبكة لمستخدميها، ووجود برمجيات مجانية على الشبكة، وأخرى في حزم البرمجيات المتوفرة في سوق البرمجيات المحلية، وسهولة استخدامها دون أن نغض البصر عن هيمنة التقنية الغربية على جلّ مفرداتها،الذي بات يشكل خطورة كبيرة على الأمن القومي لكثير من الدول...

لذا يمكن القول أن للعصر الرقمي إفرازات سلبية، تشكل معاناة يتم العمل على التصدي لها بجهود تنجح أحياناً وتخفق أحيانا أخرى، ومن أكبر السلبيات ما اصطلح على تسميته بأمن المعلومات، واستدعى الأمر بناء جوانب قانونية وفنية لحماية المعلومات أو بعبارة أخرى تحقيق "أمن المعلومات"، وبيان المخاطر التي تهدد المعلومات ومصادرها وآليات ووسائل وأدوات الحماية التقنية والإدارية للمعلومات واستراتيجيات حماية المعلومات.

فالأمن المعلوماتي يلمس أمن الثروة الرقمية والثقافية للناس، والمنظمات والبلدان، فالتحديات المعنية معقدة، كما أن التصدي لها يحتاج إلى وجود إرادة قانونية وسياسية، لوضع وتنفيذ

[1]- الحميد نجم عبد الله السامرائي و قطيشات منيب، نظم المعلومات الإدارية ،قواعد البيانات، دار وائل،عمان،2005، ص ص235-236.

إستراتيجية لتنمية البنى الأساسية، والخدمات الرقمية التي تشمل إستراتيجية للأمن المعلوماتي، قابلة للتحقق منها ويسيرة الإدارة وفعالة ومتماسكة.

إن هدف الأمن المعلوماتي هو المساعدة على حماية أصول المنظمات ومواردها من النواحي التنظيمية، والبشرية، والمالية، والتقنية والمعلوماتية[1] بحيث يسمح لها بمواصلة مهمتها، والهدف النهائي هو ضمان عدم تضررها ضرراً دائماً، وهذا يتمثل في تقليل احتمالات تجسد أي تهديد، والحد من الضرر الناجم أو سوء الأداء، وضمان استعادة العمليات العادية لحالتها السابقة خلال إطار زمني مقبول وبتكلفة مقبولة في أعقاب وقوع حادث أمني.

وتشمل عملية الأمن السيبراني المجتمع بأسره، من حيث يكون كل فرد فيه معنياً بتنفيذها، ويمكن دعم ذلك بتطوير مدونة سلوك سيبرانية لأجل الاستخدام السليم لتكنولوجيا المعلومات والاتصالات، وإعلان سياسات أمن واقعية تقنن المعايير التي يكون متوقعاً من مستخدمي الأمن السيبراني (الكيانات والشركاء والموردون) الوفاء بها.

وبإعتبار القانون مرآة عصره فلقد تأثر هو أيضا بزخم و وهج التكنولوجيا، وهو ما دفع إلى توصيفه بعبارة" تكنولوجيا القانون"، أو تقننة أو مكننة القانون"، فقد كان من نتائج هذا التفكير بروز فروع جديدة للقانون تتجاوز عتبة التقسيم التقليدي للقانون- عام و خاص- إلى عتبة التقسيم التقني للقانون كقانون التهيئة والتعمير، الصحة، النقل، المرور، المصرفين، حماية المستهلك، المنافسة، التأمين، الجبائي، البيئي، الملكية الفكرية، مع ظهور قانون المعاملات الإلكترونية أو التجارة الإلكترونية[2]...

---

[1]- المعلوماتية: في معناها الواسع تعني التعامل الفوري مع المعلومة، وهي علم التعامل المنطقي مع المعلومات باعتبارها ناقلة المعارف الإنسانية، والعلاقة وثيقة بين القانون والمعلوماتية، فالقانون يحدد القواعد التي تحكم أنماط السلوك المختلفة والكثير من أنماط السلوك تتعامل الآن مع المعلوماتية كظاهرة تفرض نفسها على الواقع الاقتصادي والسياسي والاجتماعي والحربي،هدى حامد قشقوش، بحث مقدم الى مؤتمر القانون والكمبيوتر والانترنيت للفترة من 1-3/ماي/2000، جامعة الإمارات العربية المتحدة،كلية الشريعة والقانون، ط3، المجلد الثالث، 2004، ص887، لمزيد من التفاصيل في موضوع المعلوماتية أنظر:

- A. Vitalis, Informatique, pouvoir et liberté, 1988, P 22. voir aussi, le Rapport S. Nora et A. Minc, L`informatisation de la société, Point Seuil 1978, P. 11. Et S. Proulx, L`informatisation, mutation technique, changement de société, Sociologie et société1984/1, P 3.

[2]-كريم كريمة،تأثير إستعمال التقنيات الحديثة في تحقيق الأمن القانوني مقال منشور على الرابط التالي manifest.univ-ouargla.dz/...national../KARIM%20Karima.pdf. ص2.

والحقيقة المرة أن معظم الدول النامية لا تعتمد خطة وطنية شاملة، مبنية على استراتيجية مدروسة لحماية معلوماتها و معاملاتها الإلكترونية، لتواكب التطور الذي حصل في أداء الأعمال في العالم المتقدم.

فلا بد من وضع خطة وطنية شاملة *National Information Protection* مبينة على إستراتيجية واضحة ومدروسة جيداً لحماية وأمن المعلومات، تسمح بانسيابية الأعمال ولا تتعارض مع الانفتاحية المعلوماتية ولا تعكر صفو الشفافية المطلوبة لمجاراة العولمة بكل تحدياتها، دون التضحية بالأسرار الوطنية، وهذا ليس بالأمر الهين، بل يتطلب كفاءات متخصصة ومجهود كبير، ينطلق من تخطيط قانوني وتقني سليم، لرسم هذه الخطة التي ستظهر على شكل الإستراتيجية، بسياسات وأنظمة وقوانين وإجراءات مطبقة على نظم الحاسوب، وكذلك مطبوعة في أدلة يتم توزيعها والالتزام بها ومتابعة تنفيذها على مستوى الوطن.

فبظهور طوفان الشبكة العنكبوتية "الانترنت"،[1] والتزايد المستمر لمستخدميها، أصبح هناك مهاجمون ومقتحمون ومتطفلون يقضون الساعات في محاولة اختراق أو سرقة موقع أو الوصول إلي معلومات مهمة وحساسة، تودي بصاحبها إلى عمليات الابتزاز المادي والمعنوي.

---

[1] – الفرق بين الانترنت، الانترانت ، الاكسترانت:

كثرت المصطلحات التي تشير إلى معان متقاربة، فقد بتنا نسمع مصطلح الإنترنت (Internet) والإنترانت (Intranet)والإكسترانت (Extranet)وكلها عبارة عن شبكات أو خدمات شبكية متشابهة تفصل بينها حدود دقيقة وديناميكية تتغير معياريتها من يوم لآخر استنادا إلى ما يستجد في العالم التقني المعاصر.

1 -الإنترنت: الإنترنت هي "شبكة الشبكات" حيث تتكون الإنترنت من عدد كبير من الحاسبات المترابطة في جميع أنحاء العالم . ومعظم استعمالات الإنترنت هي البريد الإلكتروني و(WWW)، ويتصل العديد من مستخدمي الإنترنت المتمرسين ببعض الملفات عبر الانترنت بواسطة بروتوكولات أقل استخداما كـ(FTP) ، (Usent)

وهناك العديد من البروتوكولات الموحدة التي تستخدمها شبكة الإنترنت والبروتوكول الرئيسي المستخدم هو .TCP/IP قدرت الإحصاءات أن هناك أكثر من 30 مليون مستخدم إنترنت اليوم وحوالي 8 إلى 10 منهم يملكون وصولا إلى الويب. تمكن الإنترنت مستخدميها من الاستفادة من عشرات الخدمات المختلفة و التخاطب مع المستخدمين الآخرين . فهي نافذة على العالم بشعوبه و ثقافته و علومه المختلفة ووسيلة اتصال بين الباحثين و رجال الأعمال و الدوائر و القطاعات المشتركة. و يوجد في الإنترنت كم هائل من المعلومات المتجددة و المتنوعة و الشاملة لجميع أنواع الحقول و الميادين إذ بإمكان المستخدم تصفح هذا الكم الهائل و البحث فيه, كذلك فان العديد من الشركات تقدم عشرات الآلاف من البرامج المجانية و التكميلية لمختلف الحاسبات, وبإمكان المستخدم نقل ما يريد من برامج على حاسبه الشخصي و استخدامها.

أيضا فانه يوجد على الإنترنت جميع أنواع الأخبار السياسية والاجتماعية والاقتصادية والفنية والرياضية والمناخية وغيرها. و مؤخرا فقد تكاثرت المجلات و الصحف اليومية و الأسبوعية على الإنترنت. كما تقدم العديد من وكالات الأنباء و الجهات الإخبارية أخبار و تقارير دورية عن أحداث العالم السياسية و الاقتصادية و الرياضية و غيرها.

إذ تمثل البيانات والمعلومات لب اقتصاد المعرفة، والواقع أن الإقتصاديات الحديثة لا تستطيع المحافظة على بقائها، إذا كانت الشبكات والخدمات والبرمجيات والبيانات غير مؤمَّنة، ولذلك يعد الأمن المعلوماتي أحد أكبر التحديات التي تواجه شركات الأعمال، والإدارات والحكومات والمواطنين في القرن الواحد والعشرين.

وعلى الرغم من أن الشبكة العالمية اليوم تعتبر من أوسع البيئات لممارسة المعاملات التجارية المختلفة، إلا أن هذه المعاملات التجارية لن تستمر وتتطور وتصل إلى وضعها المأمول، مالم تقل المخاطر التي تحتويها تلك المعاملات، ذلك أن ضعف ثقة المستهلك بالشبكة العالمية، وقلة اعتقاده بمصداقية الأعمال الالكترونية الموجودة عليها، والتي تعود إلى خوفه من بعض الأمور،التي تتعلق بإتمام عمليات الطلب والشراء عبر الشبكة العالمية من شأنها أن تقف في طريق تقدم التجارة الالكترونية .

وتتمثل تلك المخاوف في:

1. إمكانية اختراق خصوصية المعلومات الشخصية الخاصة، التي يقوم المستهلك بتسجيلها او احتمالية استخدامها في غير مواقعها .

2- الإنترانت: هي عبارة عن شبكة إنترنت مصغرة تكون عادةً شبكة داخلية في الشركة, ذات خصوصية يتم الوصول إليها عبر ملقم تتحكم به أنت تستعمل معايير انترنت من HTML و HTTPوبروتوكول الاتصالات TCP/IP بالإضافة إلى مستعرض ويب رسومي لدعم البرامج التطبيقية وتزويد حلول إدارية بين أقسام الشركة و يمكن أن تكون بسيطة جدا بأن تتألف من ملقم ويب داخلي يتيح للموظفين الوصول إلى كتيبات العمل ودليل الهاتف .كما يمكن أن تكون معقدة جدا بأن تضم تفاعلات مع قاعدة بيانات واجتماعات فيديوية ومجموعات مناقشة خاصة, ووسائط متعددة.

- تستعمل الإنترانت ملقم ويب، لكن خلافا للويب المتوفرة عبر الإنترنت، يكون ملقم ويب في الإنترانت موصول فقط بالشبكة المحلية التي تخص الشركة .وأيضاً تستعمل الإنترانت ملقمات البريد الإلكتروني لإنشاء مجموعات خصوصية للتراسل عبر البريد الالكتروني .
- إذا تستعمل الإنترانت أدوات الانترنت ومعاييرها لإنشاء بنية تحتية، يستطيع الوصول إليها فقط أولائك الذين يعملون ضمن الشركة "سنلاحظ أن كل ما نتعلمه عن الإنترنت يمكن تحقيقه أيضاً بواسطة شبكة إنترانت."ولا يستطيع الوصول إليها من خارج الشركة إلا بتصريح دخول عن بعد، وفي معظم الحالات يستطيع موظفوا الشركة الخروج إلى الإنترنت لكن المستخدمين الغير مرخص لهم لا يستطيعون فعل ذلك... لمزيد من التفصيل أنظر، صالح محمد سعاده و محمد محمود الراميني و علاء علي حمدان، مقدمة إلى الانترنت، مكتبة المجتمع العربي، عمان،2008 ، ص9 .

3- الإكسترانت:شبكة الإكسترانت هي الشبكة المكوّنة من مجموعة شبكات إنترانت ترتبط ببعضها عن طريق الإنترنت، وتحافظ على خصوصية كل شبكة إنترانت مع منح أحقية الشراكة على بعض الخدمات والملفات فيما بينها .أي إن شبكة الإكسترانت هي الشبكة التي تربط شبكات الإنترانت الخاصة بالمتعاملين والشركاء والمزودين ومراكز الأبحاث الذين تجمعهم شراكة العمل في مشروع واحد، أو تجمعهم مركزية التخطيط أو الشراكة وتؤمن لهم تبادل المعلومات والتشارك فيها دون المساس بخصوصية الإنترانت المحلية لكل شركة... لمزيد من التفصيل أنظر، محمد مجبر، مذكرة ماجستير بعنوان التجارة الالكترونية و أفاق تطورها في العالم العربي، جامعة دحلب سعد، كلية العلوم الاقتصادية، جوان 2006 ، ص 16.

2. الشكوك القائمة حول إمكانية الاعتماد على الموقع التجاري الالكتروني، فيما يتعلق بجودة أنظمتها، وإمكانية إتمام عمليات الشراء وما إذا كانت الشركة التجارية، ستقوم فعلا بإيصال السلعة التي تم شرائها.
3. مخاوف استخدام بطاقات الائتمان المصرفية في عمليات الدفع، وقد يعود ذلك إلى إمكانية تعرضه للسرقة جراء تسجيله لبيانات بطاقة الائتمان، والتي عادة ما تكون سرية جدا.
4. كيفية حماية حقوق المستهلك خصوصا وان قوانين الحقوق تختلف من دولة إلى أخرى.
5. غموض سياسات الاسترجاع و التبديل، والمدة المحددة للاستلام ومستلزمات إيصال واستلام البضائع.

ومما لا يتجادل فيه اثنان أن السمة العولمية لشبكات المعلومات وسيادة الفضاء المفتوح، مع غياب المركزية في هذا العالم الشبكي وعدم وجود مرجعية تمسك بزمام أركان السلطة داخل كيان الفضاء المعلوماتي، جعل المجتمع أكثر عرضة للتهديدات المعلوماتية التي قد تعصف بكثير من مرتكزاته المعلوماتية الحيوية .

إضافة إلى وجود ثغرات أمن معلوماتي، نتيجة لتنامي الخبرات لدى لمستخدمين وتقادم التقنيات الرقمية، بسرعة كبيرة تساهم بتعميق المخاطر المحتملة للتهديدات أو الهجمات المعلوماتية.

من جهة أخرى فان السريان الدائم للبيانات والمعلومات من مصادر مجهولة المورد، بات يحتم على المقيمين في مجتمع المعلومات، تبني معايير أمنية محكمة لضمان عدم تسلل الفيروسات الحاسوبية أو قراصنة المعلومات إلى نظم المعلومات، يعيثون بها فسادا وتخريبا[1].

أما عن **أهمية الدراسة و أهدافها** فهي تكمن في:

1. استجلاء طبيعة التهديدات التي تفرضها تقنيات الاتصال الحديثة، وتطبيقاتها في مضمار الأمن المعلوماتي، وكذا تبويبها حسب المنطق القانوني .

2. العمل على إيجاد السبل لمكافحة جرائم المعلومات، ومنع انتشار هذه الظاهرة والحد منها.

وتهدف **دراسة موضوع الأمن المعلوماتي إلى التعرف** على:

[1]- حسن مظفر الرزو، الفضاء المعلوماتي، مركز دراسات الوحدة العربية، بيروت، 2007 ،ص250.

1. العمليات الرئيسة المتصلة بأمن المعلومات ؟
2. جرائم المعلومات التي ترتكب في بيئة المعلومات ؟
3. التوجهات الحديثة لمواجهة ومكافحة جرائم المعلومات، والحد منها بوصفها جرائم ارتبطت بالتقنية؟
4. المخاطر التي تتطلب الحماية وما نقاط الضعف والاعتداءات في بيئة المعلومات؟
5. أفق التعاون الدولي لحماية الفضاء السيبراني؟

الإشكالية :

هل يعتبر الأمن المعلوماتي بإستراتيجياته المتطورة، سلاح مثالي لحماية المعطيات المخزنة رقميا، من المخاطر و التهديدات الإلكترونية ،أم أنه كشف وانتهى الأمر عن قصوره النسبي في توفير التدابير الوقائية ضد تلك التهديدات الأمنية ؟.

خطة الرسالة :

أُستهلت الدراسة مقدمتها بإستعراض ملامح الأمن الرقمي لمختلف التعاملات الالكترونية، و من ثمة تتفرغ الدراسة بعد المقدمة إلى الباب الأول الموسوم بـــ"**الأمن المعلوماتي والمخاطر الرقمية على شبكة الأنترنت**"، يتلو ذلك حديث عن الفصل الأول تحت عنوان تقنية الأمن ألمعلوماتي، والفصل الثاني الذي جاء بعنوان التهديدات الالكترونية في الفلك الرقمي و الحماية القانونية منها، بعد هذه الخلفية العامة، تكون الدراسة قد تهيأت لحديث أكثر تفصيلا في الباب الثاني المعنون بـــ"**التعاون الحمائي في مواجهة مخاطر الأمن المعلوماتي**" بفصليه على التوالي الفصل الأول: سبل مواجهة مهددات الأمن ألمعلومات والفضل الثاني: الجهود الدولية في مجال الأمن ألمعلوماتي.

الباب الأول

الأمن المعلوماتي والمخاطر

الرقمية على شبكة الأنترنت

الباب الأول:

الأمن المعلوماتي والمخاطر الرقمية على شبكة الانترنت.

أضحى هاجس توفير الأمن للمعلومات يقلق بال الكثير من المستفيدين وموفري هذه التقنية الحديثة (الفصل الأول: تقنية الأمن ألمعلوماتي)، وظهر على الساحة مصطلح أمن المعلومات ويقصد به المحافظة على دقة وسرية وتوفر البيانات ضد أي مؤثرات سواءً كانت متعمدة أم عرضية (الفصل الثاني: أشكال التهديدات وواقعها على الأمن ألمعلوماتي).

ويعتبر موضوع أمن المعلومات من المواضيع المتجددة في عالم تقنية المعلومات[1] سيما في ظل الاعتماد الكبير لجميع المؤسسات سواء العامة أو الخاصة على التقنية. ومما لا يخفى على الجميع ما للمعلومات وأنظمتها في عصرنا هذا من أهمية قصوى لكونها تمثل القلب النابض لعمل جميع المؤسسات وتمثل أحد أهم الأصول - إن لم تكن الأهم – مثلها مثل أي أصول ثمينة لدى المؤسسة .

[1]- عرفت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات هذه التقنية بأنها: "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها وتطويرها ومعالجتها وتبادلها وفقاً للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكياً في نظام أو شبكة"، حررت هذه الاتفاقية بمدينة القاهرة –مصر-في 21-12-2010 ، من قبل وزراء الداخلية والعدل العرب وصادقت الجزائر عليها بموجب المرسوم الرئاسي رقم 252/14 مؤرخ في 13ذي القعدة 1435الموافق ل 8 سبتمبر2014،يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ج.ر.ر57.

الفصل الأول: تقنية الأمن المعلوماتي

بدأت الثورة المعلوماتية نتيجة اقتران تقنيتي الاتصالات[1] من جهة، والمعلومات وما وصلت إليه من جهة أخرى، فالثورة المعلوماتية هي الطفرة العلمية والتكنولوجية التي نشهدها اليوم، حتى بات يطلق على هذا العصر عصر المعلومات، وتعد المعلومة أهم ممتلكات الإنسان، اهتم بها، على مر العصور، فجمعها ودونها وسجلها على وسائط متدرجة التطور، بدأت بجدران المعابد والمقابر، ثم انتقلت إلى ورق البردي، وانتهت باختراع الورق الذي تعددت أشكاله، حتى وصل بها المطاف إلى الأقراص الإلكترونية الممغنطة[2].

وباتحاد هاتين الطفرتين في عالم التكنولوجيا، ولد علم جديد هو علم تقنية المعلوماتية Telematique،وهو مصطلح يعبر عن اقتران التقنيتين، ويتكون من الجزء الأول من كلمتي Telecommunication،وهو الاتصال عن بعد، والجزء الثاني من كلمة Information، وتعني المعلومات، وهو علم اتصال المعلومات عن بعد.

– فتقنية المعلومات أضحت ضرورة لأي مجتمع ينشد التطور والتقدم بل التعايش والتفاعل مع عالم اليوم [3]،كما أن الثورة التقنية في العالم قد شملت قطاعاً واسعاً من وسائل نقل وتخزين وبث المعرفة، مثل أجهزة الحاسوب ووسائل النشر والبريد الإلكتروني والإنترنت والوسائل المسموعة والمرئية، فضلاً عن ثورة الاتصالات التي حولت العالم إلى قرية بل إلى غرفة صغيرة، ويمكننا

---

[1]– تتكون شبكة الاتصالات من مجموعة معلومات وموارد إرسال، تعمل معاً وتقدم خدمات الاتصال، وتسمح هذه الخدمات بالنفاذ عن بعد والتشارك في موارد المعلومات المتصلة بينياً، وبالربط البيني للاستخدامات والأشخاص، والتنفيذ عن بعد للبرامج ونقل المعلومات.

[2]– هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط،1992،ص5.

[3]– سعت الجزائر إلى الاستفادة من خدمات شبكة الإنترنت والتقنيات المرتبطة بها، من خلال ارتباطها بشبكة الإنترنت في شهر مارس من عام 1994، عن طريق مركز البحث والإعلام العلمي والتقني (CERIST) – Centre de Recherche et d'Information Scientifique et Technique ، الذي أنشئ في شهر أفريل من سنة 1986 من قبل وزارة التعليم العالي والبحث العلمي، وكانت مهمته الأساسية يوم ذاك، العمل على إقامة شبكة وطنية وربطها بشبكات إقليمية ودولية، و تم في هذا الشأن إصدار المرسوم التنفيذي رقم 98-257 بتاريخ 25 أوت 1998،الجريدة الرسمية، العدد 63، والمعدل بمرسوم تنفيذي آخر يحمل رقم 2000-307 بتاريخ 14 أكتوبر 2000،ج .ر.ع 60 ، الذي يحدد شروط وكيفيات وضع واستغلال خدمة الإنترنت.

- **Le CERIST**, Le Centre de recherche sur l'information scientifique et technique, est un établissement Public Algérien à caractère Scientifique et Technologique sous la tutelle du ministère de l'enseignement supérieur et de la recherche scientifique, Adresse: 05, Rue des 3 Frères-Aissou .BenAknoun, Alger, Algerie.

استثمار هذا الأمر استثماراً إيجابياً بتحقيق التواصل والتفاهم بين مجتمعاتنا والاستفادة من تبادل التجارب والخبرات بما يزيد التضامن والتكافل الإنساني مكانة وقوة[1] .

وفي هذا الفصل سيحاول إلقاء الضَّوء على التعريفات المختلفة لمفهوم الأمن المعلوماتي، في مبحث موسوم بـــ فلسفة الأمن المعلوماتي، ثم يشرع في دراسة المبحث الثاني لمعرفة الأركان الرئيسية للأمن المعلوماتي والتحديات التي يمثلها في الفلك الرقمي .

[1]– انتصار عباس إبراهيم، أثر وسائل الاتصال في خدمات المكتبات ومراكز المعلومات، رسالة ماجستير، الخرطوم، جامعة النيلين،2005 ، ص 8.

المبحث الأول :فلسفة الأمن المعلوماتي

يعد الأمن المعلوماتي من أهم المواضيع التي تشكل أساسا لاستراتيجيات الدول والمنظمات الدولية العالمية والإقليمية، الحكومية وغير الحكومية، لمواجهة مختلف المشاكل التي تهدد استقرار الفضاء الرقمي، والذي سينعكس سلبا على السلم والأمن الدولي، وعلى هذا الأساس يرتكز الأمن الإلكتروني على مفاهيم ذات نطاق وطني وإقليمي وعالمي، ومفاهيم أخرى ذات أبعاد أمنية، وتكنولوجية، واقتصادية وسياسية، واجتماعية، وعسكرية...الخ.

و في نفس السياق يرتكز الأمن المعلوماتي على تعزيز الحماية الناجمة عن تدابير الحد من مخاطر التكنولوجيا الرقمية، بسبب استخدامها المتزايد للأغراض غير القانونية، كما يرتكز على العمليات القائمة على ضمان سرية و سلامة المعلومات و البيانات من كل الهجمات الإلكترونية، و بهذا المفهوم تتعاظم أهمية هذا الموضوع-المطلب الأول- في ظل الحكومات الإلكترونية الذي باتت فيها مسألة الأمن المعلوماتي من أهم التحديات التي تواجهها، إذ تم التأكيد على أولوية هذا التحدي في إطار المنظمات الدولية و الصكوك الدولية و المحافل العالمية،[1] بسبب ارتباطه بالعديد من المخاطر الأمنية والجرائم المنظمة كغسيل الأموال والتحريض العنصري، والإباحية الإلكترونية[2]،

[1]– اتخذت مبادرات من قبل العديد من المنظمات منها: الجمعية العامة للأمم المتحدة، الاتحاد الدولي للاتصالات (ITU)، الإنتربول/يوروبول، منظمة التعاون الاقتصادي والتنمية (OECD)، ومنظمات الأمم المتحدة المعنية بمشاكل المخدرات والجريمة (UNODC)، معهد الأمم المتحدة الأقليمي لدراسة شؤون الجريمة والعدالة، معهد بحوث (UNICRI) ومؤسسة الإنترنت للأسماء والأرقام المخصصة (ICANN) والمنظمة الدولية لتوحيد المقاييس (ISO)، واللجنة الكهروتقنية الدولية (IEC) وفرق عمل هندسة الإنترنت وFIRST منتدى الاستجابة للأحداث ومجموعات الأمن لآسيا والمحيط الهادئ، ومنظمة التعاون الإقتصادي للمحيط الهادئ وآسيا (APEC) ومنظمة الدول الأميركية (OAS) ورابطة دول جنوب شرق آسيا (ASEAN) وجامعة الدول العربية، والإتحاد الأفريقي، ومبادرات فردية من جانب دول نامية أوفي طور النمو، اما المبادرة الأكثر تقدمًا لتنظيم الشبكة العنكبوتية ومحاربة الجرائم الإلكترونية فهي إتفاقية المجلس الأوروبي - Conseil de l'Europe Convention sur la cybercriminalité (STE n° 185)، بشأن الجريمة السيبرانية، وقرارات الأمم المتحدة المختلفة لمنع جرائم الكمبيوتر ومكافحتها، وخطة عمل مؤتمر دول الـ G8 (الدول الصناعية الثمانية)، وجهود الإتحاد الدولي للإتصالات بشأن توحيد آليات تطوير الإتصالات السلكية واللاسلكية. جورج لبكي، المعاهدات الدولية للإنترنت: حقائق وتحدّيات، مجلة الدفاع الوطني اللبناني، العدد 83 ، 2013 ، متوفر على الموقع التالي :.https://www.lebarmy.gov

[2] -la «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle :

a. un mineur se livrant à un comportement sexuellement explicite;

والإرهاب الإلكتروني[1]،و القرصنة الإلكترونية و التجسس الصناعي و غيرها.

و فيما يلي سنبحث في مدى أهمية الأمن المعلوماتي وما هي الغاية منه؟ في مطلب أول، ثم في المطلب الثاني سنشرع في دراسة المفهوم القانوني للمعلومات.

---

b. une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;

c. des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite ,Article 9,Infractions se rapportant à la pornographie enfantine

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:

a. la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique .
b. l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique.
c. la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique.
d. le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique.
e. la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques ,Convention sur la cybercriminalité,Budapest,23.11.2001,Disponible sur:http://conventions.coe.int/Treaty/fr/Treaties/Html/185.

– كما جرمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010في مادتها12 على جريمة الإباحية:

1. إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات.
2. تشدد العقوبة على الجرائم المتعلقة بإباحية الأطفال والقصر.

يشمل التشديد الوارد في الفقرة (2) من هذه المادة، حيازة مواد إباحية الأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات.

[1]– المادة 15: الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات:

1. نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.
2. تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.
3. نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.
4. نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

المطلب الأول : ما أهمية الأمن المعلوماتي و ما هي الغاية منه؟

شاع استخدام مصطلح ''أمن المعلومات'' في نطاق أنشطة معالجة ونقل البيانات بواسطة أنظمة الحاسب الآلي،[1] على الرغم من ظهور الحاجة إليه قبل استحداث وسائل التكنولوجيا الحديثة للمعلومات، وباستبدال الطرق التقليدية لحفظ وتخزين ومعالجة المعلومات بالطرق الالكترونية الحديثة، أصبحت تلك المعلومات مهددة أكثر مما كانت عليه في السابق، بحيث يسهل الوصول إليها أكثر من ذي قبل، وبذلك أصبحت الحاجة إلى أمن المعلومات حاجة أساسية، واحتلت مساحة واسعة من الأبحاث والدراسات وباتت هاجسا يؤرق العديد من الجهات .

– وبنظرة عامة إلى مصطلح امن المعلومات، نجد أنه يشير إلى توفر السرية والموثوقية للمعلومات واكتمالها وضمان استمرارية وجودها، وإمكانية التحقق من كل تصرف أو كل معالجة مطبقة عليه. [2]

الفرع الأول : تطور مفهوم الأمن المعلوماتي

إن مفهوم الأمن المعلوماتي مر بمراحل تطويرية عدة أدت الى ظهور ما يسمى بأمنية المعلومات، [3] ففي الستينات كانت الحواسيب هي كل ما يشغل العاملين في أقسام المعلومات، و كان همهم هو كيفية تنفيذ البرامج و الإيعازات و لم يكونوا مشغولين بأمن المعلومات، بقدر انشغالهم بعمل الأجهزة و كان مفهوم الأمنية يدور حول تحديد الوصول أو الإطلاع على البيانات من خلال منع الغرباء الخارجيين من التلاعب في الأجهزة، لذلك ظهر مصطلح أمن الحواسيب ***Computer Security*** و الذي يعني حماية الحواسيب و قواعد البيانات، و نتيجة للتوسع في استخدام أجهزة

---

[1]– عبدالرحمن بن عبدالله السند، أحكام تقنية المعلومات، الحاسب الآلي وشبكة المعلومات، رسالة الدكتوراه في الفقه المقارن، جامعة الإمام محمد بن سعود الإسلامية، المعهد العالي للقضاء، قسم الفقه المقارن، 2005 ، ص 30 و ما بعدها .

[2] -D. Marcus Odom Anand Kumar and Laura Saunders, Web Assurance Seals How and Why they Influence Consumers Decisions ? Journal of Information Systems, Vol.16 No. 2, Fall 2002, pp. 231-250.

[3] - Laurent Bloch et Christophe Wolfhugel, Sécurité informatique - Principes et méthode, Eyrolles, 3e édition ,2011,pp9-17.Voir aussi , Gustave KOUALOROH , Audit et definition de la politique de sécurité du réseau informatique de la first bank, Université de Yaoundé I, Cameroun, Master professionnel en réseaux , applications multimédia ,2008, PP1-4. Et Kevin Freoa, La sécurité informatique dans l entreprise, projet professionnel, Dess droit et pratique du commerce électronique, université paris, René descarte,2004 ,p7.

الحاسوب و ما تؤديه من منافع تتعلق بالمعالجة للحجوم الكبيرة من البيانات، تغير الإهتمام ليمثل السيطرة على البيانات و حمايتها.

و في السبعينات تم الانتقال الى مفهوم أمن البيانات ***Data Security*** ورافق ذلك استخدام كلمات السر البسيطة، للسيطرة على الوصول للبيانات إضافة الى وضع إجراءات الحماية لمواقع الحواسيب من الكوارث، و اعتماد خطط لخزن نسخ اضافية من البيانات و البرمجيات بعيدا عن موقع الحاسوب، و في مرحلة الثمانينات و التسعينات ازدادت أهمية استخدام البيانات، و ساهمت التطورات في مجال تكنولوجيا المعلومات بالسماح لأكثر من مستخدم للمشاركة في قواعد البيانات، كل هذا أدى الى الإنتقال من مفهوم أمن البيانات الى أمن المعلومات، وأصبح من الضروري المحافظة على المعلومات و تكاملها و توفرها و درجة موثوقيتها، حيث أن الإجراءات الأمنية المناسبة يمكن أن تساهم في ضمان النتائج المرجوة و تقلص اختراق المعلومات و التلاعب بها[1].

- كما أن أمن المعلومات هو قضية تبحث في نظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.
- ومن زاوية تقنية، هو الوسائل والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية .
- ومن زاوية قانونية، فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهذا هو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها[2].

[1]–نايف شايع حسن الدوسري، سلمان بن محمد سلمان ،الأمن المعلوماتي ،جامعة نايف العربية للعلوم الأمنية، كلية العلوم الادارية، المملكة العربية السعودية ،2013، ص 7 و ما بعدها

[2]– شريف درويش اللبان، خبرة عربية منقوصة، أمن المعلومات في ظل تحديات البيئة الرقمية، المركز العربي للبحوث و الدراسات، 2015 ، متوفر على الموقع التالي : http://www.acrseg.org

الفرع الثاني: أهمية الأمن المعلوماتي.

من المعروف منذ عقود عديدة إن المعلومات هي من أهم مصادر القوة، ليس فقط للأشخاص والمختصين، كل في مجاله، ولكن ايضا للمؤسسات والشركات وللدول كذلك، وكلما كانت تلك المعلومات حديثة ومتكاملة وشاملة بالنسبة للمجال الذي تتعامل معه، كلما كانت أكثر أهمية وفائدة وتأثيرا بالنسبة لمستخدميها والمعنيين بها. ومن هنا ظلت المعلومات ونتائج البحوث العلمية من أسرار الدول، خاصة وانه يتم الانفاق عليها بشكل كبير.

– وعندما بدأت شبكة المعلومات العالمية في التوسع والوصول إلى أصقاع العالم،

ومع ما صاحب تطورها من تعدد الوسائل والسبل والتطبيقات المرتبطة بها، واكتسابها أهمية بالغة خاصة فيما يتصل بالاعتماد على تقنية المعلومات في عمليات تشغيل العديد من المرافق، بدءا من مرافق البنية الأساسية كمحطات المياه والطاقة ووسائل النقل، والبنوك ومراكز التحكم، ووصولا إلى تطبيقات ومجالات عديدة في قطاعات الدفاع والأمن والشرطة وغيرها، ازدادت أهمية وحيوية الحفاظ على الأمن المعلوماتي، بمستوياته المختلفة، ليس فقط للحفاظ على عمليات تشغيل وتطوير هذا القطاع الحيوي بمشتملاته المختلفة، ولكن أيضا لحمايته ضد محاولات الاختراق، سواء عبر قراصنة محترفين، أو من خلال هجمات فيروسية، أو غير ذلك.[1]

الفرع الثالث : الغاية من الأمن المعلوماتي

يكمن الهدف الأساس لأمن المعلومات وراء مبدأ حماية الموجودات المعلوماتية للمؤسسات الحكومية والأفراد، منَ الهجمات والاختراقات التي تستهدف استخدامًا غير مشروع لمواردها، أو إحداث خلل في هيكليتها أو محتواها.[2]

– بصورة عامة، تنبثق السياسة الأمنية لمؤسسة ما من مجموع السياسات الفنية

[1]– سيف بن سعود المحروقي، الأمن المعلوماتي ضرورة وليس ترفا،2 فبراير 2015م،متوفر على الموقع التالي :
http://omandaily.com

[2] -B.McDermott, E.Geer, Information security is information risk management In Proceedings, of the 2001 Workshop on New Security Paradigms, NSPW 01, pp. 97 – 104.

والاقتصادية، التي تنتهجها في تسيير دفَّة أنشطتها، فتصنِّف على ضوئها البيانات التي تقيم في نظامها المعلوماتي، وأساليب تداوُلها بين مختلف مستويات الكوادر العاملة، وسُبُل المحافَظة عليها منَ الانتشار والإعلان، وحمايتها من موارد الخَلَل والتَّلَف.

- لا زالتِ الإدارات المعلوماتية، والجهات المستفيدة منَ الخدمات المعلوماتية بشتى مستوياتها في الجزائر و الوطن العربي – تفتقر إلى رؤية واضحة عن مقومات الأمن الوطني المعلوماتي، والتي تعتبر الركيزة الأساسية لتحقيق الكفاية الأمنية لنظم المعلومات؛ ولكي تتحقق الخطوة الأولى على طريق صياغة سياسة أمن معلوماتي واضحة المعالِم لهذا الموضوع الحيوي، والتوجه صوب إعداد خطط محكمة لإعداد ملاكات معلوماتية، تنهض بأعباء مهام حماية الأمن المعلوماتي الوطني.[1]

- كما يشكل أمن الأنظمة والشبكات وحماية الخصوصية والبيانات الهاجس الأكبر

لجميع الشركات والمؤسسات في عصر الاقتصاد الرقمي وتقنية المعلومات، الذي بات فيه كل شيء مستنداً إلى تقنيات الحوسبة والإنترنت والشبكات، ومن الطبيعي أن يتصاعد القلق حيال مسألة أمن البيانات في ظل ازدياد المخاطر الأمنية على اختلاف أنواعها، كالاختراقات والثغرات والفيروسات، ناهيك عن الخسائر الضخمة التي من الممكن أن تتكبدها الشركات والمؤسسات جراء تعرضها لمشكلة أمنية حقيقية أو مجموعة مشكلات

ولهذا السبب تعكف الكثير من الشركات المتخصصة في أمن الأنظمة وحماية البيانات على تطوير أفضل برامج الجدران النارية ومكافحة الفيروسات، في محاولة منها لمنع حدوث الكوارث وما يترتب عليها من ويلات، ولعل أفضل وسيلة يمكن اتباعها لضمان أقصى حماية ممكنة للشبكات والبيانات، تتمثل في تبني منظومة أمنية متعددة الطبقات مصحوبة بسياسة احترازية دقيقة الإجراءات[2].

* لماذا أمن شبكات المعلومات؟

---

[1] -Paul Taylor, How Ethical Hackers Pinpoint Security Weakness, Financial Times, September 3rd ,1997 , pp. 1-2.

[2] - http://www.itp.net.

يشكل أمن المعلومات في العصر الحديث حجر الزاوية في علميات نهضة تكنولوجيا المعلومات والاتصالات، حيث أن المساهمة المتاحة للخصوصية تتناسب عكسياً مع التقدم التكنولوجي المعلوماتية والاتصالات، لقد أنهينا في الفقرات السابقة إيضاح أهمية شبكات المعلومات للجميع، وبالتالي فإنه من البديهي أن يكون لهذه الأهمية درجة من الحماية تتدرج في الأهمية بتدرج أهمية المعلومات المخزنة في هذه الشبكات، للإجابة على هذا السؤال لابد لنا أن نعرض بعض النماذج التي تم فيها اختراق بعض الشبكات لنبين أهمية أمن الشبكات والمخاطر التي يمكن ان تحدث في حالة عدم توفره.

1. الحالة الأولى: في عام 2002 اكتشفت شركة *Daewoo Securities* أن ما قيمته 21.7 مليون دولاراً من الأسهم التي تديرها قد بيعت بشكل غير قانوني، وذلك نتيجة مباشرة لاختراق شبكة الحاسوب الخاصة بها.[1]
2. الحالة الثانية: في عام 2003 قام موظف بإحدى الشركات الروسية باختراق شبكة المعلومات الخاصة بالشركة، وقام بتعديل راتبه الشهري ومجموعة من زملائه بزيادة الرواتب بنسبة معينة، مما أدى بخسائر مالية للشركة لعدة شهور لعدم اكتشاف هذا الاختراق[2].
3. يمكن أن نرى مدى الخسائر التي تمثلها مثل هذه الاختراقات الأمنية لشبكات المعلومات، سواء كانت هذه الخسائر مالية كما في حالة الشركات أو خسائر معلوماتية واستخباراتية لا تقدر بمال ويمكن أن تمس باستقلال بلدان كبيرة مثل أمريكا، ومن هنا يتضح الأهمية القصوى لعمليات تأمين شبكات المعلومات، ويمكن أن نجمل بعض الأسباب التي أدت إلى الاهتمام بموضوع "أمن شبكات المعلومات" مؤخراً في النقاط التالية :

أ - التقدم التكنولوجي: فكما أدت التطورات الهائلة في مجال تكنولوجيا المعلومات والاتصالات، إلى طفرة كبيرة في وسائل الاتصال وتكنولوجيا شبكات المعلومات وتخزينها، فإنه في نفس الوقت أدى إلى وجود عقول تعمل على إيجاد الثغرات الأمنية في هذه الشبكات، واستغلالها الاستغلال السيئ فيما يسمى بـــ"الوجه القبيح للتكنولوجيا".

---

[1]- خالد بن محمد الغثير، الاصطياد الإلكتروني، الأساليب والإجراءات المضادة، مكتبة الملك فهد الوطنية، الرياض، 2008،متوفر على الرابط التالي : http://www.journal.cybrarians.org

[2]- سليمان بن صالح العقلا و فؤاد أحمد إسماعيل، إنشاء الشبكات، المبادئ الأساسية لإختصاصي المكتبات والمعلومات، الرياض، مكتبة الملك فهد الوطنية، 2000، متوفر على الرابط التالي : http://www.journal.cybrarians.org

ب – الطفولية والإندفاع: حيث يتملك بعض الشخصيات دوافع طفولية وإندفاعية للحصول على المعلومات بطرق غير مشروعة لمجرد الإحساس بنشوة الإنتصار وكسر حواجز السرية والأمان المفروضة على شبكات المعلومات.

ج – إنتشار جرائم المعلومات فقد سادت في الفترة الأخيرة هوس الجرائم الإلكترونية وجرائم المعلومات والتي تبدأ من الأشخاص والمنظمات والشركات المتنافسة وتنتهي بالدول، وذلك فيما يعرف بـــ"حرب المعلومات".[1]

4. وهنا يمكن أن نقول أن أنظمة أمن شبكات المعلومات تتطلب حماية أصول وموارد نظم المعلومات بطرق مشروعة، وكذلك تنظيم العلاقات والاتصالات داخل شبكات المعلومات من دون تأثير على كفاءة النظام ولا على قدرة المستخدمين في الأداء.

5. ولكن ... هل كل شبكات المعلومات تحتاج إلى تأمين؟ بالتأكيد يعتمد ذلك على ما تحتويه هذه الشبكات من معلومات وبيانات وطبيعة المستخدمين فيها، وكذلك رغبة الجهة المسؤولة عن هذه الشبكات في حماية موارد وممتلكات هذه الشبكات من عدمه، ولكن بصفةٍ عامة يجب أن يكون هناك نوع من الحماية ولو على الأقل الحماية البسيطة لهذه الشبكات على سبيل الاحتياط ومنع دخول غير المرغوب فيهم من الأوساط الخارجية، وعلى الجانب الآخر، فإن هناك أنواع من شبكات المعلومات لابد من وجود نظام أمان وحماية لها ولا يمكن أن تترك بلا أمان، وذلك نظراً لما تمثله من أهمية كبيرة سواء على مستوى ما تحمله من بيانات ومعلومات أو على مستوى المستخدمين لهذه الشبكات، ومن أمثلة هذه الشبكات ما يلي:

أ الشبكات الداخلية "*Local Area Network*"*LAN*[2] . مثل شبكات الشركات الصغيرة أو المدارس أو المستشفيات.

---

[1] -HADDAD Sabine, définition de la cybercriminalité ,Article juridique publié le 04/02/2013,Disponible sur :http://www.legavox.fr

[2]– يمكن تعريفها على أنها مجموعة من الأجهزة و الحاسبات متصلة مع بعضها لكي تؤدي الغرض الذي تم من أجله بناء هذه الشبكة في مساحة جغرافية محدودة مثل مبنى إداري أو كلية جامعية أو مؤسسة و قد تمتد هذه الشبكة إلى مسافة أقل من 10 كيلومتر، و تكون هذه الشبكة مملوكة لمؤسسة أو هيئة خاصة قنوات اتصال خاصة بالمؤسسة، راجع مزهر شعبان العاني، شوقي ناجي جواد، العملية الإدارية و تكنولوجيا المعلومات، إثراء للنشر و التوزيع، الشارقة ، 2008 ، ص198 .

ب الشبكات الواسعة "*Wide area Network* " *WAN*[1]. مثل الشبكات الدولية التي تربط بين أجزاء من الدول.

ج الشبكات الخاصة *Intranet*.

6. ويمكننا القول إن الغاية من الأمن المعلوماتي تتلخص في الإجابة عن السؤال التالي: ما الذي نريد أن نحميه؟ وهناك أربع نقاط رئيسية لأية غاية أمنية فعالة.

أولاً: يجب وضع إطار قوي للبرنامج الأمني المطلوب تنفيذه على أن يتضمن تفاصيل شاملة للمعايير والإجراءات التقنية.

ثانياً: ينبغي أن توضع تفاصيل توثيق السياسة وانتشارها، مع ضمان فهم المعنيين داخل المؤسسة وخارجها للسياسة فهماً كاملاً، وكيفية تحديدها لمسؤولياتهم.

ثالثا : مراقبة التهديدات الناشئة، والتعامل معها على نحو يضمن تطور السياسة والحلول التي تستند إليها أيضاً.

رابعا: ينبغي التأكد من أن جميع الأنظمة التي تندرج تحت المنظومة الأمنية متوافقة وملتزمة بالسياسة الأمنية والتعليمات الخاصة بها التزاماً كاملاً ."

وكما هو معروف فإنه ليس هناك حماية مطلقة في عالم تقنية المعلومات وأمن البيانات والشبكات، والمطلوب هو الحرص على تحقيق أقصى حماية ممكنة، ولعل النقطة الأهم في عالم الحماية والأمان في مجال تقنية المعلومات تتمثل في الوعي والتدريب، ولا شك بأن الوعي قد ازداد كثيراً تجاه أمن وحماية البيانات، ولكنه لا يزال غير كاف، فحتى الآن يسود اعتقاد بين كافة شرائح المستخدمين بأن حماية أمن البيانات والشبكات ينحصر ببرامج مكافحة الفيروسات، وبرامج الجدران النارية، علماً بأن هاتين الأداتين لا تشكلان سوى جزء صغير من المنظومة الكاملة لأمن المعلومات[2] ."

[1]- و تتمثل في تلك الشبكات التي تغطي مواقع متباعدة مكانيا، من خلال مساحات جغرافية شاسعة قد تشمل دولة أو مملكة أو قارة أو عدة قارات، مثل التي تربط بين الحاسبات الآلية لفروع المنظمة المختلفة داخل الدولة، أو التي تربط بين الحاسب الآلي للمنظمة و الحاسبات الآلية بمركزها الرئيسي في دولة أخرى مثلا، مزهر شعبان العاني، المرجع السابق ، ص 200 .

[2]- في الشرق الأوسط تعمل الدول على تطبيق استراتيجيات وطنية لأمن المعلومات، مع تكليف بعض المؤسسات المتخصصة بمراقبة الشبكات في البلاد وحماية الدولة من الهجمات المعلوماتية، مثل "الهيئة الوطنية للأمن الإلكتروني NESA "و"مركز الاستجابة لطوارئ الحاسب الآلي "

كما أنه ينبغي أن يكون هناك سياسة أمنية هدفها الأول والأخير تقليص الصدع الأمني بين الوضع المعياري والوضع الراهن إلى أقصى درجة ممكنة، "يجب أن تكون السياسة مبنية على أمور عدة، على رأسها تحديد حجم الأصول المعلوماتية، ونقاط الضعف الموجودة فيها، سواء على مستوى الشبكات، أو أنظمة التشغيل، أو التطبيقات، أو قواعد البيانات، ومن ثم الشروع في البحث عن نقاط الضعف في النظام الأمني العام للشركة.

ولا بد أيضاً من تحديد الثغرات الأمنية، والقصور الأمني إن وجد، ومن ثم العمل على رأبها من خلال اختيار الحلول والأدوات المناسبة، وليس بالضرورة الأعلى ثمناً في السوق، وإنما الحلول الأفضل القادرة على تلبية المتطلبات التي تم تحديدها بشكل دقيق.[1]

المطلب الثاني : المفهوم القانوني للمعلومات

المعلومات، كلمة لم تفتأ آذاننا تخفي يوماً سماع صداها يدوي في آفاق وسائل الاتصال المسموعة، و لم تعدم أبصارنا رؤية حروفها تسطر على صفحات وسائل الاتصال المقروءة، و لم تخل مجالسنا ومحافلنا من تجاذب أطراف الحديث عن التغني بأهميتها ودورها وأثرها في حياتنا [2].

- أن المعلومة في هذا العصر تُعد كتر عظيم وهام لاسيما في ظل وجود تكنولوجيا المعلومات التي ساهمت بشكل فعّال في معالجة، تخزين، وبث المعلومات؛ وبالتالي فامتلاكها يُشكل قوة لصاحبها[3].

---

aeCERTفي الإمارات العربية المتحدة، و"فريق مواجهة الطوارئ الحاسوبيةQCERT "التابع لـــ"المجلس الأعلى للاتصالات وتكنولوجيا المعلومات في قطرictQatar "، و"المركز الوطني الإرشادي لأمن المعلومات" في المملكة العربية السعودية.

إضافة إلى ذلك، دفعت هجمات العامين الماضيين عدداً من البلدان لتحديث قوانين أمن المعلوماتية القديمة لديها، وأنشأت لجاناً بهدف إعداد سياسات لأمن المعلومات وضوابط تبادلها بين المؤسسات الحكومية، مثل لجنة تنظيم أمن المعلومات ISR في دبي بالإمارات العربية المتحدة، و"سياسة تأمين المعلومات الحكومية GIA "في قطر http://www.alarabiya.net .

[1]- مصطفي سرهنك، رئيس شركة "إنترنت سيكيوريتي سيستمز" الشرق الأوسط، إحدى أبرز الشركات العالمية المتخصصة في مجال أمن المعلومات .iss_sarhank.jpg

[2]- خالد ممدوح إبراهيم ، أمن الجريمة الالكترونية ،الدار الجامعية، الإسكندرية ،2008،ص 25 و ما بعدها.

[3] -J. M Anderson, Why we need a new definition of information security ?. Computers & Security, 2003, pp308–313.

و لم تعد المعلومات الآن مجرد نوع من الترف تتباهى بها المجتمعات أو المنظمات وإنما أصبحت ركيزة أساسية في تطور المجتمع و تحقيق الرفاهية المنشودة، و لقد دخلت تكنولوجيا المعلومات و الاتصالات جميع الميادين العلمية الاجتماعية و الإنسانية، فعصرنا الحالي و المستقبلي هو عصر المعلومات الالكترونية في خدمة المجتمع، ويرتكز هذا المجتمع بصفة أساسية على تعظيم شان الفكر و العقل الإنساني بالحاسبات الآلية، و شبكات ووسائل الاتصال الحديثة و الذكاء الاصطناعي و نظم الخبرة.

و يتطلب التعرض لماهية المعلومة أن نتناول تعريفها، و أنواعها، و الشروط اللازم توافرها فيها، و طبيعتها القانونية.

الفرع الأول : تعريف المعلومة.

ان المعلومات حالة ذهنية و ظاهرة كونية أساسية، لا نستطيع التعرف على كنهها وجه اليقين، إلا أننا ندرك أثرها، و أثرها موجود في كافة المجالات التي تتعلق بالإنسان [1].

فالملاحظ لمفردات المعلومات في المجتمعات، أنها ظاهرة تلاقت حولها اهتمامات كثير من الباحثين من مجالات علمية وتخصصات مهنية قلما تتلاقى، وتفرقت في النهاية حولها وجهات نظرهم؛ حيث نجدها الآن محط اهتمام الباحثين في مجالات هندسة الاتصالات، والحاسب الآلي، وعلم اللغة، وعلم النفس، وعلم الاجتماع، والإعلام، والمكتبات، وعلم المعلومات، هذا فضلاً عن بعض مجالات العلوم البيولوجية والأحياء.

ولا شك أن لكل فئة من هذه الفئات دوافعها واتجاهاتها ورؤاها، عندما تتعامل مع المعلومات.

لكن الغريب في الأمر أن كل فئة تحاول أن تستحوذ عليها وتبعد الآخرين عن بلاطها[1] ويلفت الانتباه كذلك أن المعلومات تتخذ في مواقف كثيرة وسيمة لوصف حقبة زمنية ؛ فنسمع

[1]– ضياء مصطفى عثمان، السرقة الالكترونية، دراسة مقارنة، دار النفائس للنشر و التوزيع ،الاردن ،ط1 ،2011، ص 94 و ما بعدها

كثيرين يقولون : نحن نعيش " عصر المعلومات "، كما نسمع من يتخذها كذلك وسيمة للتعبير عن التحولات التي تشهدها ظاهرة المعلومات أو تقنياتها فيقولون : " ثورة المعلومات"، كما نلاحظ تواتر استخدامها في الآونة الأخيرة للتعبير عن التحولات التي يشهدها كثير من النظم الاقتصادية المعاصرة فيقولون : " اقتصاد المعلومات "، والنظم السياسية المعاصرة فيقولون "حرب المعلومات "، بل باتت كلمة شائعة بين عامة الناس وخاصتهم، لوصف المجتمعات التي تسخر تقنيات المعلومات في إدارة شؤونها، وما يرتبط بذلك من تحولات في كل مجريات أمورها فيقولون " مجتمع المعلومات".

ونتيجة لكثافة تواتر استخدام هذه الكلمة، فما المعلومات إذاً؟ وما دلالتها اللغوية والاصطلاحية؟

البند الأول : المدلول اللغوي والاصطلاحي للمعلومة

تشريح لغوي : المعلومات مشتق من مادة "ع ل م" وتدور مشتقاتها في نطاق العقل ووظائفه، وهي المقابل الأشمل والأدق للأصل الأجنبي***INFORMATION***، والمفرد "المعلومة" جائز في حالات معينة، و "الإعلام" حالة خاصة من حالات التعبير عن أحد معاني الكلمة الأصلية، وليس عنها جميعا بصورة شاملة[2].

تشريح اصطلاحي : وهو الذي يدخل في إطار اهتمامنا، فيمكن القول إنه ليس هناك حتى الآن تعريف جامع مانع " للمعلومات "، وكل ما هنالك هو اجتهادات وآراء ونظريات قد تحظى بالقبول في مجتمع أو عند فئة معينة، وقد لا يكون حالها على هذا النحو في مجتمع آخر أو لدى فئة أخرى، وقد عبر أحد الباحثين عن هذه الظاهرة بقوله: المعلومات ظاهرة مراوغة متعددة الصور والأبعاد، لا يمكن إدراك كنهها على وجه اليقين، وكل ما يمكن إدراكه هو التحقق من وجودها عن طريق ما تحدثه من أثر[3] .

---

[1]- ولفرد لانكستر، أساسيات استرجاع المعلومات، ترجمة حشمت قاسم، مكتبة الملك فهد الوطنية ،ط2، الرياض، 1997،ص ص15-41 .

[2]- ناريمان متولي إسماعيل، اقتصاديات المعلومات، دراسة للأسس النظرية وتطبيقاتها العملية على مصر وبعض البلاد الأخرى ،المكتبة الأكاديمية ، القاهرة،1995،ص ص 65-69.

[3]- ولفرد لانكستر ، نفس المرجع ، ص ص 17-41.

المعلومات ***Information*** :هي "المعاني التي يُفترض أن تُمثلها المعطيات للناس[1] "ويعرفها البعض بأنها "البيانات التي تجري عليها معالجات معينة وذلك بترتيبها وتنظيمها وتحليلها بغرض الإستفادة منها والحصول على نتائج معينة من خلال استخدامها [2]".

وقد عرفها البعض على أنها "تمثيل لحقائق المحيط عبر وسيط[3]، والوسيط هو الوسيلة التي يتم من خلالها نقل المعلومات، وقد تطورت هذه الوسائل تبعاً لمستوى تطور المجتمع الإنساني ابتداء بالإشارات واللغة المحكية مع بزوغ فجر التاريخ، مروراً بالكتابة على الألواح الطينية والحجرية ثم الجلود والورق، مروراً بالطباعة والتي شكلت بدورها فتحاً في مجال المعرفة، وانتهاء بنظم المعلومات وشبكات الاتصالات، والتي تثبت يوماً بعد يوم إمكانياتها الهائلة في معالجة ونقل وتخزين البيانات والمعلومات.

إذن المعلومات لابد لها من وسيط يحتويها قد يكون الورق هو هذا الوسيط أو يكون مغنطيسيا كالأقراص الممغنطة أو الصلبة، وقد يكون هذا الوسط عبارة عن كبلات تسري فيها نبضات، حتى الهواء الذي تسري فيه موجات كهرو مغنطيسية يحتوي على المعلومات المنقولة وهو من وسائط المعلومات، فكل نوع له مخاطره الخاصة به وله الإجراءات الأمنية التي تحفظ المعلومات فيه من التلف أو الضياع أو الاطلاع الغير المرخص به، ومن الشائع أن تكون إحدى وسائل المحافظة على المعلومات من الضياع هي إعداد نسخة أخرى منها على وسيط مختلف كأن تحفظ بصورة ورقية للبرامج المخزنة للحاسب، أو نحتفظ بشريط ممغنط كنسخة احتياطية في محتويات القرص الصلب، هذه النسخ في بعض الأحوال قد تكون قيمتها محدودة أو ربما تكون معدومة القيمة مثل الصور المنشورة عن الأعمال الفنية الأصيلة وغير ذلك...

[1]- معجم مصطلحات المعلوماتية ،الجمعية العلمية السورية للمعلوماتية، ط1 ، 2000، ص277.

[2]- انتصار نوري الغريب ، أمن الكمبيوتر والقانون، دار الراتب ،بيروت ،لبنان ،1998،ص 80.

[3]- عبد المجيد الرفاعي، المعلومات بين النظرية والتطبيق، دار الأعلام ، دمشق ،ط1 ،1998،ص26.

البند الثاني : مدلول المعلومة في تشريعات الدول

عرف المشرع الأمريكي المعلومات في قانون المعلومات التجارية الالكترونية لسنة 1999 في المادة العاشرة[1] بأنها "تشغل البيانات و الكلمات والصور والأصوات و الرسائل و برامج الكمبيوتر و البرامج الموضوعة على الأقراص المرنة وقواعد البيانات أو ما شابه ذلك . "

و يتبين من التعريف السابق انه أعطى مفهوما موسعا و شاملا للمعلومة إذ أجاز أن تكون في أي شكل كانت، و قد أضاف المشرع عبارة أو ما شابه ذلك ربما تحسبا لما قد يظهر من أشكال جديدة للمعلومة، إذ مع التطور التكنولوجي قد تظهر وسائل أخرى تنقل بواسطتها المعلومة .

وفي فرنسا و وفقا للقانون 652/82 الصادر في 26 يوليو 1982[2] تعرف المعلومة بانها صوت او صورة او مستند او معطيات أو خطابات أيا كانت طبيعتها .

[1] -The National Conference of Commissioners on Uniform State Laws. ,july23-30-1999, information me ans data , text , images, sounds, codes, computer programs, software, data bases, or the like.

[2] - Loi n°82-652 du 29 juillet 1982 sur communication audiovisuelle , JORF du 30 juillet 1982 page 2431- Article 1 La communication audiovisuelle est libre. la communication audiovisuelle est la mise à la disposition du public, par voie hertzienne ou par câble, de sons, d'images, de documents, de données ou de messages de toute nature. Cet article a été Abrogé par Loi 86-1067 1986-09-30 art. 110 JORF 1er octobre 1986,ainsi Modifié par Loi n°2004-669 du 9 juillet 2004 - art. 109 (V) JORF 10 juillet 2004 en vigueur le 1er août 2004 Modifié par LOI n°2009-258 du 5 mars 2009 - art. 36 Modifié par LOI n°2009-258 du 5 mars 2009 - art. 36 On entend par communications électroniques les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique.

On entend par communication au public par voie électronique toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée.

On entend par communication audiovisuelle toute communication au public de services de radio ou de télévision, quelles que soient les modalités de mise à disposition auprès du public, toute communication au public par voie électronique de services autres que de radio et de télévision et ne relevant pas de la communication au public en ligne.

ومن القوانين العربية التي عرفت المعلومات القانون الأردني للمعاملات الالكترونية رقم 85 لسنة 2001 حيث عرفها في المادة الثانية[1] من هذا القانون بأنها "البيانات أو النصوص أو الصور أو الأشكال أو الأصوات أو الرموز أو برامج الحاسوب أو قواعد المعلومات، التي أنشأت أو أرسلت أو استلمت أو خزنت بوسائل الكترونية" .

كما عرف قانون إمارة دبي بشان المعاملات و التجارة الالكترونية رقم 2 لسنة 2002[2] عرفت المعلومات الالكترونية بأنها "معلومات ذات خصائص الكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج حاسب ألي أو غيرها من قواعد البيانات" .

وفي هذا الصدد أيضا نجد أن القانون الاتحادي لدولة الإمارة العربية المتحدة رقم (1) لسنة 2006بشان المعاملات و التجارة الالكترونية عرف في مادته الأولى المعلومات الالكترونية بأنها " البيانات و معلومات ذات خصائص الكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج الحاسب الآلي أو غيرها [3].

أما القانون الإمارات الاتحادي رقم (2) لسنة 2006 في شان مكافحة جرائم تقنية المعلومات فقد عرف المعلومات الالكترونية أنها " كل ما يمكن تخزينه و معالجته وتوليده و نقله بوسائل تقنية المعلومات و بوجه خاص الكتابة و الصور و الصوت والأرقام و الحروف و الرموز و الإرشادات و غيرها.

أما قانون البحرين 83 لسنة 2002 بشان المعاملات الالكترونية[4] فقد عرف المعلومات بأنها البيانات و النصوص و الصور و الأصوات و الرموز و برامج الحاسوب والبرمجيات و يمكن أن تكون قواعد البيانات و الكلام .

---

[1]- عرف القانون الأردني للمعاملات الالكترونية رقم 85 المؤرخ في 11 ديسمبر 2001 المعلومات: البيانات والنصوص والصور والاشكال والاصوات والرموز وقواعد البيانات وبرامج الحاسوب وما شابه ذلك.

[2]- قانون إمارة دبي، بشان المعاملات و التجارة الالكترونية رقم 2 لسنة 2002، المؤرخ في 12 فبراير 2002.

[3]- قانون الإمارة العربية المتحدة رقم 1 لسنة 2006م في شأن المعاملات والتجارة الإلكترونية، المؤرخ في 30يناير 2006.

[4]- قانون البحرين رقم 13 لسنة 2006 عدل بعض أحكام المرسوم رقم 83 لسنة 2002 بشأن المعاملات الإلكترونية، 2006/13.

والمعلومات قد لا تكون شيئا يمكن لمسه أو يمكن رؤيته أو سماعه أو الإحساس به، فنحن عادة نصبح على علم بشيء ما أو بموضوع ما، إذ ما طرا تغيير على حالتنا المعرفية في ذلك الموضوع .

فالمعلومة هي تعبير يستهدف جعل رسالة قابلة للتوصيل إلى الغير، ثم إن قابليتها للتوصيل بفضل علامة أو إشارة من شانها ان توصل المعلومة للغير فواقعة معينة أو فكرة ما لا تعتبر معلومة طالما أنها لم تأخذ شكل إشارة ملموسة .

وتتطلب المعلومة بطبيعتها وجود وسط تخزن فيه و تختلف وسائط التخزين المعلومات فقد تكون أحبارا و ألوانا و ينطبق ذلك على جميع المعلومات المدونة على دعائم ورقية، و قد يكون الوسط ذبذبات كهربائية في الفضاء كموجات الراديو *Electromagnétique Pulses*، أو قطع و وصل إلكتروني كالإشارات الرقمية في الحاسبات الآلية*électronique switches* ولا شك أن التلاعب الذي يقع على هذا الوسط من شانه تعريض المعلومات للخطر.

كما تعرف بأنها هي البيانات التي تمت معالجتها و أصبحت ذات دلالة و ذات قيمة، و هي عبارة عن مجموعة من الحقائق و المفاهيم و الآراء التي تتعلق بموضوع و يكون الهدف منها زيادة المعرفة، ويمكن الحصول عليها من خلال القراءة، الرؤية، السمع، والذوق أو الحس[1] "

ويمكن تعريفها بأنها عبارة عن مجموعة من الحقائق ذات المعنى و المفيدة للعنصر البشري في عمليات معينة مثال عملية صنع القرارات الإدارية[2] "فالمعلومات هي مجموعة الحقائق والمفاهيم التي تخص أي موضوع من الموضوعات، والتي تكون الغاية منها تنمية الإنسان وزيادة معرفته، ويمكن أن تكون أماكن، أشياء، أو أناس.

و يمكن الحصول على المعلومات من خلال البحث، أو القراءة، أو الاتصال، أو ما شابه ذلك من وسائل اكتساب المعلومة والحصول عليها، ويجب أن تحمل المعلومات قيمة[3] ."

و يمكن تعريف المعلومة بصفة عامة بأنها : مجموعة من الرموز أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال*communication*أو التفسير أو للتأويل*interprétation* أو

---

[1]- سليمان مصطفى الدلاهمة، نظم المعلومات المحاسبية و تكنولوجيا المعلومات، الوراق للنشر والتوزيع، عمان، 2008، ص 31 .

[2]- نبيل محمد مرسي، نظم المعلومات الإدارية، المكتب الجامعي الحديث، الاسكندرية، 2006 ،ص18 .

[3]- لمين علوطي، أثر تكنولوجيا المعلومات و الاتصالات على إدارة الموارد البشرية بالمؤسسة، أطروحة دكتوراه، كلية العلوم الاقتصادية، جامعة الجزائر، 2008 ، ص49 .

للمعالجة *processing* سواء بواسطة الأفراد أو الأنظمة الالكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وجمعها، أو نقلها بواسطة وسائل وأشكال مختلفة.

ويذهب البعض إلى وجوب التفرقة بين المعلومات و البيانات ، فالبيانات تعبر عن مجموعة من الأرقام و الكلمات و الرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها البعض، أما المعلومات فهي المعنى الذي يستخلص من هذه البيانات .

أي هناك تفرقة بين اصطلاحي البيانات و المعلومات، فالبيانات *DATA* هي المدخلات *IN PUT* الجهاز الكمبيوتر بهدف تشغيلها *processing* ومعالجتها داخل الجهاز والحصول على المخرجات *out put* في صور المعلومات *information* .

البند الثالث : العلاقة بين المعلومات و البيانات و المعرفة.

المعلومات مصطلح يندرج في طياته عناصر ثلاثية الأبعاد، متعارف عليها" بالمعلومات "وهي : البيانات ،المعلومات، المعارف (المعرفة)وممكن إضافة عنصر رابع و هو الذكاء بصفته وسيلة لتوليد المعرفة و توظيفها

وتختلف هذه المفاهيم و تتداخل بشكل عام لدى الناس و عليه يمكن توضيح العلاقة بينها كما يلي:

- البيانات.*(DATA*) هي المادة الأولية التي نستخلص منها المعلومات ،لأن البيانات هي مجموعة من الحقائق والمشاهدات و الأرقام و القياسات أو الرموز، لوصف فكرة أو موضوع أو حدث أو حقيقة من الحقائق[1] .
- المعلومات(*Information*) هي ناتجة عن معالجة البيانات تحليلا أو تركيبا، لاستخلاص ما تتضمنه البيانات مثل تطبيق عمليات حسابية وموازنات و معدلات و طرق إحصائية ورياضية و منطقية.

أو هي جملة البيانات والدلالات والمعارف والمضامين، التي تتصل بالشيء أو الموضوع، وتساعد المهتمين بالتعرف عليه والعلم به.

[1]– هاني شحادة الخوري، تكنولوجيا المعلومات على أعتاب القرن الحادي و العشرين، مركز رضا للكومبيوتر، دمشق، 1998 ، ص23 .

فالمعلومات إذن توضح مفهوم الشيء وتعطيه قدره، وتوضح سماته وخصائصه وتبين استخداماته ووظائفه[1].

- المعرفة(*Connaissance*) هي حصيلة خبرة و معلومات و تجارب و دراسات فرد أو مجموعة أفراد أو مجتمع معين أو منظمة في وقت محدد، و المعرفة هي خلاصة البيانات و المعلومات[2] ، و هي الاستخدام الأمثل للمعلومات من أجل الوصول إلى نتائج مفيدة.

هي أساساً مجموعة المعاني والمعتقدات والأحكام والمفاهيم والتصورات الفكرية، التي تتكون لدى الإنسان نتيجة لمحاولات متكررة لفهم الظواهر والأشياء المحيطة به، تمثل حصيلة أو رصيد خبرة ومعلومات ودراسة طويلة يملكها شخص ما في وقت معين.

- الفرق بين المعلومات و المعرفة: يرى أكسفورد أن المعرفة هي عملية تمثيل للحقائق، فالمعرفة أمر شخصي بالنسبة للإنسان فهي تتجسد في شخصيته، يستعملها فهي مسألة شخصية خصوصية. أما المعلومات فهي على العكس من ذلك عامة و يمكن الحصول عليها.

المعلومة أكثر أساسية من المعرفة لكنها ليست أكثر منها أهمية، أي بلا معلومة يستحيل تصور معرفة لكن العكس بلا معرفة يمكن تصور معلومة.

المعرفة = المعلومات + المحاكمة العقلية

وتعد المعلومات ومراكزها من أهم ركائز الوثائق الإلكترونية وأمنها، وتزداد أهميتها بزيادة أهمية المعلومات التي تحتويها، وزيادة الاعتماد عليها في تيسير الكثير من الأعمال الاقتصادية والأمنية ومدي الاستفادة منها، هذا بالإضافة إلي الأبعاد الأمنية والأهمية الاقتصادية للمعلومات، ويعتبر أي تعد أو تخريب وسوء استعمال للحاسب ومعداته أو ما يتصل به أو وسائل التخزين تهديد لأمن المعلومة أو الوثيقة الالكترونية، وازدادت الخطورة على أمن المعلومات بتطور تقنية الاتصالات بين مراكز المعلومات في العالم وشبكاتها المتطورة، لتشكل شبكة هائلة لتناقل المعلومات

[1]- اليافي شادن، الإنسان و المعرفة في عصر المعلومات ،دارالعبيكان،الرياض،2001، ص 20.

[2]- مصطفى الدلاهمة، المرجع السابق، ص31

والبيانات ومعالجتها، الذي فتح المجال للعابثين من المخربين وقراصنة المعلومات للوصول إلي المعلومات والبيانات والعبث بها أو سرقتها أو تخريبها .[1]

البند الرابع : مستويات الأمن المعلوماتي

اذا صنف مستوى الأمن حسب درجة السرية القائمة [2] فنكون أمام المستويات التالية:

أ. إذا كان الأمن المستهدف لنظم المعلومات أمنا كليا، كانت درجة السرية المطلوبة سرى الغاية.

ب.إذا كان الأمن المستهدف لنظم المعلومات أمنا جزئيا ، كانت درجة السرية المستهدفة درجة سرى .

ج. إذا كان الأمن المستهدف لنظم المعلومات أمنا مناسبا ،ـــ كانت درجة السرية المستهدفة درجة هام فقط .

1- أما إذا صنف مستوى الأمن حسب **الإجراءات المتبعة** ، فنكون أمام المستويات التالية:

أ. إذا كانت عمليات الأمن المطلوبة وقائية ، كانت الإجراءات المتبعة تستهدف منع الأخطاء المتعمدة أو غير متعمدة .

ب.إذا كانت عمليات الأمن المطلوبة ثابتة ، كانت الإجراءات المتبعة تستهدف تحقيق الدفاع عن النظام المعلوماتي ، بتأخير عمليات الاختراق و رفع تكلفته .

ج. إذا كانت عمليات الأمن المطلوبة متحركة، كانت الإجراءات المتبعة تستهدف تحقيق الدفاع عن النظام المعلوماتي، بوسائل تتعامل مع المخترق ذاته.

2- وإذا كان التصنيف **نوعيا** فتكون الإجراءات المتبعة على النحو التالي :

أ. تستخدم وسائل طبيعية للأمن، حينما يكون الأمن طبيعيا أي عندما يقل احتمال وصول مستخدم غير قانوني، والوسائل الطبيعية للأمن تستهدف بالأساس منع الاختراق الطبيعي.

---

[1]- حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000م ، ص122 .

[2]- طارق إبراهيم الدسوقي عطية ، المرجع السابق، ص 490 .

ب.تستخدم وسائل صناعية للأمن، حينما يكون الأمن صناعيا أي عندما يزيد احتمال وصول مستخدم غير قانوني، والوسائل الصناعية للأمن تستهدف بالأساس استخدام وسائل صناعية إضافية لمنع تنظيم الوصول عن بعد

ج. تستخدم وسائل مختلطة للأمن، حينما تتساوى الاحتمالات، و الوسائل المختلطة للأمن تستهدف استخدام كلا الوسيلتين الطبيعية و الصناعية.

د. و هناك بالطبع مستويات أو أنواع أخرى لتصنيف الآمن المعلوماتي، فقد يكون المستوى المطلوب للأمن مستوى شموليا، و قد يكون المطلوب أمنا محكما لا يمكن اختراقه، و قد يكون ذا مستوى للجودة بالقياس لمعيار ما، او غير ذلك من التصنيفات المختلفة .

البند الخامس: هوية المعلومات.

شبكة التعريفات التي ألقت بظلالها على محيط المعلومات تعددت لكن من الصعوبة ان يكون لمثل هذه الشبكة أن تقود الإطار العام لبنية المعلومات، والخلاصة الحقيقية ان كل هذه التعريفات تدور في فلك أن المعلومات تمثل "أي إضافة فكرية تضاف للعقل البشري"

1. منظومة مجتمع المعلومات : *Information Society*

في البداية ومن خلال قراءة اللفظ السابق (مجتمع المعلومات) يتبادر جليا الى الذهن من التحليل اللفظي لمصطلح مجتمع المعلومات انه مقسم الى (معلومات، مجتمع مستفيد من المعلومات، طرف يجهز المعلومات) وهذا ما ينطبق على المنظمومة المعلوماتية، سواء الافتراضية او الواقعية اي بشكلها الالكتروني والورقي.

فالمعلومات هنا تمثل القاعدة العريضة لأضلاع ذلك المثلث، بينما يمثل الضلع الثاني معالج المعلومات (المؤسسة أو الشخص الاعتباري) أو باحث المعلومات ، أما الضلع الثالث فهو مجتمع المستفيدين ويتقاسم في هذا الضلع مجتمع المستفيدين ومعالج المعلومات بالتداخل والتناوب[1].

مما سبق نستطيع أن نقدم التحليل التالي لعناصر مجتمع المعلومات:

[1]– محمد مكاوي، الادارة الافتراضية ،مستقبل ام خيال ،قراءة لمستقبل مشروع الحكومة الاليكترونية، متوفر على الرابط التالي: http://alyaseer.net

أ. أوعية المعلومات: هي تلك الأوعية أو المادة التي تحمل المعلومة وهي إما في شكل تقليدي أم غير تقليدي، أو بشكلها المرئي المسموع منها والمقروء، وكذلك الشكل الورقي، ويندرج تحت هذه الأوعية العديد من الأشكال من كتاب ودورية وتقرير وصحيفة أو الشكل آلي، مثل مخرجات الحاسب الآلي والأوعية المؤتمتة من أقراص مضغوطة وبرامج (*Software*).

ب. مجتمع المستفيدين: وهو الطرف المتلقي للمعلومات وقد يكون هو نفس الطرف المغذي بالمعلومات وتتعدد أوجه المستفيدين من باحثين وصحفيين ومواطنين وأجانب وموظفين[1]

ج. معالج المعلومات: وهذا الطرف هو المخول إليه تغذية وحفظ واستدعاء المعلومات والتفاعل والمشاركة المرتدة مع الطرف المستفيد وقد يكون هذا الطرف مؤسسة أو حكومة أو فرد اعتباري

2- فجوة المعلومات *Information Gab* : بين الفهم الغائب والمعيار الدقيق الفجوة الحقيقة للمعلومات ليست كما يراها البعض في القدرة الاستعمالية لتكنولوجيا المعلومات أو عدم توافر الميديا الاليكترونية أو قلة استخدام أنظمة الاتصالات الحديثة أو حتى التعويل على قضايا النشر الاليكتروني أو وسائل نقل المعلومات عبر البوابات الالكترونية أو خلافه، ولكن الفجوة الحقيقة تكمن في تضييق المسافة بين إطارين أساسيين:

الإطار الأول: النفاذ للمعلومات، وهذه القضية قد تختزل الكثير من المفاهيم مثل قضية الإفصاح وحرية التداول وقضايا الإتاحة المتبادلة بين الأفراد والمؤسسات.

الإطار الثاني: تطويع المعلومات المتاحة في خدمة الفرد (المجتمع) وبالتأكيد فانه لا يمكن الاستدلال على عملية تقييم او تقويم لقيمة المعلومات دون الرجوع لأصل الهدف وهو هدف الحصول على المعلومة والذي يختزل هو الآخر عدة مفاهيم تكمن في خدمة الفرد والمجتمع.

[1] -Tony Capaccio, Warfare in The Information Age, Popular Science, July 1996, pp.52-57.

والواضح ان طرفي معادلة فجوة المعلوماتية (*Information Gab*) مرتبط في الأساس بتهيئة المناخ اللازم لتوفير مساحة من الشفافية حول قضية الأمن والسرية من جانب وقضية الإتاحة والإفصاح من جانب آخر.

وكلا الجانبين يمثلا محصلة الثقافة السائدة والفكر الجاري حول مبدأ المعلومات إما باعتبارها خدمة أو وقوعها في محيط واسر مقومات السلعة.

مبادئ وأدبيات المعلومات: لابد لكل قارئ وكل باحث وكل من يتابع حركة المعلومات، أن يعلم أن مجال المعلومات ينقسم إلى قسمين :

أولهما : قطاع خدمات المعلومات:

وهو القطاع الذي يندرج تحته المكتبات ومراكز المعلومات وكل المؤسسات التي تهتم بخدمة المستفيد (باحث أو كاتب أو صحفي ...الخ)

ثانيهما: قطاع تكنولوجيا المعلومات:

لم تحض تكنولوجية المعلومات – كغيرها من المصطلحات الجديدة – خاصة مع ظهور الاقتصاد الجديد بتعريف موحد، بل تعددت هذه التعاريف وتنوعت تبعا لرؤية كل واحد لها، لذا سندرج عدة تعاريف حتى تبرز لنا أوجه الاختلاف والاتفاق فيما بينها.

تم تعريفها أنها « تكنولوجية المعلومات هي استعمال التكنولوجية الحديثة للقيام بالتقاط ومعالجة، وتخزين واسترجاع، وإيصال المعلومات سواء في شكل معطيات رقمية، نص، صوت أو صورة».[1]

كما تم تعريف صناعة تكنولوجيا المعلومات و الاتصالات حسب منظمة التعاون الاقتصادي والتنمية *OECD* بأنها مجموعة المنتجات و الخدمات المتعلقة بالصناعة الالكترونية القادرة على تلبية الوظائف و المهام المتعلقة نقل و تشغيل المعلومات و الوظائف الالكترونية."

[1]– مراد رايس، أثر تكنولوجية المعلومات على الموارد البشرية في المؤسسة، رسالة ماجستير في علوم التسيير، فرع إدارة الأعمال ،جامعة الجزائر 2005- 2006 ،ص 28 .

وهو القطاع المستحدث الذي يخدم القطاع الأول من الناحية التكنولوجية كحماية وصيانة البرامج واستحداث وتطوير البرامج الخاصة بتقديم المعلومة. وكلا القطاعين يمثلا وجهي عملة واحدة وهي مجتمع المعلومات وبشكل آخر لا يمكن أن يتم اكتمال النضج التكنولوجي للمعلومات دون أن يكون هناك خدمة يستفاد منها ألا وهي خدمة المحتوى (المتن) او صناعة المحتوي أي ما تحمله أوعية المعلومات التكنولوجية من محتوى معلوماتي والتي من المفترض ان تكون غاية التطور وهي الخدمة ، وهذين القطاعين متداخلين تارة بالتناوب وتارة اخرى بالتكامل[1].

البند السادس : مجالات الأمن المرتبط بالمعلومات

هناك أنواع عدة و مجالات متنوعة للأمن المرتبط بنظم المعلومات ، نذكر منها :

1-امن المعلومات *information Security*

و هو المرتبط بالمعلومات التي هي أساس أو هدف نظام المعلومات القائم و الذي يشكل عصب او حياة المنشاة الحديثة أو الكيان أو النظام على اختلاف صبغتها اقتصادية أو إدارية أو خدمية ، و هو يعمل على حماية المعلومات ذاتها و أيضا العمل و بذات الدرجة على حماية المخازن المعلومات و البيانات بمعناه الفني أو الاصطلاحي الحديث.

2-أمن الوصول إلى الأنظمة *Access control*

و هو يعني بعملية التامين المعلوماتي، المرتبطة بالأساس بعمليات التعامل مع البيانات و المعلومات القائم عليها النظام المعلوماتي بالمنشاة، و تشمل تلك الإجراءات تامين أو عمليات التحكم في الدخول لنظام المعلومات ذاته و التحكم في التطبيقات التي يعمل عليها نظام المعلومات بالمنشاة، و هو غالبا ما يكون على عدة مستويات طبقا للمستوى الوظيفي لمستخدم هذا النظام، ودرجة احتياجه للمعلومات المراد التعامل معها، بالنسبة لتخصصه الوظيفي أو للصلاحية الشرعية المسموحة له بالمنشاة .

[1] -Joseph S.N, Owens, W.A, America's Information Edge, Foreign Affairs, March/April 1996, pp.20-36.

3-أمن برمجيات نظم المعلومات *software Security*

و هي العملية التي تستهدف حماية البرامج التي تشغل أو يقوم عليها نظام المعلومات ذاته، و هي البرامج التي تحدد مسار البيانات و كيفية التعامل معها و المعلومات بالمنشاة

و كيفية الاستفادة منها و توظيفها ، و هي تشمل عمليات التامين ضد أعمال القرصنة،

و التامين ضد السطو عليها من الخارج أو الداخل أو أعمال التخريب أو الإتلاف المتعمد لها.

4- أمن الإتصالات *communication Security*

و هي عمليات تأمين وسائل الإتصال التي تعمد عليها المنشأة في أعمالها الوظيفية، و تشمل تامين وسائل الاتصال السلكي من خطوط تليفونية و خطوط و مسارات و كوابل نقل المكالمات و أجهزة نقل و تداول الاتصالات، و أيضا محطات الاتصالات المركزية أو الرئيسية الداعمة أو المقوية للاتصالات التليفونية، كما تشمل عمليات التامين و وسائل الاتصال اللاسلكي، سواء كانت وسائل اتصال لا سلكي مستقل، او و سائل اتصال لاسلكي ملحة بأجهزة أخرى[1] .

الفرع الثاني: أهمية المعلومات .

إن المعلومة وجدت مند أن خلق الله عز وجل الإنسان، اي خلق ادم عليه السلام و علمه الأسماء كلها، فكانت أول معلومات بشرية تسجلها ذاكرة الإنسان، هي الأسماء قال تعالى: "و علم ادم الأسماء كلها ثم عرضهم على الملائكة"[2].

"يؤكد هذا النص القرآني الكريم، أن الإنسان بدا عالما، عابدا، ناطقا، متملكا بلغة منطقية مفهومة في الوقت الذي ينادي اغلب علماء الدراسات الإنسانية (الانثروبولوجيا) بان الإنسان الأول لم تكن له قدرة على الكلام .

ونظرا لأهمية المعلومات في حياة الانسان سعى إلى جمعها و تسجيلها على وسائط حفظ مختلفة، بدءا من جدران المقابر و المعابد في عصر الفراعنة إلى أن تم اختراع الورق في الصين، وعرفت اولى محاولات تسجيل المعلومات في التاريخ على أيدي قدماء المصريين الذين سجلوا حضاراتهم على جدران المقابر و المعابد، و هذا هو السبب في الإبقاء على حضاراتهم محفورة في

[1]- طارق إبراهيم الدسوقي عطية ،نفس المرجع، ص ص491-492.

[2]- سورة البقرة الآية 31.

ذاكرة التاريخ، و يحكي لنا التاريخ عن حضارات عظيمة اندثرت لعدم تسجيلها، لذلك تعتبر المعلومات رمزا من رموز الحضارة الإنسانية على مدى التاريخ .

وأن النصف الثاني من القرن العشرين، شهد ثورة معلوماتية ضخمة، حيث تتصل تقنية المعلومات في وقتنا الحاضر بشتى جوانب الحياة الإنسانية على وجه الأرض، و لان نظام المعلومات لا يعترف بالمكان و يوفر الزمان و البحث و الإجهاد الذهني، فقد أصبح النظام المعلوماتي في نهاية القرن الماضي من لوازم الحياة الضرورية و المتطورة على مستوى العام والخاص .

ومن هذا المنطق نثبت فكرة بنوك المعلومات التي تتحكم فيها أنظمة عملاقة، تقدم كما معينا من المعلومات المخزنة لمن يملك الثمن، وهو ما جعل المعلومات تستحق أن يطلق عليها البترول الرمادي نظرا لأهميتها و قيمتها المالية المرتفعة .

وإذ يسعى المنتمون لمجتمع الأعمال بكل ما أوتوا من قوة من اجل الحصول على المعلومات سواء بالطرق المشروعة او غير مشروعة، الأمر الذي حدا بالبعض إلى التقرير بوجود سوقين لشراء المعلومات، أحداهما شرعي و الثاني يطلق عليها "السوق السوداء "للمعلومات، وهو الذي يرتبط بالجانب الأكبر من الجرائم التي تستهدف الأنشطة الاقتصادية للمجتمع، ومن خلاله يمكن الوصول للمعلومات المالية التي تتصل بالوضع المالي والإداري، وتداول رؤوس الأموال، والإستثمارات في المنشئات سواء كانت خاصة أو عامة .

ومن خلالها يمكن الوصول للمعلومات التجارية والصناعية، التي تتعلق بالأبحاث المرتبطة بالسوق والمشروعات الاستثمارية والصناعة والإنتاج والتجارة .

وأيضا يمكن للمجرمين الوصول للمعلومات الشخصية المخزنة في ذاكرة الحاسب الآلي، وعلى نظيرها المعلومات المخزنة في ذاكرة الحواسيب لدى بنوك و المحامين و الأطباء ومراكز الشرطة، كما يمكن الوصول للمعلومات العسكرية التي يكثر الطلب عليها خاصة من الدول الأجنبية و القوى المعادية مما يجعلها أكثر رواجا في السوق السوداء .

إن المعلومات محمية جنائيا بما أنها ذات أهمية ثقافية وسياسية واقتصادية، وهذا ما أكده الفقيه *catala* حين قال أن المعلومة هي كل رسالة يمكن نقلها إلى الغير بأي وسيلة كانت يعاقب عليها قانون العقوبات على من يسرق الدعامة المسجلة عليها المعلومات بالعقوبات المقررة لجرائم السرقة [1].

فأوجه أهميتها-المعلومات[2]-متعددة ومتسعة، ولا يحتمل المجال هنا الاستطراد في بيان جميع هذه المجالات، وحسبنا الإشارة فقط إلى أهم هذه الجوانب.

فالمعلومات لا يمكن إغفال دورها ـــأو بالأحرى أثرها، في إتخاذ القرارات بأنواعها وأشكالها كافة، سواء على المستوى الفردي أو الجماعي أو المجتمعي، وبصرف النظر عن طبيعة هذه القرارات سواء أكانت قرارات سياسية أو إقتصادية أو عسكرية، ذلك ببساطة لأن اتخاذ قرار معين يعني الإحاطة بكل القرارات البديلة، ولا يمكن أن يتم ذلك إلا بتوافر المعلومات عن كل البدائل المتاحة.

وللمعلومات دورها كذلك في مجال البحث العلمي؛ حيث لا يمكن لأي باحث أن ينتج بحثاً علمياً ما لم تتوافر له المعلومات الكافية عن طبيعة المشكلة التي يدرسها، وعن الأساليب المناسبة لدراسة هذه القضية، وعن الجهود السابقة التي تناولت هذه المشكلة، وأهم ما انتهت إليه من نتائج ... إلى غير ذلك من معلومات تسهم في دراسة القضية دراسة علمية منهجية تفضي إلى نتائج جديدة وليس مجرد تكرار لنتائج سابقة [3].

كذلك ثمة علاقة قوية بين المعلومات والإنتاجية بكل أشكالها وفي مختلف القطاعات؛ حيث تؤدي المعلومات الحديثة والتي يتم نقلها لمواقع الإنتاج وللمنتجين إلي تغيير بعض الأساليب القديمة المرتبطة بتطوير منتجات معينة، أو إلى تطوير منتجات حديثة تتفوق في إمكاناتها وكفاءتها عن تلك المنتجات القديمة .

ففي مجال الزراعة،على سبيل المثال لا الحصر، يمكن أن تحدث المعلومات الحديثة التي يتم توصيلها للمزارعين تغييراً في بعض المفاهيم القديمة تجاه أساليب زراعية، أو نوعيات معينة من المحاصيل والمنتجات الزراعية، والتي تؤدي بدورها إلى ارتفاع واضح في ناتج تلك المحاصيل،ولا

[1] - (p) Catala pafillon, la réception de l'innovation technologique en droit pénal, rev.s.c ,1990,p273-274.

[2]- ولفرد لانكستر ،المرجع السابق، ص 19.

[3]- نفس المرجع ، ص.ص 23-41.

شك أن ارتفاع معدلات الإنتاج والإنتاجية يكون له مردوده على الاقتصاد الوطني، ومن ثم على التنمية الاجتماعية الشاملة بكافة جوانبها الاجتماعية والاقتصادية والسياسية ...

الفرع الثالث: أنواع المعلومات

تقسم المعلومات إلى ثلاثة طوائف هي المعلومات الاسمية، والمعلومات المتعلقة بالمصنفات الفكرية، والمعلومات المباحة، ونتناولها بشيء من التفضيل على النحو التالي:[1]

الطائفة الأولى : المعلومات الاسمية *information nominatives*

وتنقسم هذه المعلومات بدورها إلى مجموعتين وهما المعلومات الشخصية و المعلومات الموضوعية .

1. المعلومات الموضوعية : و هي تلك المعلومات المرتبطة بشخص المخاطب بها مثل اسمه، موطنه و حالته الاجتماعية، و هذه المعلومات مرتبطة بشخص صاحبها، فلا يجوز للغير الاطلاع عليها إلا بموافقته الشخصية أو بأمر من السلطات المختصة .

2. المعلومات الشخصية : و يقصد بها تلك المعلومات المنسوبة إلى أخر مما يستدعي إدلاء الغير برأيه الشخصي فيها، و هي بذلك تتفق مع المعلومات الموضوعية في أنها خاصة بشخص معين، و تختلف عنها في أنها موجهة الى الغير بحسب الأصل و ليست لصيقة بشخصية صاحبها، مثل مقالات الصحف و الملفات الإدارية للعاملين لدي جهة معينة .

الطائفة الثانية : المعلومات الخاصة بالمنافات الفكرية :

و هي عبارة عن معلومات متمثلة في منصفات فكرية، و هذه المنصفات محمية بقوانين الملكية الفكرية، يستوي في ذلك ان تكون القوانين متعلقة بالملكية الأدبية و الفنية أو متعلقة بالملكية الصناعية .

الطائفة الثالثة : المعلومات المباحة

و يقصد بها تلك المعلومات التي يتاح الجميع الحصول عليها لأنها بدون مالك.مثال : ذلك تقارير البورصة اليومية و النشرات الجوية، و تنعقد ملكية هذه المعلومات للأسبق إلى جمعها و صياغتها .

[1]- خالد ممدوح إبراهيم، المرجع السابق ، ص 29.

و يلاحظ أن هذه المعلومات إذ تم تجميعها بغرض معالجتها، ليتم تشغيلها على الكمبيوتر و تخزينها و استرجاعها، أو بقصد تخلق معلومات جديدة فإنها تنقسم على النحو لتالي :

1. المعلومات المعالجة : و يقصد بها المعلومات التي تعالج للتشغيل على جهاز الكمبيوتر بقصد تخزينها و حفظها فيه و استرجاعها و قت الحاجة.
2. المعلومات المتحصلة : و يقصد بها التي تنتج عن معالجة مجموعة من المعلومات و تقرر حق ملكيتها هنا طبقا لقاعدة حيازة المال المنقول .

الفرع الرابع: خصائص والشروط الواجب توافرها في المعلومة.

البند الأول : خصائص المعلومة

عادة ما تكون المعلومة مرتبطة بحدث أو موقف لذا نجد أنها تختلف باختلاف الموقف فقد تكون كمية ،وصفية ،رقمية... الخ ، و على العموم هناك عشرة خصائص أساسية للمعلومات وذلك على النحو التالي[1]:

1. **التوقيت:** ومعني هذا عدم وصول المعلومات لمتخذ القرارات بعد الحاجة لها او قبل ذلك بفترة طويلة ، لاحتمالات تقادمها.
2. **الدقة** : و تكون في إجراءات القياس المستخدمة في إعداد المعلومات و تشغيلها و تجهيزها و تلخيصها و عرضها.
3. **الصحة:** أي درجة خلو المعلومات من الأخطاء سواء كانت لغوية او رقمية.
4. **إمكانية التعبير الكمي** : إمكانية التعبير عن المعلومات بالأرقام و النماذج الكمية إذا لزم الأمر.
5. **إمكانية التحقق** : درجة الاتفاق فيما بين المستخدمين المختلفين عندما يتفحصون نفس المعلومات.
6. **إمكانية الحصول عليها:** و المقصود درجة اليسر والسرعة في الحصول على المعلومات الأزمـــة.

[1]- خالد ممدوح إبراهيم، المرجع السابق ، ص 30 .

7. **الخلو من التحيز:** أي غياب النية في تعديل او تحريف المعلومات للتأثير على المتلقي، او لتحقيق أغراض خاصة.
8. **الشمول:** اكتمال المعلومات.
9. **الملائمة** : مدى ارتباط المعلومات بمتطلبات المستخدم المحتمل لها.
10. **الوضوح** : مدى خلو المعلومات من الغموض[1].

البند الثاني : الشروط الواجب توافرها في المعلومة

هناك شروط يجب توافرها في المعلومات بصفة عامة، حتى تتمتع بالحماية القانونية و تتمثل هذه الشروط في الآتي :

أ- يتوافر في المعلومة التحديد و الابتكار

إن المعلومة المحددة و المبتكرة هي خصيصة أولى تفرض نفسها دائما، فالمعلومة التي تفتقر لصفة التحديد لا يمكن أن تكون معلومة حقيقية، فإذا كانت المعلومة هي تعبير وصياغة محددة تجعل رسالة ما قابلة للتبليغ عن طريق علامات أو إشارات معينة فهذا يتطلب أن تكون محددة و يصبح هذا التحديد ضروريا، و بصفة خاصة في مجال الاعتداءات على الأموال، فهذه الاعتداءات تفترض دائما وجود شيء محدد .

أما فيما يتعلق بالابتكار، فهده صفة أساسية في المعلومة، فمعلومة غير مبتكرة، هي معلومة عامة شائعة متاحة للكافة [2]و غير مرتبطة بشخص أو أشخاص معينين.

ب- أن يتوافر في المعلومة السرية أو الاستئثار

السرية صفة لازمة للمعلومة لأنها تحصر حركة الرسالة و تحمل المعلومة في دائرة محددة من الأشخاص، و لا يمكن تصور الجرائم الخاصة بالسرقة و النصب و خيانة الأمانة إذا انعدم هذا الحصر لان المعلومة غير السرية تقبل التداول و من ثم تكون بمنآي عن أي حيازة .

وتكتسب المعلومة وصفها إما بالنظر إلى طبيعتها أو بالنظر إلى إرادة الشخص أو بالنظر إلى الأمرين معا، كما في حالة الرقم الري الخاص باستعمال بطاقات الائتمان، و يقلل الطابع السري

[1]- ثابت عبد الرحمن ادريس، نظم المعلومات الادارية في المنظمات المعاصرة، الدار الجامعية،الاسكندية،2005،ص 80.

[2]-عبد الفتاح مراد، شرح جرائم الكمبيوتر و الإنترنت، دار الكتب و الوثائق المصرية ،الإسكندرية ، ص 51 .

في هذه الحالات المختلفة من استخدام المعلومات و يقصرها فقط على دائرة المؤتمنين عليها و الذين يجدون أنفسهم هكذا منتفعين بحق الاستئثار عليها .

- وضوابط سرية المعلومات هي ثلاثة أمور :

1. الجدية : و الجدية المقصودة هنا هي الجدية النسبية و ليست المطلقة، لأن المعلومة قد تكون معروفة لعدد من الأشخاص مع ذلك محتفظة بطابع السرية، فحدود سرية المعلومات فيما يتعلق بالجدية يتوقف على عدم التهاون في تعريضها و كشفها للعامة.

2. أن يكون للمعلومات قيمة معتبرة في مجالها : فقيمة هذه المعلومات تعكس حاجتها للحماية، و لا شك أن قيمة المعلومات نرتبط بسريتها و بصعوبة التوصل إليها، وكلما كان من الصعب الحصول عليها زادت قيمتها .

فعلى سبيل المثال في مجال الصناعة المشروبات الغازية مازالت شركة كوكا كولا الأمريكية تتفوق على منافسيها في هذه الصناعة، و السبب يعود إلى سر الوصفة الخاصة، فالمحافظة على سر هذه الوصفة من الشيوع و حمايتها من التعرض لمتر صديها، جعل هذه الشركة تجني أرباحا تقدر بالمليارات .

3. أن تتخذ تدابير للمحافظة على سريتها لا يكفي لاعتبار السرية في المعلومات، التعامل معها بجدية و أن يكون لها قيمة معتبرة في مجالها، بل لابد من اتخاذ تدابير وإجراءات معقولة من قبل الحائز الشرعي للمعلومات للمحافظة على سريتها .

والمعقولية في اتخاذ الإجراءات تختلف باختلاف طبيعة المعلومات، و درجة أهميتها وقيمتها، و حسب نوع النشاط المستخدمة فيه.

فالإجراءات البسيطة التي يتخذها صاحب مشروع صغير، مثل وضع المعلومات في مكان مغلق، قد تكون كافية للمحافظة على الأسرار، بينما لا تكفي هذه الإجراءات لحماية أسرار المشروعات الكبيرة أو المنشأة العسكرية التي تحتاج عادة إلى إجراءات أمنية أكثر تعقيدا[1].

[1]- ضياء مصطفى عثمان، المرجع السابق، ص 99 .

ولا شك أن السرية هي أهم الخصائص المعلومات التي تنطبق عليها الحماية القانونية ولا يشترط أن تكون درجة السرية التي تتوافر في المعلومات مطلقة حيث أن المعلومات لا تفقد طابع السرية لمجرد أن عددا محدودا من الأشخاص يعرفونها، و هي ما يعني أن السرية تتوافر في المعلومة و لو عرفها عدد غير محدود من الأشخاص إذ قد تتطلب طبيعة التعامل البوح ببعض الأسرار للطرف الأخر .

ولا يشترط أن تكون المعلومات السرية معروفة لمشروع واحد بحيث يكون هو الحائز لتلك المعلومات، إذ أن تتوافر المعلومات السرية لعدد محدود من المشروعات المنافسة لا يؤدي إلى زوال صفتها السرية طالما أن المعلومات غير معرفة على نطاق واسع في مجال التخصص المتصل بنشاط هذا المشروع .

ولاشك أن القيمة الاقتصادية للمعلومات ترتبط بالسرية لان قيمة المعلومة تنخفض كلما زاد عدد من يعرفونها ، كما ترتبط بمدي صعوبة أو سهولة حصول الغير على المعلومات بوسائل خاصة [1].

و تعد خاصية الاستئثار بالمعلومة ***information exclusive*** امرأ ضروريا، أنه في مختلف الجرائم التي تنطوي على اعتداء قانوني على الأموال، فان الفاعل يعتدي على حق يخص الغير على سبيل الاستئثار، و يتوافر للمعلومة هذه الصفة، إذا كان الوصول إليها غير مصرح به لأشخاص محددين و يذهب البعض إلى أن الحماية القانونية للمعلومة، باعتبارها شيء قابل للاستحواذ

---

[1]– و نجد هذا واضحا في احد القضايا التي نظرت أمام المحكمة الاستئناف الفيدرالية في الولايات المتحدة الامريكية و هي قضية:

national fund raising consultants , inc. pate.v a Colorado Corporation; Maurice Deshazer; and Rozanne Deshazer, Defendants/Appellees. No. 92-3765. United States Court of Appeals, Submitted Sept. 16, 1993. Decided March 30, 1994.

و تخلص وقائع هذه القضية في أن ثار نزاع بين طرفين بشان تنفيذ عقد فرنشايز كان قد ابرم بينهما، و من المعلوم أن عقود الفرنشايز هي من العقود التي ترتكز على الترخيص باستغلال الاسم و العلامة التجارية، و يلتزم المرخص بموجب العقد بتزويد الرخص له بالمعرفة و الخبرة الفنية الأزمة للإنتاج و التوزيع، و عند طرح القضية على محكمة الاستئناف الفيدرالية الأمريكية كان النزاع يدور حول مدي اعتبار المعلومات التي قدمت من الشركة المرخصة و هي شركة nfrc إلى المرخص له بمناسبة عقد الفرنشايز المبرم بينهما تعد من أسرار التجارية، و بعد أن استعرضت المحكمة العناصر الواجب توافرها في الأسرار التجارية وفقا للقسم 759 من مدونة القانون الأمريكي بشان المسؤولية عن الفعل الضار لسنة 1939 restatemet of torts،استخلصت المحكمة من وقائع الدعوة و مستنداتها و من شهادة الشهود أن الشركة المرخصة بذلت جهدا و أنفقت مالا في تجميع المعلومات التي قدمتها إلى المرخص له و قدمت للشركة المرخص لها برنامج تدريب متميزة و من الصعب الحصول عليها من مصادر أخرى، و قد استفاد المرخص له من تلك المعارف مما أدى إلى زيادة أرباحه خلال فترة زمنية قصيرة ، و بناء عليه قضت المحكمة الاستئنافية بتأييد قرار هيئة المحلفين فيما انتهى إليه من وقوع اعتداء على الأسرار التجارية الخاصة بالشركة المرخصة .

U.S. Court of Appeals for the Eighth Circuit - 20 F.3d 341 (8th Cir. 1994) Submitted Sept. 16, 1993. Decided March 30, 1994 https://law.resource.org/ http://law.justia.com

و الاستئثار، يجد أساسه في دعوة المنافسة غير المشروعة و التي تجد أساسها في قواعد المسؤولية التقصيرية من خطأ و ضرر وعلاقة سببية [1].

الفرع الخامس : الطبيعة القانونية للمعلومة

يرى جانب من الفقه أن المعلومات تعد أموال منقولة و انه يمكن تقويمها بالمال انطلاقا من القيمة الاقتصادية لها، وبالتالي يصح أن تكون محلا للحقوق المالية و على الأخص حق الملكية، على أساس أنه يمكن استغلالها في تحقيق عوائد مادية أو تحسين أداء المشروعات الإنتاجية، وبالتالي يجوز أن يرد عليها جميع أنواع التعاملات التجارية، وتتمتع المعلومات بحماية القانون باعتبارها مال مقوم يستوي في ذلك أن تكون مبتكرة آو غير مبتكرة، لأنها إذا كانت مبتكرة فهي محمية بمقتضى قانون حماية الملكية الفكرية، وإذا لم تكن كذلك فهي تعد محمية طبقا لقواعد العامة في القانون المدني[2].

ويعتبر الفقه الفرنسي أن المعلومات أموالا ذات طبيعة خاصة انطلاقا من ان غياب الكيان المادي للمعلومات، لا يجعلها محلا لحق مالي من توع الحقوق المتعارف عليها في الفقه و التي ترد على كيانات مادية، و إن جاز اعتبارها محلا لحق ملكية أدبية أو فنية أو صناعية، وبالتالي فان المعلومات التي لا تكون متصلة بالنواحي الأدبية والفنية والصناعية التي تتأتى بطبيعتها على أن تكون محلا لمثل هذه الحقوق، يلزم بالضرورة استبعادها من طائفة الأموال و ليس من مقتضى هذا الاستبعاد ان تظل هذه المعلومات عارية عن حماية إذا ما جرى الاستيلاء عليها أو استخدامها استخداما غير مشروع فهذه المسؤولية تتحرك وفق قواعد المسؤولية المدنية المستندة إلى نص المادة 1382 من قانون المدني الفرنسي[3]، و بالاعتراف بالخطأ تكون المحكمة قد اعترفت بوجود حق و هو الحق في المعلومات" مما مؤداه ان يكون للمعلومات طبيعية خاصة تسمح بان يكون الحق الوارد عليها من نوع الملكية العلمية .

[1] – طارق ابراهيم الدسوقى عطية ، المرجع السابق، ص 44 و ما بعدها

[2]- خالد ممدوح إبراهيم، المرجع السابق ، ص 34 .

[3] – Article 1382 « Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence. » Créé par Loi 1804-02-09 promulguée le 19 février 1804.

فصناعة المعلومات أصبحت هي المجال الأهم لجذب الاستثمارات، خصوصا مع تحقيق التزاوج بين المعلوماتية و الاتصال، فهي تعتبر مالا لأنها ذات قيمة اقتصادية حيث تمثل مصدر حقيقي لتحقيق عائد مادي لصاحبها، و من ثم فإنها يمكن أن تكون محلا للتعاقد و الانتقال من شخص إلى آخر، فكل عمل إنساني مفيد ينتج فائدة اقتصادية يجب ان يتم تكييفه مالا، و لذلك فهم يقترحون لحماية المعلومات أدوات جديدة و ذلك من خلال النظرية التي ابتدعها القضاء الفرنسي و هي نظرية الأعمال الطفيلية .

الفرع السادس: المسؤولية في مجال المعلومات.

يرى جانب من الفقه[1] إن المسؤولية في مجال المعلومات التي تبث عبر شبكات الانترنت مسؤولية موضوعية تقوم على أساس الخطأ المفترض من واقع حيازة المعلومات وحراستها، و التي يحكمها نصوص المواد 138من القانون المدني، و يرى هذا الرأي انه بالنسبة لتطبيق المسؤولية المفترضة في مجال شبكات الانترنت، فان هذه المسؤولية قد توجد بشقيها :

الشق الأول : و يتعلق بالمسؤولية عن حراسة المعلومات ، و ذلك بعد الاتفاق على اعتبار المعلومة شيئا غير مادي يدخل في مفهوم المادة 138 من القانون المدني الجزائري [2]، و المادة 1/1384 مدني فرنسي [3]، و بذلك يكون حارسها و الذي يكون غالبا هو المورد هو المسؤول عن الأضرار التي يسببها بث المعلومة عبر الشبكة للغير، ولا يعفي من المسؤولية إلا بإثبات السبب الأجنبي .

---

[1]–محمد عبد الظاهر حسين، المسؤولية القانونية في مجال شبكات الانترنت، دار النهضة العربية ،2002،ص 116 و ما بعدها و قد أشار إليه خالد ممدوح إبراهيم ، امن الجريمة الالكترونية ، هامش ص 35 .

[2]– سواء قبل التعديل أو بعده " كل من يجب عليه قانونا أو إتفاقا رقابة شخص في حاجة إلى الرقابة بسبب قصره أو بسبب حالته العقلية أو الجسمية ، يكون ملزما بتعويض الضرر الذي يحدثه ذلك الشخص للغير بفعله الضار. ويستطيع المكلف بالرقابة أن يتخلص من المسؤولية إذا أثبت أنه قام بواجب الرقابة أو أثبت أن الضرر كان لابد من حدوثه ولو قام بهذا الواجب بما ينبغي من العناية"

[3] – Article 1384 "On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde". Modifié par Loi n°2002-305 du 4 mars 2002 - art. 8 JORF 5 mars 2002.

الشق الثاني : و يتعلق بمسؤولية المتبوع عن التابع، وهو يتحقق في مجال الانترنت في حالة ان تتولى شركة القيام بجميع مراحل بث المعلومات، ويسأل في مواجهة الشخص المضرور في جميع هذه المراحل، ويعد كل متدخل في أي مرحلة على الشبكة تابعا له و يسال عن فعله .

الفرع السابع : مصادر المعلومات الإلكترونية

تعرف مصادر المعلومات الإلكترونية: بأنه "تلك الفئة التي يتم تسجيلها أو إنشاؤها واختزانها والبحث عنها، واسترجاعها وتناقلها واستخدامُها إلكترونيا أو رقميا بواسطة الحاسب الآلي، سواء كانت محملة على أحد الوسائط المادية، كالأقراص المرنَة، أو الأقراص الصلبة، أو الأقراص المليزرة، أو متاحةً عبر الشبَكات".[1]

كما أن مصادر المعلومات قد تكون تقليدية ورقية، وقد تكون غير ورقية مخزنة الكترونيا على وسائط سواء ممغنطة، او ليزرية بأنواعها، و قد تكون المصادر اللاورقية مخزنة أيضا الكترونيا في ملفات قواعد بيانات و بنوك المعلومات متاحة للمستفيدين عن طريق منظومة الأقراص المكتزة، و المتطورة الأخرى مثل الأقراص المتعددة و أقراص DVD .

البند1: مصادر المعلومات الإلكترونية حسب الوسط المستخدم:

1- الأقراص الصلبة: وهي عبارة عن أقراص، أو قرص يحتوي على أسطوانة أو أكثر، مغَطاة بمادة يمكن تسجيل البيانات عليها مغناطيسيا، ومعها رؤوس للقراءة والكتابة، وأداة ميكانيكية لضبط حركة تلك الرؤوس وموتور لتدوير الأسطوانات، وجميعها محفوظة داخل علبة لحمايتها.

2- الأقراص المرنة: هو عبارة عن قرص رقيق ومرن، يستخدم لدرء المعلومات في الكمبيوتر وأجهزة تنسيق الكلمات.

[1]- خالد ممدوح إبراهيم، المرجع السابق ، ص 36.

3- الأقراص والأشرطة : هو قرص مستدير، مَطْلِي بمادة يمكن تسجيل البيانات عليها، وقراءتها بواسطة محرِّك الأقراص، أمَّا الشَّريط المُمَغنط فهو عبارة عن شريط ذي وجْهٍ ممغنط، تُخَزَّن عليه البيانات بمغنطة أجزاء معيَّنة من السَّطح، وأشرطة القيد والكاسيت والأشرطة التي تُسَجَّل عليها البيانات بالكمبيوتر .[1]

البند2: مصادر المعلومات الإلكترونية حسب نقاط الإتاحة وطرق الوصول

تقسم إلى :

1.الشبكات المحلية: وهي نظام يضم مجموعة من الحاسبات الآلية، يتم من خلالها تقاسم البرامج والبيانات المتوافرة

2.قواعد البيانات الداخلية أو المحلِّية:وهي البيانات والمعلومات التي تعكس نشاطات وخدمات مؤسسة معينة. الفهارس المتاحة على الخط المُباشِر.

3.شبكة الإنترنت: على الرغم من أن شبكة الإنترنت لم تستطع على عالمنا إلا منذ سنوات قليلة، إلا أنها استطاعت أن تثبت جدارتها في كونها إحدى أهم الوسائل التكنولوجية الحديثة، التي تستطيع تلبية الاحتياجات الفعلية للمستفيدين من المعلومات في كافة قطاعات المعرفة البشرية، في أي وقت من الأوقات فقط من خلال الضغط على الفأرة، فأصبحت بمثابة قناة المعلومات الرئيسية التي يمكننا من خلالها الإبحار حول العالم، إلى جانب قدرتها على إعداد قاعدة اتصالات عريضة بين كافة المستفيدين على مستوى العالم.

واستطاعت شبكة الإنترنت أن تثبت جدارتها في كونها إحدى أهم وأحدث التقنيات التكنولوجية، التي تستطيع تلبية الاحتياجات الفعلية للمستفيدين في كافة قطاعات المعرفة البشرية،

[1]- أمل وجيه حمدي، المصادر الإلكترونية للمعلومات، الدار المصرية اللبنانية، القاهرة، ط1، 2007م، ص 55.

باعتبارها مصدراً خصباً للبحث في الإنتاج الفكري بما يتوافر عليها من قواعد بيانات ببليوجرافية، وقواعد [1]:

بيانات النص الكامل فأصبحت بذلك الشغل الشاغل لمختلف شرائح المجتمع، باعتبارها قناة المعلومات الرئيسية التي يمكننا من خلالها الإبحار حول العالم.[2]

البند3: وتتنوع مصادر المعلومات الالكترونية حسب التغطية و المعالجة الموضوعية، وتنقسم إلى:

1. مصادر المعلومات الموضوعية ذات التخصصات المحددة والدقيقة، وهي التي تتناول موضوعا محددا أو موضوعات ذات علاقات مترابطة مع بعضها .

2. مصادر المعلومات الموضوعية ذات التخصصات الشاملة، أو تعرف أحيانا بغير المتخصصة، و تمتاز بالشمولية و التنوع الموضوعي لقواعد البيانات التي تحويها، إضافة إلى كثرة هذه القواعد التي تزيد دائما على الخمسين و تصل إلى بضعة مئات في بعض الحالات .

3. مصادر المعلومات العامة : و هي ذات توجيهات إعلامية و سياسية و لعامة بعد النظر عن تخصصاتهم و مستوياتهم العلمية و الثقافية .

4. مصادر المعلومات التليفزيونية : وهي من الأنواع الحديثة لمصادر المعلومات الالكترونية، و المتميزة في طبيعة المعلومات التي تقدمها كونها تجيب على طلبات وتلبي احتياجات الناس الاعتياديين، وبعبارة أخرى فهي تخص الحياة العامة و المتطلبات اليومية والمعيشية، فهي وليدة المجتمع المعلوماتي الجديد، والتي تسد إحدى خدمات المعلومات في المجتمعات التي تركز غالبا خدمات المعلومات للباحثين، ويمكن للمستفيد هنا أن يحصل على المعلومات من خلالها وهو في البيت أو المكتب وعبر التلفزيون الإعتيادي، وتقدم معلومات عن السفر والسياحة والفنادق، أجبار المال

---

[1]– عامر إبراهيم قنديلجي، إيمان فاضل السامرائي، حوسبة المكتبات، ط1، دار المسيرة، الأردن، 2004،ص225

[2]– نرمين عبد القادر، رقابة شبكة الإنترنت، دراسة لتطبيقات برامج الحجب في المكتبات ،قسم المكتبات – جامعة القاهرة،ص1.

والتجارة والأسواق المالية، فرصة العمل، حركة الطائرات، التسويق والترويج للسلع، الرياضة، التسلية والترفيه، الطقس والمناخ، أخبار العالم، العقارات، إعلانات .... إلخ .

وتعرف عادة ببنوك المعلومات التلفزيونية (الفديو تكس *Video text – Video Data* أو الفيديو تكس المتفاعل *(Interactive Video text)* ومن أشهر هذه المصادر ما يعرف بنظام *(Ceefax, Prestol)* في بريطانيا *(Teletell)* في فرنسا[1].

5. مصادر المعلومات الالكترونية حسب جهات المسؤولة عنها، و تقسم كالآتي :

1. مصادر المعلومات الكترونية تابعة لمؤسسات تجارية : و هي تكون هدفها الأول هو الربح المادي، وتتعامل مع المعلومات كسلعة تجارية و يمكن أن تكون منتجة أو بائعة أو موزعة ووسيطة .
2. مصادر المعلومات الالكترونية التابعة لمؤسسات غير تجارية : هذه المؤسسات لا تهدف للربح المادي كأساس في تقديمها للخدمات المعلوماتية، بقدر ما تبغي الأهداف العلمية و الثقافية و خدمة الباحثين .

الفرع الثامن : مدى انطباق وصف المال على المعلومات

من الأمور البديهية أن الجزء المادي من النظام المعلوماتي،[2]والمتمثل في جهاز الحاسب الالي والمعاهدات الملحقة به والأقراص بكافة أشكالها التي تخزن عليها المعلومات و غير ذلك، هي مال مادي له كيان خارجي، وبالتالي فجريمة الاعتداء عليها تصنف ضمن جريمة السرقة المنصوص عليها في قوانين العقوبات[3].

---

[1]- جاسم محمد جرجس وبديع محمود القاسم، مصادر المعلومات في مجال الإعلام والاتصال الجماهيري،مركز الإسكندرية للوسائط الثقافية والمكتبات، مصر، 1998،ص264 و ما بعدها.

[2]- إذا نظرنا في تحديد المقصود من الأموال في القانون المدني الجزائري05-10مؤرخ في 20يونيو سنة 2005 في المادة 682 على أنه (كل شيء غير خارج عن التعامل بطبيعته أو بحكم القانون يصلح أن يكون محلا للحقوق المالية). فالمعلومات يمكن الانتفاع بها و تحقيق عوائد مالية ضخمة منها، و هي لا تخرج عن التعامل بطبيعتها و حكم القانون .مثل البرامج الخاصة بالتعليم أو عرض موضوع ما، أو البرامج الأدبية و غيرها، و إذ يتم تخزينها على شكل أقراص صلبة أو لينة، و يمكن الحصول عليها من وكلاء التسويق ضياء مصطفى عثمان ،المرجع السابق،ص 105.

[3]- ضياء مصطفى عثمان ،المرجع السابق،ص 100 .

وهي ما سميت في فرنسا بجريمة التوصل بطريق التحايل لنظام المعالجة الآلية الالكترونية للبيانات[1]، وهي جريمة مستحدثة تناولها المشرع الجزائري[2] ونظيره الفرنسي بموجب القانون رقم 19لسنة 1988بشأن بعض جرائم المعلوماتية في مادته 2/462[3]

اما فيما يتعلق بالشق المعنوي للنظام المعلوماتي و المتمثل في المعلومات و البرامج و غير ذلك، فان التساؤل الذي يطرح هل بالإمكان انطباق وصف الأموال عليها برغم طبيعتها اللامادية ؟

- بناءا على مفهوم المال و علاقة المنفعة به عند الفقهاء، يمكن تخريج رأي الفقهاء في مالية المعلومات إلى رأيين :

---

[1]– محمد سامي الشوا، الغش المعلوماتي، بحث في مؤتمر الجمعية المصرية للقانون الجنائي،القاهرة،-25-28 أكتوبر -1993 ،ص 521.

[2]– المادة 394 مكرر : يعاقب بالحبس من 3 أشهر إلى سنة 1 و بغرامة من 50.000دج الى 100.000دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.
– و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتعال المنظومة تكون العقوبة الحبس من 6 أشهر إلى سنتين 2 و الغرامة من 50.000دج إلى 150.000دج... تمم الفصل الثالث بالقانون 04-15 المؤرخ في 10 نوفمبر 2004- ج .ر.71 ص 11و 12 – و يتضمن المواد من 394 مكرر إلى 394 مكرر7.في القسم السابع مكرر الموسوم بالمساس بأنظمة المعالجة الآلية للمعطيات.

[3] – Loi numéro 88-19 DU 5 janvier 1988 relative a la fraude informatique.

-Art 462-2 alinéa 1er : délit d'intrusion dans le système d'autrui 1.1 Art 462-2 alinéa 1er

"Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatise de données sera puni d'un emprisonnement de 2 mois à un an et d'une amende de 2 000 F à 50 000 F ou de l'une de ces 2 peines seulement."

1.2 système informatique.

L'accès indu et le maintien indu dans un système informatique sont incrimines. L'accès non autorise dans le système est donc réprimé, alors même qu'il n'en ait résulte aucun préjudice. Le seul fait d'entrer dans le système sans qu'il y ait lieu à considère le but poursuivi ou les conséquences possibles, est incriminable en temps que tel. Le maintien non autorise dans un système, même de manière parfaitement inoffensive est incriminable. La personne poursuivie doit avoir pénétré le système ou s'être maintenu dans celui-ci sans y avoir droit. Non respect des conditions d'accès au système ou de maintien dans celui-ci.

1.3 La personne ou élément moral

Il s'agit d'un délit volontaire puisque l'accès et le maintien dans le système doivent avoir été accomplis frauduleusement. L'auteur ou les auteurs doivent avoir conscience de l'irrégularité de leur acte. Le maintien volontaire dans un système d'autrui est incriminable.

Exemples :

- Piratage d'un compte d'un autre utilisateur en utilisant un faux login
- Tentative de connexion dans un système en utilisant toutes les combinaisons possibles de login et de mots de passe.
- Recherche d'informations afin de contourner les mécanismes de sécurité (parcours d'une hiérarchie système ou utilisateur).

- الرأي الأول : المعلومات ليست مالا، تخريجا على رأي الحنفية لأنهم يشترطون في المال أن يكون ماديا ذا وجود خارجي، و المعلومات ليست ذات وجود مادي خارجي فهي بحسب مفهومهم للمال لا تعدوا أن تكون منفعة، و المنفعة عندهم ليست مالا .
- الرأي الثاني :المعلومات مال تخريج على رأي جمهور الفقهاء و ذلك :

1. لأنهم لا يشترطون في المال أن يكون ماديا ذا وجود خارجي، ليس ذلك و حسب،بل لأنهم عدوا المنافع أموالا، فعلى فرض أن المعلومات ليست عينا بل منفعة فهي بهذا الاعتبار تعد مالا.
2. إن المعلومات مما ينتفع به عادة و شرعا، ولها قيمة مادية في عرف الناس، وهذا من ضوابط المالية عند الفقهاء .

بناءا عليه فانه وبحسب طبيعة المعلومات، يمكن أن ينطبق عليها شرط المالية عند الجمهور بخلاف الحنفية .

و ذهب اغلب شرّاح القانون إلى أنها مال، وتصلح لان تكون محلا للاعتداء و السرقة، و ذلك لأن وصف المال عندهم لا يقتصر على ما كان جسما متميزا قابلا للوزن، طبقا لنظرية الطبيعة، بل هو يتناول كل شيء مقوم قابل للتملك .

و إذ كانت المعلومات قد تم الاستيلاء عليها بقصد الاستخدام و الانتفاع بها دون دفع المقابل لصاحبها، فإنها تكون محمية بنصوص قوانين الملكية الفكرية، كما لو كانت معلومات تتعلق باختراع أو فكرة أو برنامج معد للبيع .

هنالك اتجاه يؤيده رأي الحنفية، يعرف المال على انه كل شيء يمكن حيازته ماديا، وبالتالي فالأشياء المعنوية لا تتمتع من وجهة نظره بصفة المال، فهذا الاتجاه ينظر إلى المعلومات باعتبارها عديمة القيمة أو ذات قيمة منخفضة .

إلا أن التطور الحاصل –المشار إليها في مقدمة هذا المبحث – أدى إلى البحث عن معيار آخر غير معيار مادية المال، اذ تم اللجوء إلى معيار القيمة الاقتصادية للشيء حيث يعتبر الشيء ليس مالا ليس بالنظر إلى ما له من كيان مادي ملموس فحسب، و إنما بالنظر إلى قيمته الاقتصادية .

ويمكن القول إن بقاء الاتجاه الذي يعد مادية الشيء هي الأصل في المالية عند البعض يعتبر جمودا، لأنها نظرة منعزلة عن الواقع الموجود، و غير مواكبة للتطورات الهائلة التي حصلت، وهذا ما ذهب إليه الأستاذ (كاربونير) حيث قال : "انه من الواضح أن أي قانون يرفض أن يرى قيمة في شيء له أهمية اقتصادية سيبقى حتما بمعزل عن الحقيقة" .

- إذن لابد تثبيت أمرين :

أ. القيمة المادية للمعلومات في عرف الناس

ب. جواز الانتفاع بها

البند الأول : القيمة المادية للمعلومات

بالنسبة للقيمة المادية للمعلومات، فيرجع الفضل في إضفاء وصف القيمة المادية على المعلومات إلى الإسلام العظيم، فالرسول صلى الله عليه و سلم بين في موقفه من أسرى بدر قيمة المعلومات، بحيث جعل فداء كل أسير أن يعلم عشرة من أبناء المسلمين، كما انه صلى الله عليه و سلم كان لا يكشف وجهته في الحرب حرصا على عدم تسرب المعلومة المهمة، وهذا كله يشير إلى اعتبار المعلومات ذات أهمية اعتبارية و مادية[1] .

لا يوجد ثمة شك بان المعلومات تعد المفتاح الذهبي للنشاطات الاقتصادية المثمرة بعصرنا الراهن، كما أنها باتت تمثل أكثر الموجودات المهمة للمؤسسات و الشركات من اجل هذا ذهب البعض إلى القول "إن التنظيم الذي كان يدور حول تداول الاشياء، و رأس المال قد تحول بكليته إلى إدارة عجلة الاقتصاد حول المعلومات.

وبناءا على ما للمعلوماتية من قيمة اقتصادية و مالية، فقد اتجه الرأي الغالب إلى أن المعلومات تعتبر مالا متقوماّ و تتمتع بحق الحماية، يستوي في ذلك أن تكون المعلومة مبتكرة، فان كانت مبتكرة فهي محمية بتشريعات حماية حقوق المؤلف و أحكام الملكية الفكرية .

[1]- ضياء مصطفى عثمان ،المرجع السابق، ص 102.

و إن لم تكن مبتكرة فالمال المعلوماتي يجب أن يكون محميا بنصوص خاصة، وان تكيف تشريعات جزائية تتلاءم مع التطور الهائل لتكنولوجيا المعلومات و حماية الثورة المعلوماتية من الاعتداء .

وقد وضح (فيفانت)[1] قيمة المال المعلوماتي بربطه بالملكية الفكرية، فالملكية الفكرية التي يحميها القانون تقوم على أساس واحد و هو أن للمعلومة قيمة مادية من الناحية القانونية، و سواء كانت هذه المعلومة في شكل براءة اختراع أم نموذج أم مؤلف أم كانت مجرد معلومة تنتمي لمؤلفها فانه يجب الاعتراف بوصف القيمة لها، وانتهى فيفانت إلى ما اسماه بالقيمة المعلوماتية و هي حقيقة تحتاج إلى إرساء نظرية عامة بشأنها .

فالمعلومات المخزنة إلكترونيا أو ما يسمى المادة الإلكترونية، هي نتاج علمي لعمل العقول البشرية بما يحقق مصالح الخلق في تسيير شؤونهم الدينية، و هي أن اتخذت هده الصفة إلا أنها تعتبر أيضا سلعة مرجو الانتفاع منها بما يعود ريعه على صاحب المعلومة أو الإنتاج الفكري .

و بما إن الإنتاج العلمي المتمثل في المادة الالكترونية لا يبقى أبدا في ذهن المنتج على صورته المجردة، بل ينفصل عنه ليستقر في صورة مادية شانها في ذلك شان الأفكار المتخذة من الكتاب محلا لها، فالمادة الالكترونية سواء كانت مستقرة في عين مادية كقرص صلب ام كانت مخزنة في الحاسب الآلي، فإنها سلعة تحمل منفعة جرى العرف على تمولها، و اقرها ّ الفقه الإسلامي، لكونها علاقة اختصاص ولا تصادم نصا شرعيا .

البند الثاني: جواز الانتفاع بالمعلومات

إذا كان للمعلومات قيمة مادية بين الناس، فهي حتما ينتفع بها، فالمال عصب الحياة، وقوام الأمم وقوتها، والمعلومات أو المادة الالكترونية يمكن احتواؤها واستفتاء منفعتها وهي المقصودة، وبما أن المعلومات ليست مقصودة لذاتها، بل المقصود تحصيل منافعها، كما يقول العز بن عبد السلام: " إن المنافع هي المقصود الأظهر من جميع الأموال، إذ لا يمكن أن تحاز المنافع إلا بحيازة

[1] – Michel Vivant, Informatique et propriété intellectuelle, A-propos des biens informatique , Édition générale , doctrine, 1984, no 3169.p p31-32.

أعيانها، وقد جرى العرف بين الناس على حيازة المادة الالكترونية كسبيل لتحصيل الفائدة منها، فقد أضحى لها قيمة بين الناس، و الناس لا يحوزون مالا قيمة له، و ما له قيمة يعد ملا، فكل ما فيه منفعة فيه قيمة، و بقدر المنفعة تكون القيمة المالية، فالمنفعة مناط القيمة سواء في ذلك الأعيان أم المنافع أم الأمور المعنوية.

- **فالمعلومة أصبحت منفعة و مصدر قوة للمعرفة و الحصول على المعرفة و حسن استخدامها عاملان أساسيان من عوامل التقدم، ولذلك فان التكنولوجيا الحديثة تتعلق بالمعرفة** [1].

الفرع التاسع : حقوق الإنسان من المعلومات

هناك تخوف من تدني مؤشرات حقوق الإنسان من المعلومات، خصوصا في ظل هذه التطورات المتلاحقة لموجات التطور التقني، لمعالجة المعلومات وباتت مؤسسات المعلومات تهتم بترويج المعلومة باعتبارها سلعة وليس باعتبارها خدمة ومن هذه المؤشرات: [2]

1- الاتجاه نحو تركيز خدمات المعلومات في عدد من شركات تقنيات المعلومات، التي تهتم بالربح في المقام الأول.

2- تركيزها لدى الشركات التجارية بهذا الشكل، قد يوفر أرضا خصبة لضياع حقوق الفرد من المعلومات، وذلك لحكرها على ذوي اليسار مما يلحق الضرر بالفرد غنياً كان أو فقيراً.

3- استفادة المناطق الريفية ببطء وفي ذلك عدم عدالة في التوزيع، بالمقارنة بالمناطق ذات الاهتمام البؤري التي تتركز فيها عناصر الخدمة، صحيح أن الاتصالات بعيدة المدى *Télécommunications* ،قد وفرت الكثير من الخدمات لمثل هذه المناطق النائية إلا أن لمثل هذه الأبعاد الكثير من الانتقادات.

4- إن أغنياء المعلومات ربما يكونون دولاً أو مؤسسات، وربما يكونون أفراداً أيضاً، لأن الفرد هنا يستطيع من محطة تشغيل واحدة أن يقوم بمئات الوظائف في مجالات تجميع وتجهيز البيانات،

---

[1]- ضياء مصطفى عثمان ،المرجع السابق، ص 104.

[2]- تكنولوجيا المعلومات في المكتبات ومراكز المعلومات العربية بين الواقع والمستقبل (وقائع أوراق المؤتمر العربي الثامن للمعلومات، برعاية الاتحاد العربي للمكتبات، والجمعية المصرية للمكتبات، جامعة القاهرة 1-4 نوفمبر 1997.(محمد محمود مكاوي ، مجتمع المعلومات في المملكة العربية السعودية، اللجنة الاقتصادية والاجتماعية لغربي آسيا: الاسكوا، 2004. حسني عبد الرحمن الشيمي، اللاورقية أو الكتاب الورقي بين الزوال والبقاء، القاهرة، ط1، 1993.

وبث ونشر المعلومات، مستعيناً في ذلك بمراصد المعلومات ووسائل الاتصال الوطنية والدولية جميعاً.

و ختاما لمضمون هذا المبحث يمكن القول أن الأمن، هو مجموع القواعد، التي يضعها مسؤولو الأمن في أي مكان، والتي يجب أن يتقيد بها، جميع الأشخاص الذين يمكنهم الوصول إليه. فمفهوم الأمن مفهوم واسع، يطال جميع عمليات الدخول، والخروج، والبقاء، أو التصرف، في مكان ما.

وعليه يشمل الأمن في الفضاء الرقمي، قواعد وأصول ضبط الإتصال، وإنتقال المعلومات، وتخزينها وحفظها، كما يشمل أمن المواقع، وأمن الأنظمة الإلكترونية، وعمليات استثمارها، إضافة إلى امن الاتصالات .

والأمن بحسب الإعلان الأوروبي[1]،هو قدرة النظام المعلوماتي على، مقاومة محاولات الاختراق، أو الحوادث غير المتوقعة، التي تستهدف البيانات .

و فيما يلي سنتعرف على الأركان الرئيسية لأمن المعلومات و التحديات التي يمثلها الأمن الرقمي.

[1] - Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques Journal officiel n° L 013 du 19/01/2000 p. 0012 - 0020, décret no 2001-272 du 30 mars 2001 en France, décret no 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

المبحث الثاني: الأركان الرئيسية لأمن المعلومات والتحديات التي يمثلها الأمن الرقمي

أهم ما يميز هذا العصر هو توفر المعلومات وسهولة الحصول عليها من مصادر مختلفة ومتعددة، وتتفاوت نوعية هذه المعلومات وخصائصها باختلاف مصادرها، ولكنها تتحد في إمكانية نسخها بأقل التكاليف وإمكانية تعديلها أو حذفها بدون ترك أية آثار تدل على ذلك، ما لم تتوفر الحماية اللازمة لمصادر هذه المعلومات من خلال الاعتماد على أنظمة أمن المعلومات.

المطلب الأول : الأركان الرئيسية لأمن المعلومات

يتخلص هدف جميع مستخدمي الانترنت،[1] في الحصول على المعلومات و نقلها بشكل امن، وهناك مجموعة من التحديات التي يجب أخذها في الحسبان، لضمان نقل امن المعلومات بين الاطراف المتصلة، وتنحصر هذه التحديات في ثلاث محاور هي : الخصوصية (*privacy*)، وسلامة المعلومات (*IntergrIity*)،والتحقق من هوية الاطراف الاخرى (*Peer authentication*) [2].

الفرع الأول: السرية *Confidentiality*.

حماية و سرية المعلومات: انه من الضروري ايجاد وسائل لنيل ثقة الناس و توفير الضمانات لهم حيال استخدام الحكومة الالكترونية،[3] و بالتالي فان مسالة الحماية و سرية المعلومات، فهي من العوامل الهامة جدا بل و الاساسية لنجاح الحكومة و التجارة الإلكترونية[4] .

أن الأنترنت بطبيعتها عبارة عن محيط مفتوح من عمليات الحاسوب، و بالتالي فإنها مفتوحة و معرضة للعديد من المخاطر المتعلقة بالحماية و سرية المعلومات، ومن أكثر الأساليب التي يتبعها المتطفلون و المخربون لاختراق الانظمة ما يلي :

1. البرمجيات الخبيثة والبرمجيات التجسسية (*Spyware*) :

---

[1]- عبد الله الكرم ونجيب محمد العلى، التعلم الإلكتروني، المفهوم والواقع والتطبيق، التربية والتعليم وتكنولوجيا المعلومات في البلدان العربية، الهيئة اللبنانية للعلوم التربوية، الكتاب السنوي، 4ط،2005، ص .ص 131 - 156.

[2]- أبو بكر محمود الهوش، الحكومة الإلكترونية، الواقع و الآفاق، مجموعة النيل العربية ،ط2006،1، القاهرة،ص372 .

[3]- ذياب البداينة، المنظور الاقتصادي والتقني والجريمة المنظمة، أبحاث الحلقة العلمية حول الجريمة المنظمة وأساليب مكافحتها،نوفمبر1998م،أكاديمية نايف العربية للعلوم الأمنية،الرياض،1999م،ص ص 210 – 215.

[4]- حسن طاهر داوود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 1999،ص ص 65-66 .

هي عبارة عن برمجيات صغيرة يقوم المستخدم بتحميلها، والموافقة على تمكينها في حاسوبك الشخصي، وهذه البرمجيات تراقب باستمرار كما كبيرا من المعلومات، بعضها يتعلق بالذوق الموسيقية وبعضها الاخر يقوم بتسجيل نوع السواقة الصلبة الموجودة في الجهاز، الى جانب رقمها التسلسلي فيما تستطيع بعض هذه البرمجيات نقل رقم بطاقة اعتماد استعملتها في شراء سلعة من شركة ما .

صممت البرمجيات الخبيثة حسب موقع مايكروسوفت بهدف إلحاق الضرر بحاسوب واحد أو أكثر وتعتبر الفيروسات والبرمجيات التجسسية وبرامج (حصان طروادة) أنواعا من البرمجيات الخبيثة.

أما البرمجيات التجسسية: فهي برمجيات تراقب المعلومات الشخصية المخزونة على جهاز الحاسوب، وتسجل المواقع التي يجري الولوج إليها على شبكة الانترنيت بهدف توجيه رسائل دعائية تتلاءم مع ذوقك.

- **فكيف تنتقل هذه البرمجيات إلى جهاز الحاسوب ؟ وهل هي معدية ؟ وما هي أعراض الإصابة ؟**

تأتي البرمجيات الخبيثة من عدة مصادر وتعتبر شبكة الانترنيت أساسا لجميع هذه المصادر، ويمكن اعتبار البرمجيات الخبيثة طفيليات تعيش على شبكة الانترنيت .

وتنتقل هذه البرمجيات إلى حاسوبك عند تحميل برامج صغيرة من شبكة الانترنيت، وخاصة عندما يطلب منك الموافقة بالنقر على "ok" لمتابعة التأكد من أداء جهاز الكمبيوتر، مثلا او عندما تعد بعض البرامج المستخدمة بإمكانية الولوج المجاني إلى مواقع المراهنة، وهذه البرامج قد تحتوي على برمجيات تجسسية تحمل وتجهز على الحاسوب بعد النقر على زر المتابعة، هذا وتقوم مواقع أخرى بتضمين موافقة المستخدم لرخصة الاستخدام قبولا بتحميل وتشغيل هذه البرمجيات على حاسوبه .

و لم تثبت حتى الآن إمكانية انتشار هذه البرمجيات عبر الانترنيت، وعبر الشبكات إذ أنها تنتقل عند تحميل برامج أخرى من الشبكة لاسيما وان معظم أنظمة التشغيل تحتاج إلى تدخل من المستخدم لتحميل برمجيات إضافية، ولكن هذا قابل للتغيير في أية لحظة بحيث يمكن في المستقبل ان تنتقل هذه البرمجيات مع الفيروسات، وعندئذ ستكون الكارثة .

و لم يبدأ العاملون في مجال تكنولوجيا المعلومات والاتصالات إلا مؤخرا بالتنبه إلى هذه البرمجيات الخبيثة أو التجسسية، وضرورة التعاطي معها على أساس أنها مشكلة يجب إيجاد الحلول لها .

وفي غياب الإحصاءات الدقيقة يمكن القول ان معدل انتشار هذه البرمجيات يتجاوز الخمسين في المائة من مجموع الحواسيب المتصلة بالأنترنيت في العالم[1].

ولكي نتخلص من هذه البرمجيات الخبيثة ينبغي تثقيف مستخدمي الحاسوب بخطورة هذه البرمجيات وخطورة الولوج إلى المواقع التي تنشر مثل هذه البرمجيات . كما يجب قراءة نص رخصة الاستخدام للبرمجيات التي يجري شحمها من الانترنيت على وجه الخصوص بدقة قبل القبول بها .

وفيما يستعد مجتمع تكنولوجيا المعلومات والاتصالات إلى مواجهة الخطر الداهم، تنحصر مسؤولية المستخدم بمراقبة حاسوبه بانتظام وباستخدام مواقع الأمن السيبراني، للحصول على المعلومات والأدوات التي تسمح بفحص الأجهزة وإزالة العدوى دوريا.

2. إغراق ذاكرة (*buffer*) : و هي أسلوب هجوم شائع الاستغلال، ويمكن تنفيذه بأساليب مختلفة، حيث يكشف المخترقون أساليب جديدة له في كل يوم، كما أن هذا الأسلوب يستخدم للحصول على معلومات "سوبر يوزر " من اجل الدخول إلى النظام و تدميره .

3. الهجوم على لب النظام (*kernal attack*) : و هو أسلوب هجوم متقدم يتيح للمخترق، تثبيت برمجيات في لب نظام التشغيل نفسه بغرض السيطرة على أوامر النظام،وعلى استدعاءاته وعرض العمليات، والدخول إلى البيانات بغرض التسبب في تدمير النظام .

4. ثغرات أمنية في التطبيقات: من البديهيات في عالم الحاسوب ألا يخلو برنامج من أخطاء (*bugs*)، و بخاصة إذا أخدنا في الاعتبار سرعة سوق تطبيقات الأعمال الإلكترونية

5. ((*e-business*))، والتي يمكن استغلال العديد منها الحصول على مدخل للتطبيقات الأخرى او للأنظمة نفسها.

6. نصوص *CGI*: من المعروف أن نصوص *CDI* مليئة بالأخطاء بطبيعتها، و تتضمن ثغرات امنية يمكن استخدامها بسهولة لمهاجمة خادمات الويب[1] .

[1]- كريمة شافي جبر، الإرهاب المعلوماتي، مركز المستنصرية للدراسات العربية والدولية، مجلة كلية الآداب، العدد 96، ص 645.

7. تشمم كلمات السر (*password sniffing*): كثيرا ما يستخدم المخترقون هذا الأسلوب على الحصول على مدخل يخترقون به الأنظمة، وهم يقومون بذلك بعدة طرق، إما بمحاولة تخمين كلمات السر لمستخدمين شرعيين، أو باعتراض طريق كلمات السر أثناء انتقالها عبر الشبكات غير مشفرة..

8. الخطأ الإنساني: تعتمد المؤسسات على الممارسات الأمنية لموظفيها لحماية أنظمتها، ومع ذلك فانه من الشائع للمخترقين، أن ينتحلوا صفة الموظفين في دوائر تكنولوجيا المعلومات أو في دوائر شركات لها علاقة بالشركة المستهدفة، أو من خلال نشاطات اجتماعية للمهندسين من اجل الوصول إلى كلمات سر لأجهزة حاسوب، يمكن استغلالها فيما بعد بغرض السرقة أو التدمير.

9. الفيروسات و حصان طروادة : وهي برامج توحي للمستخدم بأنها تقوم بعمل معين، بينما هي في حقيقة الأمر تقوم بعمل آخر، ويكون ضارة على الأغلب وتتميز عن الفيروسات بكونها غير قادرة على إنتاج نفسه.

10. القنبلة المنطقية *Bombard Logical* : وهي برامج شبيهة إلى حد ما بالفيروس ويتم تنشيطها بوقوع حدث أو حالة معينة ويمكن أن تكون جزءا من برنامج الفايروس *Virus* أو حصان طروادة .

---

[1] - La Common Gateway Interface (littéralement « Interface de passerelle commune »), généralement abrégée CGI.

Au lieu d'envoyer le contenu d'un fichier (fichier HTML, image), le serveur HTTP exécute un programme, puis retourne le contenu généré. CGI est le standard industriel qui indique comment transmettre la requête du serveur HTTP au programme, et comment récupérer la réponse générée. Un exemple classique de paramètre est la chaîne de caractères contenant les termes recherchés auprès d'un moteur de recherche.

La Common Gateway Interface (littéralement « Interface de passerelle commune »), généralement abrégée CGI, est une interface utilisée par les serveurs HTTP. Elle a été normalisée par la RFC 3875

- http://httpd.apache.org/docs/current/fr/howto/cgi.html
- http://wiki.uniformserver.com/index.php/CGI:_VBScript_CGI

ويلجأ إرهابيوا المعلوماتية إلى تحميل ملفات مفَورسة على الشبكة، في بعض المواقع الأكثر زيارة، بعض الملفات المفَورسة تنتقل مباشرة عبر الشبكة إلى الحاسوب بمجرد فتح الموقع، وبعض آخر يكمن للمستخدم في ملفات معينة ما إن يقوم بفتحها حتى ينتقل الفايروس إلى حاسوبه .

11. رفض الخدمة (*denial of service*) : في هذا النوع من الهجمات يتم إغراق جهاز الحاسوب الخادم بسيل من الطلبات المزورة تسبب في إغلاق الجهاز، أو إبطاء عمله، و يستغل فغي الغالب لتنفيذها أجهزة قوية أخرى ثم السيطرة عليها بعد اختراقها (تسمى أجهزة زومبي)، حيث تزرع فيها برمجيات لتوليد هذه الطلبات المزورة و إرسالها بشكل تلقائي.

12. إن هناك الكثير من الأساليب التي يمكن إتباعها للحد من تلك الاختراقات والتقليل من مخاطرها، وتعتبر أنظمة منع الاختراق القائمة على أنظمة تشغيل موثوقة(*operating trusting system*) من الوسائل الجيدة، ومنها منتج *pit bull* الذي يمتاز بتوفيره لحماية على مستوى نظام التشغيل نفسه، مما يشكل نظام عزل يغلف التطبيقات من دون أن يتدخل بها و يمنع أي محاولات لاستغلالها قبل الوصول اليها[1].

إن الأمن ألمعلوماتي يتطلب نظام حماية على مستويين أثنين :

الأول: حماية حاسوب المستخدم من الاختراق سواء كان الاختراق لهدف القرصنة او لعمل تخريبي.

الثاني: حماية المواقع أو السيرفر والمقدّم، أو الذي يؤمن اتصال بالأنترنيت وهذا عمل عصي على الأفراد، بل يجب أن تقوم به الحكومات أو الشركات الكبرى نظرا للتكلفة المادية الكبيرة التي يتطلبها هذا المستوى من الحماية[2] وهذا الجانب يشتمل على الإجراءات والتدابير اللازمة، لمنع إطلاع غير المصرح لهم على المعلومات التي يطبق عليها بند السرية أو المعلومات الحساسة، وهذا

[1] - EM milner, managing information and knowledge in the public sector , routledge,london,2000.p 78.

[2]-D.M. Trent Hackers , crackers , and Trackers American legion magazine .,February , 1997, p.34.

هو المقصود بأمن وسرية المعلومات[1]، وطبعاً درجة هذه السرية ونوع المعلومات يختلف من مكان لآخر وفق السياسة المتبعة في المكان نفسه، ومن أمثلة هذه المعلومات التي يجب سريتها: المعلومات الشخصية للأفراد، الميزانية المالية للشركات قبل إعلانها، المعلومات والبيانات العسكرية الخاصة بالجيوش والمواقع العسكرية في البلاد.[2]

الفرع الثاني : الموثوقية وسلامة المحتوى*Integrity*

يؤمن النظام الآمن تكاملية البيانات المخزنة فيه،[3] ويقصد بالتكاملية حماية البيانات من عمليات الحذف والتخريب[4]،ويتم تأمين ذلك من خلال مجموعة من الأساليب توفرها نظم قواعد المعطيات كقوائم النفاذ والصلاحيات، بالإضافة إلى علاقات الترابط *Referential Integrity* ما بين البيانات المخزنة فيها.

كما يؤمن النظام الأمن تكامل البيانات المرسلة، لمعرفة فيما إن تم تعديل أو حذف أي جزء منها أو أنها غير مكررة، وتحقيق ذلك يمكن أن يتم من خلال توليد مفتاح أو جواز مرور (توقيعاً) للرسالة المرسلة، باستخدام بعض الخوارزميات، مثل خوارزمية*MD5*[5].

---

[1] -Bernard Foray, La fonction RSSI ,Responsable Sécurité Système d'Information, Guide des pratiques et retours d'expérience - 2e édition, Dunod, 2011,P60

[2]–يسري زكي، تبسيط أمن المعلومات والاتصالات، متاح على الرابط: yomgedid.kenanaonline.com

[3]– محمد محسن عمر، الإدارة والتقنية، شركاء في مواجهة عصر الإنترنت، بدون طبعة، بدون سنة النشر، 1997م، ص ص 162 –164.

[4] – récupère ; Cryptologie : la science relative à la protection et à la sécurité des informations notamment pour la confidentialité, l authentification, l intégrité et la non répudiation ; Cryptologie (Moyens de): l ensemble des outils scientifiques et techniques (matériel ou logiciel) qui permettent de chiffrer et/ou de déchiffrer ; Cryptologie (Prestation de): toute opération visant la mise en œuvre, pour le compte de soi ou d'autrui, des moyens de cryptologie… La Convention de l'Union Africaine (UA) sur la Cybersécurité et la protection des données à caractère personnel a été finalement adoptée par la 23ème Session Ordinaire de la Conférence de l'Union qui s'est tenue le 27 juin à Malabo, République de la Guinée Equatorial.

[5] - L'algorithme MD5, pour Message Digest 5, est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier (on parle souvent de *message*). Il a été inventé par Ronald Rivest en 1991.

أو خوارزمية *SHA*[1] ، وتضمين إذن المرور هذا مع كل رسالة ترسل عبر الشبكة، وبالتالي التأكد من أن الرسالة صحيحة و لم يتم العبث بها[2]

ففي هذا الجانب لا يكون الهم الأكبر هو الحفاظ على سرية المعلومات، وإنما يكون الحفاظ على سلامة هذه المعلومات من التزوير والتغيير بعد إعلانها على الملأ، فقد تقوم هيئة ما بالإعلان عن معلومات مالية أو غيرها تخص الهيئة وهنا يأتي دور الحفاظ على السلامة بأن تكون هذه المعلومات محمية من التغيير أو التزوير، ومن أمثلة ذلك مثلاً: إعلان الوزارات أو الجامعات عن أسماء المقبولين للعمل بها، تتمثل حماية هذه القوائم في أن تكون مؤمنة ضد التغيير والتزوير فيها، بحذف أسماء ووضع أسماء غيرها مما يسبب الحرج والمشكلات القانونية للمؤسسات، وأيضاً بالنسبة للمعلومات المالية بتغيير مبلغ مالي من 10000 إلى 1000000 وهذا هام جداً لما يترتب عليه من خسائر فادحة في الأموال.[3]

L'utilisation de cette fonction de hachage dans les signatures numériques peut conduire à de multiples scénarios d'attaqueet n'est plus considérée comme un composant fiable de l'infrastructure à clés publiques. Cependant dans le calcul de la « signature » d'un fichier il reste plutôt fiable, même si l'on ne peut pas assurer qu'il y a unicité entre l'empreinte calculée et le fichier ou message source :http://www.md5.fr/ ,

Bert den Boer, Antoon Bosselaers ,Collisions for the Compression Function of MD5, Berlin , London , Springer, 1993, p 293.

1 -SHA-1 (Secure Hash Algorithm) est une fonction de hachage cryptographique conçue par la National Security Agency des États-Unis (NSA), et publiée par le gouvernement des États-Unis comme un standard fédéral de traitement de l'information, (Federal Information Processing Standard du National Institute of Standards and Technology

(NIST)https://fr.wikipedia.org/wiki/SHA-1, LArticle originel, Bruce Schneier Cryptanalysis of SHA-1, sur le site,

www.schneier.com/blog/archives/2005/02/cryptanalysis

[2]- المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، ملتقى أمن المعلومات ،الاجتماع الثاني لرؤساء الإدارات المختصة بتقنية المعلومات بالنيابات العامة العربية،5/7-03-2012 بيروت ، الجمهورية اللبنانية، متوفر على الرابط التالي : http://www.shatharat.net

[3] -Frédéric Bongat, Sécurité des Systèmes d'Informations, la cryptographie appliquée, GNU, Documentation License,2008-2009, P7.

أنه من الضروري إيجاد وسائل لنيل ثقة الناس و توفير الضمانات لهم حيال إستخدام الحكومة الالكترونية، و بالتالي فان مسالة الحماية و سرية المعلومات فهي من العوامل الهامة جدا بل و الأساسية لنجاح الحكومة و التجارة الإلكترونية[1].

الفرع الثالث : استمرارية التوفر أو الوجود *Availability* .

لعله من المنطقي أن نعرف أن كل إجراءات وصناعة المعلومات، في الأساس ترمي إلى هدف واحد وهو إيصال المعلومات والبيانات، إلى الأشخاص المناسبين في الوقت المناسب، وبالتالي فإن الحفاظ على سرية المعلومات وضمان سلامتها وعدم التغيير فيها لا يعني شيئاً إذا لم يستطع الأشخاص المخولين أو المصرح لهم الوصول إليها[2]، وهنا تأتي أهمية الجانب الثالث من جوانب أو مكونات أمن المعلومات وهو ضمان وصول المعلومات إلى الأشخاص المصرح لهم بالوصول إليها من خلال توفير القنوات والوسائل الآمنة والسريعة للحصول على تلك المعلومات، وفي هذا الجانب يعمل المخربون بوسائل شتى لحرمان ومنع المستفيدين من الوصول إلى المعلومات، مثل حذف المعلومات قبل الوصول إليها أو حتى مهاجمة أجهزة تخزين المعلومات وتدميرها أو على الأقل تخريبها.[3]

هذا و يؤمن النظام الآمن استمرارية وصول المستخدمين إلى المعطيات الخاصة بهم دون أي تأخير، ولهذه الخاصية عدد من السمات المتمثلة في:

1. المقاومة *Resistance* وهي قدرة النظام على الحفاظ على نفسه من العمليات التي تجعله غير متاح للمستخدمين المخولين باستخدامه، (على سبيل المثال أن يكون النظام قادرا على منع تنفيذ استعلامات تتطلب حجز حيز كبير من ذاكرة المخدم)؛

---

[1]- حسن طاهر داوود، جرائم نظم المعلومات، المرجع السابق، ص ص65-66 .

[2] -Layton, P.Timothy,Information Security,Design, Implementation, Measurement, and Compliance. Boca Raton, FL: Auerbach publications, 2007, ISBN 978-0-8493-7087-8.

[3] – Florent Nolot,Les principes de la sécurité, Critères fondamentaux, , Master 2 STIC-Informatique. 2. Université de Reims Champagne – Ardenne

http://www.nolot.eu/Download/Cours/reseaux/m2pro/ARS0809/ArchiResoSecu-Cours1.pdf, P 5.

2. المقدرة على التوسع لسد الحاجات المستقبلية *Scalability* .

3. المرونة *Flexibility* والمتمثلة في توفر الإمكانيات والأدوات التي تمكن من إدارة النظام دون أن يستدعي ذلك إلى توقفه؛ وسهولة الاستخدام[1] *Ease of Use*.

المطلب الثاني : التحديات التي يمثلها الأمن السيبراني وما هي العلاقة بينه وبين الأمن القومي؟

يجلب الارتباط مع شبكة الانترنت تحديات أمنية جديدة لشبكات مؤسسات الدولة والشركات الكبرى [2] ، حيث أنشأت هذه المؤسسات و الشركات مواقع لها على الانترنت، وزودت موظفيها بخدمات البريد الإلكتروني، ومتصفحات انترنت، وأصبح بذلك أمام المستخدم الخارجي المسلح ببعض المعرفة وبعض الأهداف الخبيثة، طريقة جديدة للتسلل إلى الأنظمة الداخلية، حالما يصبح هذا الدخيل داخل شبكة المؤسسة أو الشركة، يمكنه أن يتجول فيها ويخرب أو يغير البيانات، أو يسرقها مسببا أضرارا من مختلف الأنواع، و حتى إذا أخذنا أكثر تطبيقات الانترنت استخداما وهو البريد الالكتروني فانه لا يعتبر مأمونا، يمكن لمن لديه محلل بروتوكولات *protocol analyzer* وإمكانية الوصول إلى الموجهات *routers* والأجهزة الشبكية الأخرى التي تعالج البريد الالكتروني أثناء انتقاله من شبكة إلى شبكة عبر الانترنت أن يقرأ أو يغير الرسالة المرسلة، إذا لم تتخذ خطوات معينة لضمان سلامتها، تتصرف بعض مؤسسات الدولة و الشركات وكأن التحديات الأمنية لم تكن خطرا حقيقيا حيث تتطلع إلى البنية التحتية لشبكة الانترنت، كوسيلة رخيصة نسبيا، لربط شبكتين أو عدة شبكات محلية *LAN* معزولة جغرافيا، مع بعضها البعض أو للربط عن بعد مع شبكة ما .

[1] – المركز العربي للبحوث القانونية والقضائية، ملتقى أمن المعلومات، متوفر على الرابط التالي :
http://www.shatharat.net

[2] -S. Ghernauti-Helie: "From the Digital Divide to the lack of digital security, the challenges of development and deployment of a unified computer-security framework in a multi-dimensional" in international cooperation and the information society context, Section Swiss policy manual mode, the University Institute for Development Studies Publications (IUED). Geneva, November 2003.o see the International Telecommunication Union, cyber security handbook for developing countries, edition 2007, ITU 2009, p. 21.

وتجدر الإشارة إلى أن أعمال التجارية على شبكة الانترنت، والتي تتطلب الملايين من التبادلات المصرفية السرية، أصبحت قريبة من متناول الكثيرين، وتستجيب أسواق أمن الشبكات*Network Security* بسرعة لتحديات أمن شبكة الانترنت عن طريق تبني تقنيات التحقق *Authentication* والتشفير*Encryption* المتوفرة في هذا المجال لتطبيقها على روابط شبكة الانترنت، وعن طريق تطوير منتجات جديدة في مجال أمن المعلومات.

الفرع الأول : التحديات التي يمثلها الأمن السيبراني

إن التحديات التي ينطوي عليها الأمن الرقمي مُعَقدة، ويحتاج التصدي لها إلى ضرورة توافر الإرادة السياسية اللازمة لتصميم وتنفيذ إستراتيجية لتطوير بني تحتية وخدمات رقمية تشمل إستراتيجية للأمن السيبراني تكون متماسكة، وفعالة، وقابلة للتحقق منها ومن إدارتها. ويجب أن تكون إستراتيجية الأمن السيبراني جزءاً من نهج متعدد التخصصات، مع وجود حلول جاهزة على المستويات التثقيفي، والقانوني، والإداري والتقني. ويمكن للاستجابة القوية للأبعاد البشرية والقانونية والاقتصادية لاحتياجات أمن البنية الأساسية الرقمية أن تبنى الثقة، وأن تُولِد النمو الاقتصادي المرغوب فيه، والذي يفيد المجتمع كافة.

إن تملك زمام رصيد المعلومات الرقمية، وتوزيع السلع غير الملموسة، وإضافة القيمة إلى المحتوى، وسد الثُغرة الرقمية كلها مشاكل ذات طبيعة اقتصادية واجتماعية، تستلزم شيئاً أكثر من مجرد إتباع نهج وحيد البُعد وتكنولوجي بحت تجاه الأمن السيبراني[1].

الفرع الثاني : السياسات الأمنية للشركات و مؤسسات الدولة لحماية بياناتها الرقمية

لن يكون الربط مع شبكة الانترنت مثل الربط مع أي نوع آخر من الشبكات آمنا تماما، وبدلا من أن تلجأ الشركات إلى تحقيق الأمن المطلق، عليها أن تعرف خطر تسرب المعلومات، وتحقق نوعا من التوازن بين احتمالات خرق الترتيبات الأمنية وبين كلفة تحقيق مختلف هذه الترتيبات.[2]

[1]- H Allen, Julia , The CERT Guide to System and Network Security Practices, Boston, MA, Addison, Wesley.2001.

[2]– وليد أبو سعد، امن المعلومات، الموسوعة العربية للكمبيوتر، قسم الدورات التعليمية الإلكترونية، 2005،ص ص 5-6.

يجب أن تركز الخطوة الأولى علي استنباط سياسة أمنية شاملة للشركة، أو على تطوير السياسة الأمنية المتعبة بحيث تأخذ في الاعتبار الربط مع الانترنت ويجب أن تحدد هذه السياسة بالتفصيل، الموظفين الذين يحق لهم الوصول إلى كل نوع من أنواع الخدمة التي تقدمها الانترنت، كما يجب أن تثقف الموظفين في مجال مسئولياتهم تجاه حماية معلومات الشركة، مثل مسؤولياتهم تجاه حماية كلمات المرور التي يستخدمونها

بالإضافة، إلى تحديد الإجراءات التي ستقوم الشركة بها في حال حدوث خرق لمثل هذه الخطة الأمنية، وتعتبر هذه السياسة أداة هامة جدا في تحديد المجالات التي ستنفق فيها أموال الشركة للحفاظ علي أمن معلوماتها، ويقدم كتاب *Site Security handbook*[1] دليل امن المواقع الذي أصدره مجموعة *Network Working Group* التابعة لهيئة *Internet* [2] *Engineering task force* أو *IETF* فكرة جيدة عن الموضوعات التي يجب أخذها بعين الاعتبار عند وضع سياسات أمنية.

تتطلب السياسة الأمنية كجزء من ترتيباتها تقدير الكلفة التي ستتحملها الشركة، في حال خرق الترتيبات الأمنية، ويجب أن ينخرط الموظفون علي أعلى المستويات في هذه العملية وقد يكون من المفيد أن تقوم الشركة بتوظيف مستشار لأمن الكمبيوتر، لضمان أمن معلوماتها، وتقدم الكثير من الشركات المزودة لخدمة الانترنت، الاستشارة والنصح في هذا المجال وتبدأ بعد تحديد السياسة المتبعة، عملية تقويم استخدام برامج الجدران النارية

[1] – This handbook is a guide to developing computer security policies and procedures for sites that have systems on the Internet. The purpose of this handbook is to provide practical ,guidance to administrators trying to secure their information and services. The subjects ,covered include policy content and formation, a broad range of technical system and network security topics, and security incident response. https://www.ietf.org.

[2] - L'Internet Engineering Task Force, abrégée IETF, littéralement traduit de l'anglais en « Détachement d'ingénierie d'Internet » est un groupe informel, international, ouvert à tout individu, qui participe à l'élaboration de standards Internet. L'IETF produit la plupart des nouveaux standards d'Internet.

Barbara Y. Fraser, Network Working Group, Site Security Handbook, SEI/CMU, September 1997 Software Engineering Institute, Carnegie Mellon University,5000 Forbes Avenue, Pittsburgh, PA 15213 , Email : byf@cert.org.

*encryption*والتشفير، *firewall* والتثبت من المستخدم *Authentication*. بعض الأمثلة على السياسات الأمنية:

1. مسح كلمة السر الخاصة بالموظف المنتهية عقدة فورا مثلا كإجراء خلال سحب أوراقه من الشركة.

استخدام الجهاز الخاص بالشركة للأنترنت، ويمنع استخدام جهاز غيره مثلا كأن يحضر *laptop*

لا يسمح بتبادل الرسائل داخل الشركة التي تحتوي على رسائل خاصة أو *malicious gossip*

2. صلاحيات كل مستخدم على البيانات الموجودة على قاعدة البيانات .

3. الدخول للشركة عن طريق البطاقة الخاصة.

4. وضع مثلا أجهزة التحقق من بصمة الشخص على أجهزة البيانات المهمة.

و فيما يلي سنحاول الالمام قدر الامكان بالتهديدات الالكترونية في الفلك الرقمي و الحماية القانونية منها، في مبحثين نبحث في أولهما الأهداف التي تكون محلا للتهديد الالكتروني ؟و من ثمة سنلج الى جرائم تقنية المعلومات في ثاني المبحثين.

الفصل الثاني:

التهديدات الإلكترونية في الفلك الرقمي و الحماية القانونية منها.

يجب ادراك أنه ليس هناك أمن مطلق للكمبيوتر، طالما أن هناك كمبيوتر مستخدم، وأن المخاطر تتدرج من المخاطر التقليدية كأي مال منقول إلى مخاطر خاصة بطبيعة عمل الجهاز ووظائفه وتنتهي بأن يكون هذا الجهاز مصدر تهديد للآخرين، كما علينا أن ندرك أيضاً أننا كل يوم أمام جديد من التقنيات والبرمجيات والبروتوكولات التي قد تستغل في أعمال غير مشروعة، وعليه فان تصنيف وتحديد المخاطر يتباين بحسب النظرية والمعايير المختلفة ولكنها لا تختلف في جملتها عن بعضها، وفي هذا الفصل سيتم تحديد الاهداف التي تكون محلا للتهديد الالكتروني[1](المبحث الأول).

و لا جرم أن الجرائم المعلوماتية[2](المبحث الثاني) تشكّل تهديداً وتحدياً خطيراً للأمن الوطني والدولي باعتبارها الظاهرة الإجرامية المتصاعدة في ظل ثورة المعلومات الحاسوبية، وافتقار كثير من دول العالم لقوانين خاصة لمواجهة هذه الجرائم المدمرة في الفضاء الإلكتروني الرحب، مع وجود عصابات منظمة تطور نفسها باستمرار لتحقيق أهدافها التخريبية لاقتصاديات الدول واختراق نظم الحماية والمواقع، فضلاً عن أعمال التجسس والتصنت والتطفّل، أو قصد الاحتيال وسرقة أرصدة البنوك وعملائها باختراق شبكات البنوك والمؤسسات المالية الضخمة، وبخاصة في ظل التوسُّع في التجارة الإلكترونية. وأصبح بإمكان الجماعات الإرهابية المدرّبة استغلال شبكة المعلومات الدولية في دعم أنشطتها الإرهابية ونشر أفكارها الهدّامة، أو التجسّس على العمليات الأمنية والمؤسسات العسكرية والصناعية والتجارية الكبرى وسرقة أسرارها. وهناك من جرائم

---

[1]- يونس عرب، جرائم الحاسوب والانترنت، إتحاد المصارف العربية ، ط1، 2002،ص 87 .

[2]- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، مجلة الحقوق للبحوث القانونية والاقتصادية، كلية الحقوق، جامعة الإسكندرية، العدد 24، 1992، ص 172. وكذلك هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقا عليها)، دار النهضة العربية، ط1،القاهرة، 2007، ص47 وما بعدها. و كذلك عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، بدون ناشر، طبعة مزيدة ومنقحة، 2009، ص114، هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات ،مكتبة الآلات الكاتبة، أسيوط، مصر، 1995 ، ص 34.

المعلوماتية ما تقوم به (مافيا) تجّار المخدرات والأسلحة والاتجار في البشر، وبيع الأعضاء وتهريب المهاجرين، وجرائم غسيل الأموال، وجرائم الآداب العامة والمواقع الإباحية، وجرائم السب والقذف والتشهير والابتزاز والتلصّص، وإنشاء مواقع لنشر الأفكار الهدّامة وازدراء الأديان، وجرائم تدمير قواعد البيانات والمعلومات وإطلاق الفيروسات[1]، وجرائم أخرى عديدة نظراً للتطوّر المذهل في عالم الاتصالات والمعلومات، وهذا مما دفع المعينين بأمر البيئة المعلوماتية إلى ضرورة تحقيق كافة عناصر الأمن لها، بأن تقوم الدولة بفرض الرقابة لمنع الدخول إلى بعض المواقع غير الأخلاقية، وإنشاء برامج على الحاسب الآلي تحت اسم (شرطة الإنترنت) يكون هدفها حجب المواقع الإباحية، أو أية مواقع أخرى لا تتناسب مع أخلاقيات المجتمع على نحو ما يجري في الولايات المتحدة الأمريكية والصين وبعض دول أوروبا، كما تزايدت الأصوات التي تنادي بفكرة إنشاء خط ساخن للإبلاغ عن اكتشاف أية حالات للإعلان عبر الإنترنت عن الفجور، أو ممارسة البغاء، أو الاستعمال غير الأخلاقي للأطفال، ووضع نظام قانوني خاص للإنترنت والمعلوماتية وتدريسه في كليات القانون، فضلاً عن العمل على تشجيع البحوث والدراسات المتخصصة حول التعامل القانوني مع هذه الظاهرة.

[1] - Y .Padova , Un aperçu de la lutte contre la cybercriminalité en France, R.S.C. 2002, P. 765, C. Meunier , La loi du 28 nov. 2000 relative a la crime nalite informatique. Rev. dr. pen. Crim. 2002. p.611.

المبحث الأول : ما هي الأهداف التي تكون محلا للتهديد الالكتروني ؟

تعد برامج الحاسوب و قواعد البيانات أحد أركان التطور التكنولوجي الذي نعيشه اليوم والذي نعتمد عليه بتسهيل وتيسير أمور حياتنا اليومية، فسواء كانت تلك البرامج مكتوبة بلغة الآلة أو المصدر، فإن جميعها سخرت لأجل خدمتنا، فمن جهاز الحاسوب إلى الهاتف النقال إلى السيارة إلى مكوك الفضاء، كلها تحتاج إلى برامج لتضمن عملها وتحقق الغاية التي صُنعت تلك الآلات من أجلها.

إن تلك البرامج وما تحتوي عليه من أفكار ووظائف كان لها كبير الأثر بتغيير حياتنا وتسهيلها، الامر الذي يدفع بنا بالتفكير بالشخص أو الأشخاص الذين كانوا وراء تطوير مثل تلك البرامج من كونها فكرة، إلى نموذج، إلى برنامج نتفاعل معه ويحقق مطالبنا التي نسعى للحصول عليها، ويدفعنا بالتفكير بالجهد الذي بذلوه وراء ذلك، والحقوق التي تتعلق بذلك الجهد، فمن صاحب الحق بالحماية بظل قانون حق المؤلف، هل هو صاحب الفكرة، أم الشخص الذي أعد تلك الفكرة على شكل نماذج وتصميمات، أم الشخص الذي كتب البرنامج بلغة الآلة، أم أنه ذلك الشخص الذي قام بوضع خطط لتجريب النموذج الأولي للبرنامج، أم أن هؤلاء لا قيمة لأعمالهم إذا تمت تحت إشراف الشخص المعنوي، وأن الشخص المعنوي الذي اشرف ووجه لكتابة ذلك البرنامج هو صاحب الحق الأولى بالرعاية وهو المؤلف بحسب القانون، وما هو مضمون الحماية المقررة لهم.

المطلب الأول : المصنفات الرقمية .

إن علم الحوسبة برمته قام على العددين (صفر وواحد)،[1] وان البرمجيات هي ترتيب لأوامر تتحول إلى أرقام تبادلية، وان نقل البيانات، رموزا أو كتابة أو أصواتا عبر وسائل الاتصال انتقل

[1] – يقصد بالتصنيف لغة، تمييز الأشياء بعضها عن بعض، وصنف الشيء أي ميز بعضه عن بعض، مكرم ابن منظور الإفريقي المصري، لسان العرب، دار إحياء التراث العربي، بيروت، المجلد11، بدون سنة النشر ،ص100.

كما عرف المشرع الجزائري المصنف أو المؤلف في المادة الأولى من الأمر رقم 73-14 المؤرخ في 29صفر 1393هـ الموافق ل 03 أفريل 1973 ،ج.ر.ر.29، المتعلق بحق المؤلف بأنه: "كل إنتاج فكري مهما كان نوعه و نمطه و صور تعبيره، و مهما كانت قيمته و مقصده و أن يخول لصاحبه حقا يسمى حق المؤلف يجري تحديده و حمايته طبقا لأحكام هذا الأمر".

من الوسائل الإلكترومغناطيسية والتناظرية إلى الوسائل الرقمية، وان الصورة وكذا الصوت والموسيقى والنص في احدث تطور لوسائل إنشائها وتبادلها أصبحت رقمية على نحو ما أوضحنا في القسم الأول من هذا الكتاب، وحتى عنوان الموقع على الانترنت وكذا العنوان البريدي الالكتروني، تتحول من العبارات المكتوبة بالأحرف إلى أرقام تمثل هذه المواقع وتتعامل معها الشبكة بهذا الوصف، وصحيح انه لما يزل هناك تبادل تناظري لا رقمي، فالقارئ الآلي في نظام الكمبيوتر يدخل الرسم وحتى الوثيقة على شكل صورة وليس على شكل نص، وصحيح أن العديد من المواقع على الانترنت واغلبها العربية ومواقع اللغات غير الانجليزية لما تزل تستخدم الوسائل التناظرية في تثبيت المواد على الموقع وليس الوسائل الرقمية، .لكن الموقع نفسه، وعبر مكوناته، يتحول شيئا فشيئا نحو التبادل الرقمي لما يحققه من سرعة وجودة وأداء فاعل قياسا بالوسائل غير الرقمية .

ومن الوجهة القانونية، تعاملت النظم القانونية والدراسات القانونية والقواعد التشريعية مع مصنفات المعلوماتية بوصفها تنتمي إلى بيئة الكمبيوتر، وهو اتجاه تعبر عنه دراسات فرع قانون الكمبيوتر في النظم المقارنة ، وقد شملت هذه المصنفات ابتداء من منتصف أوائل السبعينات وحتى وقتنا الحاضر ثلاثة أنواع من المصنفات :

البرمجيات [1]، وقواعد البيانات وطبوغرافيا الدوائر المتكاملة، وهي مصنفات جاءت وليدة علوم الحوسبة مستقلة عن علوم الاتصال وتبادل المعطيات وشبكات المعلومات، ومع ظهور شبكات المعلومات، والتي ارتبطت في الذهنية العامة بشبكة الانترنت كمعبر عنها وعن التفاعل

والدمج بين وسائل الحوسبة والاتصال، ظهرت أنماط جديدة من المصنفات أو عناصر مصنفات تثير مسألة الحاجة إلى الحماية القانونية وهي :

[1]– قد أصبحت هندسة البرمجيات أحد تخصصات علم الكمبيوتر القريبة من العلوم الاجتماعية لا العلوم الهندسية، لمزيد من التفاصيل أنظر محمد محمد الهادي، اقتصاديات هندسة البرمجيات، *cybrarians journal*العدد 14، سبتمبر 2007 متوفرة على الرابط التالي: http://www.journal.cybrarians.info

أسماء النطاقات أو الميادين أو المواقع على الشبكة *Domain Names* ، وعناوين البريد الالكتروني، وقواعد البيانات على الخط التي تضمها مواقع الانترنت، تحديدا ما يتعلق بالدخول إليها واسترجاع البيانات منها والتبادل المتعلق بمحتواها الحاصل على الخط، وهو تطور لمفهوم قواعد البيانات السائدة قبل انتشار الشبكات التي كان مفهوما أنها مخزنة داخل النظام أو تنقل على واسطة مادية تحتويها، ومادة أو محتوى موقع الانترنت من نصوص ورسوم وأصوات ومؤثرات حركية (يطلق على المؤثرات الصوتية والحركية لوسائط المتعددة *MultiMedia*)

- ويمكن القول أن المصنف الرقمي يشمل كافة المصنفات المتقدمة، فبرنامج الكمبيوتر من حيث البناء والأداء مصنف رقمي، وقاعدة البيانات من حيث آلية ترتيبها وتبويبها والأوامر التي تتحكم بذلك تنتمي إلى البيئة الرقمية، وذات القول يرد بالنسبة لكافة العناصر المتقدمة، وبالتالي نرى أن أي مصنف إبداعي عقلي ينتمي إلى بيئة تقنية المعلومات يعد مصنفا رقميا وفق المفهوم المتطور للأداء التقني وفق اتجاهات تطور التقنية في المستقبل القريب، وهذا لا يؤثر على انتماء المصنف بذاته إلى فرع أو آخر من فروع الملكية الفكرية، ونقصد هنا أن أسماء النطاقات مثلا ينظر لها كأحد المسائل المتعين إخضاعها لنظام الأسماء والعلامات التجارية بسبب ما أثارته من منازعات جراء تشابهها بالعلامات والأسماء التجارية وتطابقها في حالات عديدة أو لقيامها بذات المهمة تقريبا في البيئة الرقمية، والبرمجيات وقواعد المعلومات حسم الجدل بشأنها بان اعتبرت مصنفات أدبية تحمى بموجب قوانين حق المؤلف – مع وجود اتجاه حديث وتحديدا في أمريكا وأوروبا يعيد طرح نجاعة حمايتها عبر آلية حماية براءات الاختراع – وسيثير محتوى موقع الانترنت جدلا واسعا، فهل تحمى محتوياته كحزمة واحدة ضمن مفهوم قانون حق المؤلف، أم يجري تفصيل هذه العناصر ليسند اسم الموقع إلى الأسماء التجارية وشعار الموقع إلى العلامات التجارية – كعلامة خدمة مثلا – والنصوص والموسيقى والرسوم الى قانون حق المؤلف كمصنفات أدبية ؟[1]

المصنفات الرقمية في بيئة الانترنت : من الوجهة القانونية تثير الانترنت العديد من المشكلات على نحو مستقل عن عالم الحوسبة والاتصالات، وان كانت هذه المشكلات في

[1]– يونس عرب، التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية، ورقة عمل مقدمة أمام الدورة العلمية الخامسة حول دور التوثيق والمعلومات في بناء المجتمع العربي، النادي العربي للمعلومات، سوريا، ص 7.

حقيقتها تمثل جزءا من مشكلات تقنية المعلومات برمتها ومثارة في بيئتها، ويمكن تأطير هذه المشاكل ضمن ثلاث طوائف :

الأولى : مشكلات عقود الانترنت ابتداء من عقود الاشتراك في الخدمة مرورا بالعقود ذات المحتوى التقني، وعقود الجهات ذات العلاقة بمواقع الانترنت او عقود المستخدمين مع المواقع، بما فيها عقود طلب الخدمات والتسوق الالكتروني وعقود الخدمات المدفوعة والمجانية كعقود البريد الالكتروني ورخص استخدام وتنزيل البرامج وعقود ورخص نقل التكنولوجيا وغيرها، من العقود التي تقع في نطاق العقود الالكترونية او العقود المبرمة عبر المراسلات الالكترونية، والجامع المشترك بين هذه العقود والتصرفات المتصلة بالأنترنت انها تتعلق بالتنظيم القانوني للتعامل مع الانترنت وعبرها.

والثانية : مشكلات حماية حقوق المستخدمين والمتعاملين في بيئة الانترنت، وتضم حقوق المستهلك بوجه عام وحماية الحق في الحياة الخاصة وحماية حقوق الملكية الفكرية في بيئة الانترنت.

أما الثالثة: فتتصل بمشكلات امن المعلومات سواء بالنسبة لمواقع الانترنت أو أنظمة المستخدمين.

أما عن الطائفة الأولى فان محل تناولها دراسات الأعمال الإلكترونية والتجارة الإلكترونية والبنوك الإلكترونية، وبالنسبة للطائفة الثانية، فان موضع دراستها يستتبع الفرع محل الدراسة، فدراسة حماية الحياة الخاصة مناطه دراسات حقوق الإنسان وتأثرها بتقنية المعلومات أو الدراسات الجنائية الخاصة بأمن المعلومات محل دراسة الطائفة الثانية المشار إليها، ودراسة حماية المستهلك يكون مناطه الدراسات القانونية في حقل ميادين حماية المستهلك من المخاطر الاقتصادية والصحية والثقافية والاجتماعية وغيرها.

وبالنسبة لحماية حقوق الملكية الفكرية في بيئة الانترنت فان محل تناولها دراسات الملكية الفكرية عموما ودراسات حق المؤلف على وجه الخصوص، أما الطائفة الثالثة فان محل تناولها دراسات امن المعلومات وجرائم الكمبيوتر والانترنت والاتصالات [1].

[1]- يونس عرب ،المرجع السابق ، ص 9 .

والحماية القانونية لحقوق الملكية الفكرية في بيئة الانترنت تثير التساؤل ابتداء بشأن تحديد حقوق الملكية الفكرية في بيئة الانترنت، وتحديد المصنفات محل الحماية، واستقصاء الحماية اللازمة لمواجهة الاعتداءات والمخاطر التي تعترض هذه الحقوق، وتقييم ما اذا كانت القواعد القائمة ضمن تشريعات الملكية الفكرية او غيرها من التشريعات كافية لتوفير الحماية لهذه الحقوق ام ان هناك ثمة حاجة لتشريعات خاصة بالمصنفات محل الحماية في بيئة الانترنت .

الفرع الأول : برمجيات الحاسوب.

تعد برامج الحاسوب أول واهم مصنفات المعلوماتية أو تقنية المعلومات التي حظيت باهتمام كبير من حيث وجوب الاعتراف بها وتوفير الحماية القانونية لها.[1]

والبرمجيات هي الكيان المعنوي لنظام الكمبيوتر دونها لا يكون ثمة أي فائدة للمكونات المادية من الأجهزة والوسائط وهي بوجه عام تنقسم من الزاوية التقنية إلى برمجيات التشغيل، المناط بها إتاحة عمل مكونات النظام معا وتوفير بيئة عمل البرمجيات التطبيقية، وتمثل البرمجيات التطبيقية النوع الثاني من أنواع البرمجيات وهي التي تقوم بمهام محددة كبرمجيات معالجة النصوص أو الجداول الحسابية أو الرسم أو غيرها ، وقد تطور هذا التقسيم للبرمجيات باتجاه إيجاد برمجيات تطبيقية ثابتة وأنواع مخصوصة من البرمجيات تزاوج في مهامها بين التشغيل والتطبيق، أما من ناحية الدراسات والتشريعات القانونية فقد أثير فيها عدد من المفاهيم المتصلة بأنواع البرمجيات.

البند الأول: تعريف برمجيات الحاسوب.

البرامج جمع برنامج، و هو معرب من كلمة "برنامه الفارسية"، و تعني الورقة الجامعة للحساب، و قيل هي النسخة المكتوب فيها عدد الثياب و الأمتعة و أنواعها المبعوث بها لإنسان آخر.

ويستخدم بعض الفقهاء كلمة "البرنامج" بهذا المعنى في مسالة البيع على البرنامج ويقصدون بالبرنامج هنا الدفتر المكتوب فيه صفة ما في الوعاء من الثياب المبيعة .

[1]– محمد فواز مطالقة ،النظام القانوني لعقود إعداد برامج الحاسب الآلي ،دار الثقافة للنشر و التوزيع ،عمان، الأردن،2004،ص 16 و ما بعدها

أما برنامج الحاسب الآلي[1] فهي عبارة عن مجموعة من التعليمات التي قد تعبر عنها بأي لغة أو رمز بحيث يمكن توجيهها بطريقة مباشرة أو غير مباشرة إلى حاسب الآلي، للوصول إلى نتيجة أو غاية معينة و يعرف برنامج الحاسب الآلي (الكمبيوتر) بأنه تعليمات مكتوبة بلغة ما، موجهة إلى جهاز تقني معقد يسمى الحاسب الآلي، بغرض الوصول إلى نتيجة معينة [2].

وبرامج الحاسب الآلي لها أهمية كبيرة في مجال استخدام الحاسبات الآلية، وإليها ترجع الاستخدامات المبتكرة المتميزة للحاسب الآلي في شتى المجالات، فغياب البرنامج يجعل من الحاسب الآلي قطعة من الحديد عديمة الفائدة[3] .

ويمكن تعريفه أيضا: بأنه مصطلح عام لمجموعة من الإيعازات التي تسيطر على الحاسوب أو على شبكات الاتصالات، أما البرنامج فهو مجموعة من الإيعازات التي توجه الحاسوب لإنجاز واجبات محدده ويقدم أو ينتج نتائج محدده[4].

إن البرنامج بالنسبة للحاسوب بمثابة الروح من الجسد، لأن الاستخدامات المبتكرة والمتميزة لهذا الجهاز في شتى مجالات الحياة، لا ترجع إلى عبقرية ذاتية لهذه الآلة، وإنما ترجع إلى عبقرية البرنامج، الذي يضعه المتخصص في هذا المجال، فيجعل جهاز الحاسوب قادراً على تحقيق ما يناط به من أعمال أو مبتكرات، فالبرنامج هو بمثابة حدقة العين الباصرة في الحاسوب، وهو القلب المحرك لكل العطاءات والمستجدات التي ينبض بها هذا الجهاز المتطور.

ويمكن تعريف برامج الحاسوب بأنها :تعليمات مكتوبة بلغة ما[5]، موجهة إلى تقني متطور ومتعدد الاستخدامات، بغرض الوصول إلى نتيجة محددة أو استخلاص معلومة معينة[1].

---

[1] – يعرف الحاسب الآلي بأنه " مجموعة من الأجهزة التي تعمل متكاملة مع بعضها البعض بهدف تشغيل مجموعة البيانات الداخلة طبقا لبرنامج تم وضعه مسبقا للحصول على نتائج معينة، هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة ، 1992 ، ص6 .

[2]– محمد حسام لطفي، الحماية القانونية لبرامج الحاسب الالكتروني ،دار الثقافة، القاهرة ص302 و ما بعدها .

[3]– حسن عماد مكاوي، تكنولوجيا الاتصالات الحديثة في عصر المعلومات، الدار المصرية،القاهرة،ط1،ص 70.

4 -James A. Senn, Information Technology in Business, Prentice Hall., 1995, p60.

[5] - لقد تطورت هذه اللغات ومرت بأربعة مراحل خلال القرن الأخير نجملها على النحو التالي:

1. جيل اللغات الأول: وهي لغات الماكنة، وهي لغات مكتوبة بدلالة الرموز الثنائية فقط (0،1)، والإيعازات بهذه اللغة مكونة من جزئيين، شفرة العملية :والتي تتعلق بمجموعة إيعازات الحاسوب الأساسية، فهي تحدد ماهية العملية التي يجب أدائها، وعنوان العملية: الذي يحدد الموقع الذي يحتوي البيانات التي تجري العملية عليها

البند الثاني: أنواع البرمجيات.

من ناحية الدراسات والتشريعات القانونية فقد أثير فيها عدد من المفاهيم المتصلة بأنواع البرمجيات، أبرزها برمجيات المصدر وبرمجيات الالة والخوارزميات ولغات البرمجة وبرامج الترجمة، ونعرض فيما يلي بإيجاز لهذه المفاهيم[2]:

1. برنامج المصدر: هي الأوامر التي يضعها المبرمج أو مؤلف البرنامج وتكون مدركة له، لكنها غير مدركة للآلة التي هي الكمبيوتر كجهاز مادي (وحدة المعالجة تحديدا)، ويستخدم في تأليفها او وضعها لغات البرمجة، التي شهدت تطورا مذهلا عبر السنوات الخمسين المنصرمة، هذه اللغات التي تختلف من حيث سهولتها وتعقيدها ومن حيث فعاليتها في انجاز البرنامج للغرض المخصص له .

2. برنامج الآلة: وهو عكس مفهوم برنامج المصدر تماما، إذ تدركه الآلة وتستطيع التعامل معه وتشغيله، وبين برنامجي المصدر والآلة توجد برامج ذات غرض تحويلي أو (برامج ترجمة) بموجبها تتحول برامج المصدر إلى برامج آلة .

3. الخوارزميات: العناصر والرموز الرياضية التي يتكون منها بناء البرنامج وهي كالأفكار والحقائق العلمية، ليست محل حماية لأنها ليست موضعا للاستئثار (مادة 9 من اتفاقية تربس)[3]

---

2. جيل اللغات الثاني: لغات التجميع، والتي ظهرت بأواخر الأربعينيات من القرن الماضي وتتميز عن لغة الماكنة بأنها سمحت للمبرمجين باستخدام المختصرات الحرفية (مثل A تعبيرا عن (ADD بدلاً من الرموز الثنائية، وأيضاً استخدام رقع رمزية بدلاً من العناوين الفعلية للذاكرة الأولية كمراجع للإيعازات ومواقع البيانات

3. الجيل الثالث: لغات المستوى العالي وتتعدى 1000 لغة حالياً، حيث أن هذه اللغات تسمح بكتابة البرنامج بشكل مركز بإيعازات أقل، ولا تستدعي أن يكون المبرمج ملماً بالعمليات الداخلية للحاسوب، وتعتبر مستقلة نسبياً عن الماكنة وتعمل بأسلوب عمل الإنسان وليس الحاسوب.

4. الجيل الرابع: وهي اللغات عالية المستوى جداً، اللغات الغير إجرائية وهي اللغات التي يقوم المبرمج بوصف المخرجات المطلوبة وتقوم اللغة بنفسها بتطوير الإجراءات على خلاف اللغات السابقة حيث كان يتطلب وضع أسلوب العمل وإجراءاته، أنظر عماد عبد الوهاب الصباغ، كتاب نظم المعلومات ماهيتها ومكوناتها، دار الثقافة للنشر والتوزيع، الأردن، طبعة 2004 ، ص82.

[1]- مصطفى محمد عرجاوي، الحماية المدنية لبرامج الكمبيوتر في القوانين الوضعية، من بحوث مؤتمر القانون والكمبيوتر والانترنت المُنعقد للفترة من 1-3/مايـــو/2000، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، المجلد الثاني، ط3، 2004م، ص ص. 368-367 .

[2]- فايز عبد الله الشهري ، الانترنت وتحديات الأمن القومي : http://www.kkmaq.gov.sa

3 -Article 9 : 1. Members shall comply with Articles 1 through 21 of the Berne Convention (1971) and the Appendix thereto. However, Members shall not have rights or obligations under this Agreement in respect of the rights conferred under Article 6*bis* of that

لكنها متى ما نظمت على شكل أوامر ابتكاريه لتحقيق غرض معين أصبحنا أمام برنامج، وهو بهذا الوصف إن توفرت له عناصر الجدة والابتكار والأصالة محل للحماية شانه شان أي من مصنفات الملكية الفكرية الأدبية الأخرى .

وقد أثارت برامج الحاسوب جدلا واسعا في مطلع السبعينات بشان طبيعتها وموضع حمايتها من بين تشريعات الملكية الفكرية، وترددت الآراء بين من يدعو لحمايتها عبر نظام براءات الاختراع لما تنطوي عليه من سمة الاستغلال الصناعي واتصالها العضوي بمنتج مادي صناعي، وبين من ذهب إلى حمايتها عبر نظام الأسرار التجارية إذ تنطوي في الغالب على سر تجاري يتجلى بالأفكار التي أنبنى عليها أو الغرض من ابتكارها، وبين داع إلى حمايتها عن طريق الشروط العقدية التي تجد مكانها في رخص الاستخدام أو اتفاقيات الاستغلال، لكن كافة هذه الآراء لم تصمد أمام الرأي الذي وجد في البرمجيات عملا ابتكارا أدبيا، يضعها ضمن نطاق مصنفات الملكية الأدبية (حق المؤلف) إذ هي أفكار وترتيب لخوارزميات تفرغ ضمن شكل ابتكاري إبداعي، وسماتها وصفاتها المميزة تتقابل مع عناصر الحماية لمصنفات الملكية الأدبية، وبالرغم من استمرار وجود نظم قانونية توفر الحماية للبرمجيات عبر واحد أو أكثر من الآليات المتقدم الإشارة إليها إلا إن الاتجاه التشريعي الغالب اعتبرها أعمالا أدبية وحماها بموجب تشريعات حق المؤلف سيما بعد أن وضعت منظمة الوايبو [1]القانون النموذجي او الإرشادي عام 1978 بشأن حماية البرمجيات وبعد سلسلة اجتماعات خبراء الوايبو ومنظمة اليونسكو عامي 1983 و1985 التي أسفرت عن توجه عام لاعتبارها من قبيل الأعمال الأدبية، كما أن اتفاقية تربس إذ اعتبرتها

Convention or of the rights derived therefrom. 2. Copyright protection shall extend to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such, The TRIPS Agreement is Annex 1C of the signed in Marrakesh, Morocco on 15 April 1994. The TRIPS :Agreement on Trade Related Aspects of Intellectual Property Rights

[1] – تأسست المنظمة العالمية للملكية الفكرية World Intellectual Property Organization (الويبو) عام 1970 بغرض النهوض بحماية حقوق الملكية الفكرية والانتفاع بها في جميع أنحاء العالم، ويعمل في تلك المنظمة التي تقع في جنيف نحو 700 موظف دولي، وتضم 177 دولة عضواً، أي ما يزيد على 90 بالمائة من بلدان العالم وأصبحت المنظمة إحدى الوكالات المتخصصة للأمم المتحدة عام 1974، وللمزيد عن المنظمة يمكن الرجوع إلى موقعها على الإنترنت http://www.wipo.int/portal/index.html.en

كذلك وإضافتها إلى المصنفات الأدبية والفنية محل الحماية بموجب اتفاقية بيرن[1] (م 1/10) فيكون الاتجاه الدولي قد حسم لصالح هذا الموقف .

ووفقا لاتفاقية تربس فان البرمجيات محل للحماية سواء أكانت بلغة الآلة أم المصدر(م 1/10)[2] ولمؤلفها كافة الحقوق المالية والمعنوية لمصنفات حق المؤلف إضافة إلى حقه في إجازة أو منع تأجيرها – شأنها شأن التسجيلات الصوتية والمرئية (م 11)[3] ، ويستثنى وفق هذه المادة حالة

---

[1] - La Convention de Berne, adoptée en 1886, porte sur la protection des œuvres et des droits des auteurs sur leurs œuvres. Elle offre aux créateurs (auteurs, musiciens, poètes, peintres, etc.) les moyens de contrôler la manière dont leurs œuvres peuvent être utilisées, par qui et sous quelles conditions. Elle repose sur trois principes fondamentaux et contient une série de dispositions définissant le minimum de protection qui doit être accordé, ainsi que des dispositions spéciales pour les pays en développement. Convention de Berne pour la protection des œuvres littéraires et artistiques (modifiée le 28 septembre 1979
http://www.wipo.int/treaties/fr/ip/berne/

– المرسوم الرئاسي رقم 97-341 مؤرخ في 13 سبتمبر 1997 ، يتضمن انضمام الجمهورية الجزائرية الدمقراطية الشعبية، مع التحفظ، إلى اتفاقية برن لحماية المصنفات الأدبية والفنية المؤرخة في 9 سبتمبر 1886 والمتممة بباريس في 4 مايو 1896 والمعدلة ببرلين في 13 نوفمبر 1908والمتممة ببرن في 20 مارس 1914 والمعدلة بروما في 2يونيو 1928 وبروكسل في 26 يونيو 1948 واستوكهولم في 14 يوليو 1967وباريس في 24 يوليو 1967 والمعدلة في 28سبتمبر 1979 ، المنشور بالجريدة الرسمية الجزائرية، والصادر في العدد رقم61 .

[2]- AGREEMENT ON TRADE-RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHT ,Article 10 : Computer Programs and Compilations of Data

1. Computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971).

2. Compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such. Such protection, which shall not extend to the data or material itself, shall be without prejudice to any copyright subsisting in the data or material itself.

3 -AGREEMENT ON TRADE-RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHT

Article 11 : *Rental Rights* "In respect of at least computer programs and cinematographic works, a Member shall provide authors and their successors in title the right to authorize or to prohibit the commercial rental to the public of originals or copies of their copyright works. A Member shall be excepted from this obligation in respect of cinematographic works unless such rental has led to widespread copying of such works which is materially impairing the exclusive right of reproduction conferred in that Member on authors and their

التأجير التي لا يكون فيها البرنامج الموضوع الأساسي للتأجير . وأما بخصوص مدة الحماية فإنها تمتد إلى 50عاما محسوبة على أساس حياة الشخص الطبيعي[1] فان لم تكن كذلك فمن نهاية السنة التي أجيز فيها النشر أو تم فيها إنتاج العمل (م 12 تربس).[2]

الفرع الثاني: البيانات الرقمية

تحظى البيانات الرقمية بأهمية كبيرة،[3]مع تزايد الاعتماد على الأجهزة الإلكترونية في القيام بمهام الحياة اليومية.[4]

---

successors in title. In respect of computer programs, this obligation does not apply to rentals where the program itself is not the essential object of the rental".

[1] – المادتان 12 و 14 اتفاق تريبس (TRIPS)اختصارا لـ (Agreement on Trade Related Aspects of Intellectuel Property Rights) الاتفاقية حول الجوانب التجارية لحقوق الملكية الفكرية أو اتفاق تريبس.

كما نظمت المادة السابعة من اتفاقية برن مدة الحماية بوجه عام على أن تشمل مدة حياة المؤلف و خمسين سنة بعد وفاته , إلا أنها قد أوردت أحكاما خاصة بتحديد بدء هذه المدة بالنسبة للمصنفات السينمائية أو التي تحمل اسم المؤلف أو تحمل اسما مستعارا . أما إذا كان المصنف مشتركا فتحسب المدة المقررة على إثر وفاة آخر من بقي من الشركاء حيا (م 7 ثانيا) هذا و قد نصت م 5/7 على احتساب مدد الحماية المقررة على اعتبار أول يناير من السنة التالية للوفاة أو الواقعة المقررة في الفقرات 2 , 3 , 4 من ذات المادة، كل ذلك مع إتاحة تقرير مدة أطول للحماية في تشريعات الدول الأعضاء. حسن جميعي، الحماية الدولية لحق المؤلف والحقوق المجاورة، ندوة الويبو الوطنية عن الملكية الفكرية للمسؤولين الحكوميين، المنامة،2004،ص7 .

أما بشأن مصنفات التصوير الفوتوغرافي و الفن التطبيقي فقد أوردت المادة (2/7) حداً أدنى للحماية مقداره خمس و عشرين سنة من تاريخ إنجاز المصنف

[2]- agreement on trade –related aspects of intellectual property right.

-Article 12: Term of Protection :

-Whenever the term of protection of a work, other than a photographic work or a work of applied art, is calculated on a basis other than the life of a natural person, such term shall be no less than 50 years from the end of the calendar year of authorized publication, or, failing such authorized publication within 50 years from the making of the work, 50 years from the end of the calendar year of making.

[3]– محمد السعيد خشبة ،نظم المعلومات، المفاهيم والتكنولوجيا، القاهرة، جامعة الأزهر ،1987 ، ص 117

[4]– علي كمال شاكر، نظم إدارة قواعد البيانات لأخصائي المكتبات والمعلومات، أسس وتطبيقات عملية، ط1، القاهرة، الدار المصرية اللبنانية،2005 ،ص199.

البند الأول: تعريف البيانات الرقمية

إن المشرع الجزائري ذكر قاعدة البيانات من بين المصنفات المحمية، وهذا بموجب أحكام المادة 05 من الأمن 05/03[1]، و نظرا لتطور هذا المصنف فقد ترك المجال للفقه لإضفاء التعريفات المصاحبة لتطوراته المتلاحقة، فقد عرفها : أنها مجموعة من المعلومات التي

تتكون من معطيات ووقائع و غيرها سواء كانت في شكل مطبوع أو مجموعات ذاكرة كمبيوتر أو شكل أخر ...[2]

البند الثاني : آلية جمع البيانات الرقمية

تبدأ عملية تجميع البيانات الخاصة بالمستخدم عند اللحظة التي يقوم بتصفح أحد المواقع الالكترونية بواسطة بعض العناصر التي تحتوي عليها صفحة الإنترنت، مثل بروتوكول الإنترنت(*Internet Protocol*) أو ما(*IP address*)يعرف اختصارا بإسم وهو بروتوكول أو مرسوم بكيفية تبادل المعلومات بين طرفين على شبكة، الإنترنت بحيث لا يتشابه أي عنوان للبروتوكول مع غيره على الإطلاق، فيما يشبه بصمة اليد ولكن بشكل رقمي، وعن طريق تتبع عنوان البروتوكول يتم الوصول إلى البيانات الشخصية للمستخدمين والتعرف أيضًا على موقع الجهاز الذي يقوم بعملية التصفح على الإنترنت، فمثلا إذا كان عنوان للمستخدم (IP) 001.002.003.004)فإن رقم (001) يشير إلى بلد الجهاز المستخدم، ورقم (002) يشير إلى الجهة المنظمة للإنترنت داخل البلد، و003) إلى شركة الإنترنت المشترك معها المستخدم، و (004)إلى رقم المشترك لدى شركة الإنترنت، وبالتالي عند إرسال مجموعة من البيانات أو استقبالها على شبكة الإنترنت يتم تقسيم تلك الرسالة إلى

[1]- الأمر رقم 03-05 مؤرخ في 19 جمادى الأولى عام 1424 الموافق لـــ 19 جويلية 2003والمتعلق بحقوق المؤلف والحقوق المجاورة، والملغي للأمر رقم 97- 10 ، ج.ر.ر13،

[2]- محمد علي فارس الزعبي، الحماية القانونية لقواعد البيانات وفقا لقانون حق المؤلف، منشأة المعارف، مصر،2003،ص 9.

مجموعة من القطع الصغيرة والتي تعرف بإسم" حزم"، يحتوي كل منها على عنوان المرسل والمستقبل[1].

عنصر أخر يتم عن طريقه جمع البيانات الرقمية للمستخدمين على شبكة الإنترنت وهو ملفات تعريف الارتباط (*cookies*) أو الكوكيز ويقصد به الملفات النصية الصغيرة التي ترسلها شبكات الاتصال الخاصة، بالمواقع الذي نقوم بزيارتها وتسمح للموقع بالتعرف على بياناتنا وبيانات الجهاز الرقمية، وعادة ما يتم ضبط تلك الملفات ضبطًا تلقائيًا بحيث تقوم بجمع تلك البيانات دون الحصول على موافقة المستخدم.

وبرغم أن تلك الملفات هي التي تسمح لنفس الموقع بالتعرف عليك في الزيارة التالية له، حيث يقوم بتسجيل اسم الدخول أو تفضيلاتك لتسهيل عملية إعادة التسجيل، إلا أنه من ناحية أخرى، فإن الاحتفاظ بتلك المعلومات والبيانات قد تعرض الحسابات للسرقة وتمثل انتهاكا للخصوصية في حالة ما إذا كان المستخدم لا يرغب في احتفاظ الموقع ببياناته الرقمية ولو بشكل مؤقت، ولتفادي تلك المشكلة، قامت بعض الشركات بتطوير مواقعها الالكترونية بحيث تسمح للمستخدمين بالموافقة أو الرفض على احتفاظ الموقع ببياناتهم أو تخزين ملفات الكوكيز على الجهاز المستخدم.

ثالث تلك العناصر التي تحتويها صفحة الإنترنت وتعمل على جمع المعلومات بشكل تلقائي، هي ما يعرف(*Web Bugs*) باسم" الويب باجز " وهي عناصر غير مرئية تتضمنها صفحات البريد الإلكتروني والمواقع، الإلكترونية .وتعمل على إرسال المعلومات الخاصة بحركة المستخدم على الموقع الإلكتروني كَنسخ أو تحميل الصفحات، كما تمكن من التعرف على توقيت إطلاع المستخدم على بريده الإلكتروني، وما إذا كان قد قام بإرسال البريد لآخرين، أيضًا يتم استخدام تلك العناصر في تحليل صفحات الإنترنت، وقد تتواجد في ملفات

[1]- سارة الشريف، خصوصية البيانات الرقمية، سلسلة أوراق الحق في المعرفة تصدر عن مركز دعم لتقنية المعلومات، القاهرة، ص 3 و ما بعدها .

Chris Reed & colleague, Computer Law, fifth edition, Oxford University Press, New York, 2003, p. 240.

الصور وتحمل أسماء متعددة تختلف طبقًا لمكان وجودها، وهي عادةً عناصر غير ضارة ولا تعد من الفيروسات؛ إلا أن خطورتها تكمن في نوع المعلومات التي تقوم بجمعها، ويمكن توفير بعض الحماية للبيانات الشخصية من تطفل عناصر (*Web Bugs*)عن طريق إغلاق ملفات الكوكيز من متصفح الإنترنت [1].

البند الثالث: أنواع قواعد البيانات

تختلف أنواع قواعد البيانات باختلاف التركيب المنطقي الذي بنيت عليه؛ وذلك بناءً على نوع البيانات وحاجة العمليات اللازمة عليها ونوع الترابط المطلوب، مع الأنواع الأخرى من قواعد البيانات، ويمكن تصنيفها بما يلي:

1. قواعد البيانات الهرمية أو النظم الهرمية:*(Hierarchical DBMS)*

ظهرت النظم الهرمية مع ظهور نظم الحاسوب الكبيرة وهي اقدم نموذج لقواعد البيانات المنطقية وفيها يتم ترتيب سجلات قاعدة البيانات على شكل شجرة لها جذور وعدة فروع، ويمثل سجل الجذر المفتاح الرئيسي *Primary Key*ومن ثم يمكن الوصول إلى مسارات الفروع الأخرى، ولكل فرع أب واحد فقط ولكل أب عدد من الأبناء. ومثال على هذا النوع من النظم ملف العملاء بقاعدة البيانات، فالمفتاح الرئيسي للملف هو العميل والذي يتمثل بكود العميل أو اسمه، وهو بمثابة الجذر أو الأب لسجلات الفروع (الأبناء) والتي يمثلها سجلات الفواتير والتي تمثل بدورها جذراً أو أباً لحقول بيانات المنتجات.

2. نظم إدارة قواعد البيانات الشبكية:*(Network DBMS)*

رغم أن كلمة الشبكة استخدمت كثيرًا في شبكات الحاسب، ومعالجة البيانات، فقد وجد من الأفضل استخدام مسمى قواعد البيانات الصغيرة *(Plex)*رغم أن مسمى قواعد البيانات الشبكية لازال شائع الاستخدام.

- ويتغلب هيكل بيانات التركيب الشبكي على معوقات التكوين الهرمي، الذي لا يسمح للابن أن يكون له أكثر من أب واحد.

[1]- سارة الشريف، المرجع السابق ، ص 5.

- ومثل هذا النوع من قواعد البيانات حل كثيرًا من مشكلات العلاقات، فإذا فرضنا أن هناك أكثر من مورد يورد قطع غيار فإن كل مورد قادر على توريد أكثر من نوعية قطعة غيار، وبالتالي فإن كل قطعة غيار يوردها أكثر من مورد.

3. قاعدة البيانات العلائقية:

هي نموذج تم بناؤه علي نظريات الجبر العلائقي، وتتلخص فكرة النموذج في النظر إلي قاعدة البيانات علي أنها مجموعة من الجداول أو علاقات تسمى(*relations*)، والعلاقة هي عبارة عن مصطلح رياضي، وتمثل جدولاً ذا بعدين(صفوف وأعمدة)، ولا توجد هنالك أهمية لترتيب الصفوف أو الأعمدة؛ حيث تمثل الصفوف مجموعة سجلات الجداول (*records or tuple*)، وتمثل الأعمدة الصفات لهذه الجداول(*attributes*)؛ ويجب أن يكون لكل صفة مجال (*domain*)من القيم التي يمكن أن يحتويها هذا العمود، وترتبط هذه الجداول مع بعضها البعض بواسطة روابط، ويجب أن يكون لكل جدول مفتاح رئيس(*primary key*)؛ لتمييز الصفوف عن بعضها، والنقطة التي تمثل تقاطع الصف مع العمود(الصفة) تمثل قيمة لهذا الصف.[1]

وإجمالا يمكن القول أن قواعد البيانات هي تجميع للبيانات يتوفر فيها عنصر الإبتكار عبر جهد شخصي، يكون مخزنا بواسطة الكمبيوتر، ويمكن استرجاعه من خلاله، والبيانات أو المعلومات المخزنة في الحاسبات بشكل مجرد ليست محل حماية كما بالنسبة للقوانين والأنظمة وقرارات القضاء، والمراد بحماية قواعد البيانات – بوجه عام – هو الإبتكار كما تعبر عنه الاتفاقيات الدولية هذا الحقل، فتنص المادة رقم 2/10 من اتفاقية تريبس *TRIPS*على أن "تتمع بالحماية البيانات المجمعة، أو المواد الأخرى سواء كانت في شكل مقروء آلياً، أو أي شكل أخر إذا كانت تشكل خلقاً فكرياً نتيجة انتفاع وترتيب محتواها" – كما نصت المادة 5 من الاتفاقية العالمية للملكية الفكرية لسنة 1996 على أنه "تتمتع مجموعات البيانات، او المواد الأخرى بصفتها هذه أياً كان شكلها إذا كانت ابتكارات فكرية بسبب محتواها، أو ترتيبها لذا يفهم من خلال ذلك أن البيانات أو المعلومات المخزنة في نظم الكمبيوتر ليست محل حماية، كما

[1] – عباس عوض، قـــــــواعد البيانات، http://www.wasael.org

بالنسبة للقوانين والأنظمة وقرارات القضاء، لكنها متى ما أفرغت ضمن قاعدة بيانات وفق تصنيف معين وبآلية استرجاع معينة، وعندما تخضع لعملية معالجة تتيح ذلك، فإنها تتحول من مجرد بيانات إلى قاعدة معطيات، ينطوي انجازها بهذا الوصف على جهد ابتكاري وإبداعي يتحتم الحماية، وكان الاعتراف لقواعد البيانات بالحماية لم يتأت وليداً إلا من خلال جهد لمنظمة الويبو *WIPO* ولمجلس أوروبا الذي وضع عام 1996 قواعد إرشادية وقرارا يقضي على حماية قواعد البيانات ضمن حقوق المؤلف[1].

الفرع الثالث: منظومة الأجهزة الإلكترونية و ملحقاتها

إن أجهزة الحواسيب تتطور بشكل هائل بالمقابل هناك تطور في مجال السبل المستخدمة لإختراقها، مما يتطلب تطوير المهارات للعاملين في أقسام المعلومات لكي يستطيعوا مواجهة حالات التلاعب و العبث المقصود في الأجهزة أو غير المقصود [2].

كما يجب أن تعطى أهمية للمواقع و الأبنية التي يحوي أجهزة الحواسيب و ملحقاتها، و حسب طبيعة المنظومات و التطبيقات المستخدمة يتم إتخاذ الإجراءات الإحترازية لحماية الموقع، و تحصينه من أي تخريب أو سطو و حمايته من الحريق أو تسرب المياه و الفيضانات، و محاولة إدامة مصدر القدرة الكهربائية و انتظامها و تحديد أساليب و إجراءات التفتيش و التحقق من هوية الأفراد الداخلين و الخارجين من الموقع، و عمل سجل لذلك.[3]

وحتى الآن، لا يزال يعتبر أخطر جهات في المجال الإلكتروني هي الدول، على الرغم من الوفرة المتزايدة للإمكانيات الهجومية في الشبكات الإجرامية والتي قد تستخدم في المستقبل من قبل جهات غير حكومية، مثل الإرهابيين ومنظمات التجسس المتطورة والتخريب في النطاق الإلكتروني لا يزال بحاجة إلى إمكانيات وإصرار وترشيد التكاليف للدول.

---

[1] – أحمد عبد الله مصطفى .حقوق الملكية الفكرية والتأليف في بيئة الإنترنت، دبي، الإمارات العربية المتحدة ، ع 21، ديسمبر 2009 http://journal.cybrarians.info/index

[2] – عبد المجيد ميلاد، نشر الطمأنينة وبناء الثقة في العصر الرقمي، إستراتيجية أمن المعلومات، جريدة الصباح ، مارس 2006 ، ص 4 .

[3] – عبد الله بن عبد العزيز الدهلاوي ،أمن المعلومات في الحاسبات الآلية، مجلة الدفاع، العدد 93 ، 1994م.لمزيد من التفاصيل يرجى مراجعة موقع هيئة الاتصالات وتقنية المعلومات: http://www.citc.gov.sa

وحتى الآن لا يوجد ضرر مادي وإرهاب إلكتروني نشط فعلياً. لكن تكنولوجيا الهجمات الإلكترونية تتطور بشكل واضح من مجرد مصدر إزعاج لتشكل تهديدا خطيراً ضد أمن المعلومات والبنية التحتية الوطنية.

ليس هناك شك أن هناك بعض الدول تستثمر بالفعل أموال طائلة في القدرات الإلكترونية التي يمكن استخدامها لأغراض عسكرية، ويبدو للوهلة الأولى أن سباق التسلح الرقمي يقوم على منطق واضح وحتمي، لأن مجال الحرب الإلكترونية يقدم ميزات عديدة: فهي غير تقليدية وغير مكلفة وجميع المزايا تصب منذ البداية في الجانب الهجومي.

علاوة على ذلك، ليس هناك رادع فاعل في الحرب الإلكترونية لأن تحديد المهاجم عملية صعبة جداً وفيها يكون الالتزام بالقانون الدولي مستحيل تقريباً. وفي ظل هذه الظروف، قد يكون أي شكل من أشكال الرد العسكري مشكلة كبيرة جداً، من الناحية القانونية والسياسية.

كما تتطور قدرات الدفاع الإلكتروني بالقدر نفسه حيث قامت معظم الدول الأوروبية بتعزيز دفاعاتها بشكل كبير في السنوات الأخيرة.

من ناحية أخرى، تتطور قدرات الدفاع الإلكتروني بالقدر نفسه كما قامت معظم الدول الأوروبية، بتعزيز دفاعاتها بشكل كبير في السنوات الأخيرة. والدفاع الإلكتروني الجيد يُسهل التعامل مع هذه التهديدات، لدرجة أن المخاطر الثانوية الباقية تعتبر مقبولة مثل التهديدات التقليدية. [1]

وعن أخطر الهجمات الرقمية على الأجهزة الحكومية و غير الحكومية ما يلي:

في عام 2008، انطلقت واحدة من أخطر الهجمات حتى يومنا هذا ضد أنظمة حواسب الجيش الأمريكي. من خلال وصلة USB بسيطة متصلة بكمبيوتر محمول تابع للجيش في قاعدة عسكرية موجودة في الشرق الأوسط، و لم يتم اكتشاف انتشار برامج التجسس في كلا من الأنظمة السرية والغير سرية. وقد شكل هذا ما يشبه جسر رقمي، تم من خلاله نقل الآلاف ملفات البيانات إلى خوادم خارجية.

1 – http://www.nato.int.

منذ ذلك الحين، أصبح التجسس الإلكتروني يشكل تهديداً دائماً. وقد وقعت حوادث مماثلة في معظم دول الناتو – وأبرز هذه الحوادث – وقعت مؤخراً في الولايات المتحدة. وهذه المرة تم استهداف أكثر من 72 شركة من بينها 22 مكتب حكومي و13 من مقاولي قوات الدفاع.

كشف فيروس ستوكسنت عن المخاطر المحتملة للبرامج الضارة، التي قد تؤثر على أنظمة الكمبيوتر الهامة المستخدمة في إدارة موارد الطاقة.

وقد وقعت عدد من الهجمات الضخمة على مواقع وخوادم حكومية في جورجيا إبان النزاع بين روسيا وجورجيا، مما أعطى مفهوم الحرب الإلكترونية نمط أكثر واقعية. – و لم يكن الهدف من هذه الأعمال تحقيق تدمير مادي حقيقي، لكن هذه الهجمات

أضعفت الحكومة الجورجية في فترة حاسمة من النزاع، كما أنها أثرت على قدرتها على التواصل مع الرأي العام الداخلي والخارجي.

وإن لم تكن هذه التقارير تحمل التهديد الكافي، فإن فيروس ستوكسنت الذي ظهر في عام 2010 شهد قفزة نوعية وكمية في القدرات المدمرة للحرب الإلكترونية، ففي صيف عام 2010، انتشرت أخبار بأن نحو 45000 منظومة سيمنس صناعية حول العالم أصيبت بفيروس حصان طروادة الذي يمكنه التلاعب بعمليات تقنية مهمة خاصة بمحطات الطاقة النووية في إيران. وعلى الرغم من أن تقييم حجم الأضرار لا يزال غير واضح، لكنه أظهر المخاطر المحتملة للبرامج الضارة حيث تؤثر على أنظمة الكمبيوتر الهامة التي تدير إمدادات الطاقة أو شبكات النقل. وللمرة الأولى، كان هذا بمثابة دليل على أن الهجمات الإلكترونية يمكنها أن تسبب أضرار مادية حقيقية وتهدد حياة البشر.

الفرع الرابع : القطاع العام و الخاص

ويكون على رأسها: البنوك والمؤسسات المالية، ومؤسسات المنافع العامة كمؤسسات المياه والكهرباء، ومراكز القيادة والتحكم العسكرية.

البند الأول : الهجمات على الأهداف الاقتصادية

أصبح العالم الاقتصادي والمالي يعتمد على شبكات المعلومات، اعتمادا مطلق في الحصول على المعلومات، والتواصل بين البنوك والهيئات بعضها البعض، مما يجعل هذه الشبكات – بتواصلها وانفتاحها على العالم – هدفا للمتلصصين والمخترقين .وبطبيعة الحال فإن الهيئات المالية والاقتصادية تتأثر بالتوقعات والتكهنات والتشكيك في صحة المعلومات، وبالتالي فإن أي تخريب بسيط قد يحدث في هذه المعلومات قد يؤدي إلى نتائج مدمرة، حيث يؤدي إلى إضعاف الثقة في النظام الاقتصادي لتلك المؤسسات.[1]

وقد بلغت الخسائر نتيجة الخداع على الانترنت عام 2005 حوالي 13.9 مليون دولار أمريكي بزيادة بلغت 5.8 مليون دولار أمريكي مقارنة بعام 2004 كما ذكرت إحدى الدراسات الأمريكية[2].

وقد أظهرت إحصائيات شركات كروت الائتمان العالمية (ماستر كارت وفيزا كارت (أنها خسرت مع نهاية عام 2005 نتيجة الاحتيال حوالي 2.8 مليون دولار عام 2005فقط وبصفة عامة فإن الاحتيال باستخدام كروت الائتمان يكلف الشركات المالكة للكروت والمُصدِرة لها حوالي 500 مليون دولار سنويا[3].

ومن الأمثلة المشهورة على الهجمات الاقتصادية: الهجمات التي تمت عام 1997 وعرفت باسم "نادي الفوضى"، حيث قام بعض المخربون بإنشاء برنامج يعمل عبر شبكة الإنترنت بهدف خداع برنامج كويكن *Quicken* المحاسبي، لكي يقوم بتحويل الأموال من الحساب المصرفي للمستخدمين إلى حسابات أخرى لعملاء وهميين، ثم يقوموا بعد ذلك بسحبها من البنوك أو بتحويلها إلى حسابات وهمية أخرى، بهدف تصعيب مهمة ملاحقاتهم. وهذا مثال

[1]– إن مثل تلك الهجمات كلفت رجال الأعمال والعملاء الأمريكيين حوالي 56.6 مليار دولار أمريكي عام 2005

1 -http://www.idtheftcenter.org

[2] -http://www.fraud.org.

[3] -http://www.spamlaws.com.

على الطرق التي يمكن بها اختراق شبكات المعلومات الاقتصادية واستغلالها بحيث تُحدث آثار مدمرة على المجتمعات اقتصاديا[1].

وفي1 فبراير عام 2001 إخترق متسللون(*World Economic Forum*)وقاموا بسرقة أرقاماً لبطاقات الاعتماد، والأرقام الشخصية للهواتف المحمولة، ومعلومات تتعلق بجوازات السفر وترتيبات السفر لعدد من القادة الحكوميين ورجال الأعمال، وكان من بين الضحايا: بيل جيتس رئيس شركة مايكروسوفت، وسكرتير عام الأمم المتحدة السابق كوفي عنان، ووزيرة الخارجية الأمريكية السابقة مادلين أولبرايت.

وتاكيداً لخطورة جرائم الإنترنت أفاد تقرير برلماني وضعته لجنة العلوم والتكنولوجيا، في مجلس اللوردات البريطاني، بأن شبكة الإنترنت تحولت إلى مرتع للمجرمين، وتنفذ فيها عمليات سرقة الأموال من الحسابات المصرفية، وقد حذر التقرير الحكومات والمؤسسات والشركات المختصة بحتمية التدخل لتنظيم عملها قبل فوات الأوان. حيث أدت الجرائم الإلكترونية إلى الإحساس بأن الإنترنت تحول إلى منطقة شبيهة بـــ "الغرب المتوحش" في الولايات المتحدة الأمريكية في عهودها الأولى، حيث تنعدم سيادة القانون. كما أوضح التقرير أن المصارف العالمية خسرت ملايين من الدولارات بسبب هذا النوع من الجرائم حيث خسرت المصارف البريطانية وحدها عام 2007 أكثر من 67 مليون دولار[2].

البند الثاني : الهجمات على مشروعات البنية الأساسية.

لقد أصبحت الدول المتقدمة تعتمد اعتمادا كليا على شبكات المعلومات الرقمية في إدارة نظم البنية الأساسية (على سبيل المثال نظم الطاقة الكهربائية، والهجمات على هذا النوع من الشبكات له تداعيات خطيرة جدا، ومن الإحصائيات التي لها دلالة على أثر مثل هذا النوع من الهجمات هي إحصائيات الهجمات الأمريكية على العراق خلال حرب الخليج الثانية. حيث أشارت مصادر أمريكية أن ضرب مولدات الطاقة الكهربائية العراقية أدي بشكل غير مباشر إلى موت ما بين 70إلى 90 ألف مواطن عراقي كنتيجة مباشرة لعدم توفر الطاقة الكهربائية.

[1] -http://ar.wikipedia.org.

[2] -http://www.alriyadh.com.

ولذلك فإن شبكات المعلومات المرتبطة بشكل مباشر أو غير مباشر بمثل هذا النوع من الشبكات يعد من الأهداف الأساسية التي قد يستهدفها الهجوم الرقمي أو الإلكتروني.

وبالطبع يوجد الكثير من الأهداف الأخرى المتعلقة بالبنية الأساسية والتي تمكن المهاجمين من إثارة الفوضى في الحياة المدنية، فمثلا شبكات المعلومات الطبية، ففي حالة التلاعب فيها ومهاجمتها واختراقها قد تؤدي إلى كوارث وخسائر فادحة في الأرواح. وهناك الكثير من الحالات في أوروبا وأمريكا حيث تمكن المخترقون من النفاذ إلى سجلات المستشفيات وتسببوا في حقن بعض المرضى بأدوية كانت مميتة بالنسبة لهم ، وقد يصل التأثير الاجتماعي للهجمات على حسابات المستخدمين لشبكات المعلومات إلى حد تحريضهم على الانتحار، ففي إحدى مدن ولاية أوريجن الأمريكية استخدم شابًا عاطلاً عن العمل عمره 26عامًا أحد مواقع المحادثة على شبكة الإنترنت لتنظيم انتحار جماعي فيما يسمى بعيد الحب هذا العام لمن لم يوفق في حياته العاطفية.

البند الثالث : الهجمات على الأهداف العسكرية:

تستهدف هذه النوعية من الهجمات عادة الأهداف العسكرية والمرتبطة بشبكات المعلومات، ويندر هذا النوع من الهجمات حيث يتطلب إلى معرفة عميقة بالهدف وطبيعته، وبالمعلومات التي يجب النفاذ إليها، وهذه المعرفة لا تمتلكها إلا الحكومات، بالإضافة إلى أن الحكومات تقوم عادة بعزل المعلومات العسكرية السرية، ولا تقوم بوصل الأجهزة التي تحملها على الشبكات العامة، ولكن قد يحدث تسريب أو اختراق، ومن هنا لابد من استخدام نظم موثوق منها للتحقق من شخصيات المستخدمين، وتحديد مستويات التخويل الدقيق للمعلومات التي يُسمح بالنفاذ إليها.

ومن أشهر الأمثلة لهذا النوع من الهجمات ما حدث في 12نوفمبر عام 2002 حيث تم اتهام مدير شبكات سابق يدعى "جاري مكينن"، يبلغ من العمر 36 عاما، بتهمة صنفتها السلطات الأمريكية كأكبر عملية تسلل عسكرية عبر التاريخ، حيث قام "مكينن" باختراق ومهاجمة 92 شبكة تديرها وكالة ناسا، ووزارة الدفاع الأمريكية في 14 ولاية أمريكية، وتسبب في خسائر قدرت بـــ900 ألف دولار، وقد اتهم المدعي العام "مكينن" بعده جرائم

منها سرقة كلمات السر، حذف ملفات، تحكم بمرور المعلومات، إغلاق شبكات للمعلومات في قواعد عسكرية بدءاً من ميناء بيل هاربر إلى ولاية كونيكتيكت[1]

وقد تنوعت وتعدّدت الجرائم المرتبطة والمرتكبة بواسطة المعلومات[2]، وكل ما له علاقة بنظمها واستخداماتها، وقد تنوعت أساليب عرضها ومسمياتها من قِبَل الباحثين والكتّاب والمعنيين بالمحافظة عليها وصيانتها من المتخصصين بعلم الحاسب الآلي والبرمجيات المختلفة و تصنف إلى :

الفرع الخامس: تصنيف الاعتداءات الرقمية

تصنّف الاعتداءات في الحقل التقني على النحو التالي:[3]

البند الأول : خرق الحماية المادية *Breach of Physical Security*

ويُقصد بها قيام المهاجم بالبحث في مخلّفات التقنية من القمامة والمواد المتروكة، [4]بحثاً عن أي شيء يساعده على اختراق النظام، كالأدوات المدوّن عليها كلمة السر، أو مخرجات الحاسب، أو الأقراص الصلبة المرمية بعد استبدالها، أو غير ذلك من المواد، أو أن يلجأ المهاجم إلى عملية الالتقاط السلكي، أي التوصّل السلكي المادي مع الشبكة أو مع توصيلات النظام للتصنت والمهاجمة، أو للسرقة والاستيلاء على المعلومات المتبادل عبر الأسلاك، وقد يتم اختراق الحماية المادية عن طريق استراق الأمواج، وهو ما يحدث باستخدام لواقط تقنية لتجميع الموجات المنبعثة من النظم، باختلاف أنواعها، كالتقاط موجات شاشات الكمبيوتر الضوئية، أو التقاط الموجات

---

[1] -http://redda.forumotion.com.

[2]- شهد عام 2014 تطور البرمجيات الخبيثة التي تستهدف العملة الرقمية ''بيتكوين'' Bitcoin، فمع ازدياد شعبية وقيمة العملة الإلكترونية ''بيتكوين''، يعاود مجرمي الانترنت تحديد أهدافهم لسرقة العملة الرقمية من خلال الأنشطة الخبيثة.

ففي أواخر العام 2013، لاحظ الباحثون في شركة ''ديل سونيك وول'' ارتفاعًا في البرمجية الخبيثة من نوع Bitcoin-mining botnets والتي تم تصميمها لسرقة القدرات الحاسوبية الخاصة بالعملة الرقمية، أو دفع تكاليف العمليات الإجرامية رقميًا، هذا ويتوقع الباحثون أن يستمر هذا التوجه خلال العام 2016- 2018 طالما أن قيمة العملة الرقمية مرتفعة.

[3]- فايز عبدالله الشهري، الانترنت وتحديات الأمن القومي http://www.kkmaq.gov.sa . و أنظر،محمد عبدالله الخراشي، أهم التحديات التي تواجه الأمن القومي :

- http://www.kkmaq.gov.sa
- http://www.aawsat.com

[4]- يونس عرب، جرائم الحاسوب والانترنت، إتحاد المصارف العربية،ط2002،،1، ص87.

الصوتية من أجهزة الاتصال. وأخيراً قد يلجأ المهاجم في محاولة اختراق الحماية المادية إلى إنكار أو إلغاء الخدمة، أي الإضرار المادي بالنظام لمنع تقديم الخدمة ويتمثل هذا النوع من الاختراق في الآتي:

1. بحث وتفتيش المخلفات *Media Scavenge*

ويعني بحث المعلومات في مخلفات المؤسسات من القمامة والمواد المتروكة من اقراص صلبة، [1] ووسائط وخلافه من مخلفات الحاسوب وأوراق وكربون، إما لمعرفة أسرار العمل من قبل المنافسين أو للحصول على معلومات، مثل كلمات السر والشفرات وخلافها تساعدهم في الاختراق أو السرقة[2].

2. إستخلاص المعلومات من الموجات الكهروماغنطيسية *Eavesdropping Emanation* ،ويتم ذلك باستخدام أجهزة ووسائل ولواقط تقنية لتجميع الموجات الكهرومغناطيسية، من النظم باختلاف أنواعها، كالتقاط موجات شاشات الحاسوب الضوئية والموجات الصوتية من أجهزة الاتصالات وأجهزة الراديو.

3. الالتقاط السلكي *Wire Tapping* وتحليل الاتصالات *Traffic Analysis* والمقصود به التوصيل السلكي المادي مع الشبكة أو توصيلات النظام، بغرض استراق السمع وسرقة المعلومات المتبادلة عبر الأسلاك، وتنصب فكرة الهجوم بهذه الطريقة على دراسة أداء النظام ومتابعة سير الاتصالات والمعلومات، بحيث يستفاد من سلوك المستخدمين وتحديد نقاط ضعف النظام، والوقت المناسب حتى يتمكن من وضع خطة للاختراق، وتتوقف سهولة الاختراق وصعوبته على نوع الشبكة وطريقة التوصيل المادي لها.

4. إنهاء الخدمة أو عدم توفرها *Denial of Service* والمقصود هنا الإضرار بالنظام، لمنع تقديم الخدمة، ويتم ذلك بوسائل عدة خاصة عبر الانترنت مثل :

---

[1]- محمد خليفة ،الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري، دار الجامعة الجديدة –الازارطة–2008، ص 46.

[2]- وهذا ما حدث مع وزارة العدل الأمريكية عندما بيعت مخلفات أجهزة تقنية بعد أن تقرر تلافها، و كان من ضمنها نظام كمبيوتر، يحتوي قرصه الصلب على كافة العناوين الخاصة ببرامج حماية الشهود، و بالرغم من انه لم يتم استثمارها المعلومات ، إلا أن مخاطر كشف هذه العناوين استدعي إعادة نقل كافة الشهود و تغيير مواطن إقامتهم و هوياتهم و هو ما الحق تكلفة مالية باهظة ... محمد خليفة، المرجع نفسه ،ص 47.

إغراق النظام ***Sink flood*** :وذلك بجعل شبكة المعلومات أو النظام مشغولاً بصورة دائمة، وذلك بإرسال الرسائل البريدية الالكترونية دفعة واحدة، أو إرسال طلبات خدمة وبثها ونشرها بحيث تتم إعادة البث من مختلف الجهات بكميات تفوق إمكانية النظام في التعامل مع الطلبات الواردة اليها، حتى تتوقف الاجهزة المستهدفة عن الاستجابة لانشغالها.

.الإتلاف ***Sabotage*** : وهو إحداث تلف وتخريب النظام في برامجه ونظم تشغيله، وبياناته بغرض الإنتقام أو المنافسة.

خلل في الجهاز : تتكون أجهزة الحاسوب من عناصر إلكترونية وأجهزة ميكانيكية، وتعمل بواسطة نبضات كهربائية، [1] ويجري الإتصال بين وحدات الجهاز بواسطة البث المحكم لهذه النبضات الكهربائية، وتصمم الدائرة الإلكترونية للحاسوب بحيث تتحكم في التوقيت والشكل والقوة وتردد هذه النبضات، وتمتاز الحاسوب بقدرتها على إكتشاف الأخطاء بواسطة أجهزة رقابة مصممة ضمن الحاسوب، أن حدوث أي خلل في أحد العناصر الإلكترونية كالترانزستور يؤدي إلى تغيير في التوقيت أو الشكل أو القوة أو بث النبضات مما يؤدي إلى وقوع الأخطاء، ويرجع سبب مثل هذا الخلل إلى زيادة الحرارة أو الرطوبة أو تذبذب قوة التيار الكهربائي، كما أن معظم الآلات المستخدمة في عمليات الإدخال والإخراج والتخزين تتطلب بعض العمليات الميكانيكية، وهذه العمليات تتم بسرعة فائقة وغالباً ما يحدث الخلل والأخطاء الميكانيكية لوجود خلل في التوقيت أو السرعة أو خلل في وحدة القراءة والكتابة أو لسوء الاستخدام.

كل ما تقدم من أخطاء وخلل ينتج عنها فشل المنشأة في تقديم الخدمة للعملاء وينتج ما يسمى عدم جاهزية وتوفر الخدمة ***Denial of Service*** مما يؤثر سلباً على صورة المنشأة.

[1] – محمد حسن عمر مطابع الفرزدق، المراجعة والرقابة الداخلية على أعمال الحاسبات الإلكترونية، السعودية، 1984م، ص 172.

5. الكوارث الطبيعية: وتتمثل في الحوادث التي لا يمكن التكهن بها أو التحكم بها مهما حرصت المنشآت على ذلك، ومما يزيد من مضاعفات هذه الكوارث عدم جود خطط لدرئها، وتتمثل هذه الكوارث في: [1]

– الحرائق: إن من أكبر المهددات الحرائق إذ أن الحرائق تنتشر بسرعة فائقة مدمرة بذلك الأجهزة والمستندات وما تحتويها من معلومات سواء المخزنة بأجهزة أو بوسائط النسخ الوقائي.

– الأبخرة والغازات : رغم أن خطورتها أقل من الحرائق إلا أنها قد تدخل في مكونات الأجهزة الداخلية مسببة الخلل، وتكمن الخطورة أيضاً في أن مصدر هذه الأبخرة خارجية وليست ناتجة عن غرفة الأجهزة .

– الفيضانات والزلازل : إن مثل هذه الكوارث نادرة الحدوث من جراء الأمطار والسيول، إلا أن عدم اختيار الموقع السليم لغرفة الحاسوب وأرشيفها يرفع من نسبة تأثر الحاسوب من كوارث الفيضانات.

– السرقات : السرقات التي تطال الأجهزة والوسائط والمعلومات في أشكالها المختلفة، سواء كان في شكل تقارير مطبوعة أو أشرطة كمبيوتر واستخدام هذه المعلومات في غير صالح المنشأ.

البند الثاني : خرق الحماية المتعلقة بالأشخاص وشؤون الموظفين

تُعد المخاطر المتصلة بالأشخاص والموظفين، وتحديداً المخاطر الداخلية منها واحدة من مناطق الاهتمام العالمي لدى جهات أمن المعلومات، إذ ثمة فرصة لأن يحقق أشخاص من الداخل ما لا يمكن نظرياً أن يحققه أحد من الخارج، وتظل أيضاً مشكلة صعوبة كشف مثل هؤلاء قائمة، إن لم يكن ثمة نظام أداء وصلاحيات يتيح ذلك، وعموماً ثمة مسميات وطوائف عديدة لهذه المخاطر، أبرزها:

التخفّي بانتحال صلاحية شخص مفوض، واستغلال العلاقات الاجتماعية، أو القيام بأعمال الإزعاج والتحرّش، وربما التهديد والابتزاز، أو في أحيان كثيرة رسائل المزاح على نحو

[1]– عبد الرحمن عبد العزيز الشنيفي، أمن المعلومات وجرائم الحاسب الآلي، السعودية،ط1، 1994، ص 71.

يحدث مضايقة وإزعاج بالغين، وكذلك القيام بقرصنة البرمجيات عن طريق نسخها دون تصريح، أو استغلالها على نحو يخلّ بحقوق المؤلف[1].

وتتم هذه الاختراقات بالوسائل والطرق الآتية:

1- انتهاك الصلاحيات *Authorization Violation* وهو استخدام الصلاحية الممنوحة في غير الغرض المصرح به، ويسمي هذا النوع من الاختراق "المهددات الداخلية"، وغالباً ما تنتج مثل هذه المشاكل من ضعف النظم والإجراءات والتقارير الرقابية، بالمؤسسة وتنشأ من المستويات ذات الصلاحيات، وفي نظام مثل هذا، يصعب إكتشاف المشاكل إلا بعد حين.

2- انتهاك تكامل المعلومات *Information Integrity Violation* ويعني تغيير المعلومات بالتعديل أو التبديل، بالإضافة أو الحذف بطريقة غير مشروعة ومن أشخاص غير مصرح لهم، وينتج ذلك لعدم وجود نظام رقابي متكامل مما يفتح الثغرات أمام المتسللين وضعاف النفوس، لانتهاك سلامة وتكامل المعلومات، وبالتالي يؤدي إلى تزويد العملاء والإدارات بمعلومات غير صحيحة كما أنه في أغلب الأحيان يؤدي إلى تعطيل النظام والخدمات المقدمة للعملاء.

3- الإختلاس والإختطاف اللحظي للمعلومات *Hijacking Session* ويتحقق استغلال النظام من قبل أشخاص غير مصرح لهم، بطريقة غير شرعية وذلك بتحيين القرص واستخدام صلاحيات أشخاص مصرح لهم، بعمليات مثل إجراءات القيود والحركات المالية إذا ما وجدوا الشاشة مفتوحة، واستغلال غفلة الشخص المصرح له وتحين الفرص *Piggyback* والحصول علي المعلومات او باستراق النظر، كما يهدف مثل هذا النوع من الوسائل أيضاً الحصول علي معلومات تساعد في اختراق النظم لاحقاً لتنفيذ نشاط تدميري أو خلافه.

4- الهندسة الاجتماعية *Social Engineering* ويقصد به استغلال العلاقة والوظيفة أو خلافهما للحصول على طريقة لاختراق النظام، كأن يتم الاتصال بالموظف منتحلاً صفة شخص ما، ذي علاقة بالعمل أي بمحاكاة شخص مسؤول *Impersonating*وطلب

[1]- محمد عبدالله الخراشين، أهم التحديات التي تواجه الأمن القومي :

- http://www.kkmaq.gov.sa.
- http://www.aawsat.com.

اسم وكلمة سر المستخدم واستغلال نطاق صلاحية هذا المستخدم و الأسلوب الشخصي في الحصول على معلومة الاختراق سميت بالهندسة الاجتماعية ..[1]

5- .الإزعاج والتحرش *Harassment* : وهي تهديدات يندرج تحتها أشكال عديدة من الاعتداءات والأساليب، ويجمعها توجيه رسائل الإزعاج والتحرش وربما التهديد والابتزاز أو في أحيان كثيرة رسائل المزاح على نحو يحدث مضايقة وإزعاجاً[2].

6- قرصنة البرمجيات *Software Piracy* وتتحقق بنسخ البرامج دون تصريح أو استغلالها على نحو مادي دون تخويل بهذا الاستغلال أو بتقليدها أو محاكاتها والانتفاع المادي منها على نحو يخل بحقوق المؤلف [3].

7- عدم الإقرار بتنفيذ العمليات المالية (*Non Repudiation*) يتمثل هذا الخطر في عدم إقرار الشخص بالعملية التي قام بتنفيذها، كأن ينكر بأنه قام بإجراء حركات مالية في حسابه لدى البنك، أو أن ينكر أنه أصدر أمر شراء عبر شبكة المعلومات خصماً على حسابه أو بطاقة الإئتمان الخاص به.

8- خطأ إدخال البيانات: ويحدث هذا النوع من الخطأ في مجال العمل المصرفي، وخاصة عند إدخال الحركات المالية لحسابات العملاء والقيود المالية المختلفة، ما لم يكن النظام مصمماً بطريقة تضمن الرقابة على المدخلات خاصة أرقام الحسابات، وبذلك يتم إيداع المبالغ والقيود المالية في حسابات عملاء آخرين مما يفقد المنشاة مصداقيتها.

---

[1]- محمد خليفة ،المرجع نفسه ،ص 46، ولمزيد من التفاصيل مراجعة الموقع التالي :

- https://www.isecur1ty.org

[2] -Dia Kayyali and Danny O'Brien , Facing the Challenge of Online Harassment, January 8, 2015, According to studies conducted by the Bureau of Justice Statistics in 2006-2009, the prevalence of stalking and connected harassment of all kinds (including online harassment) in the United States varies by gender, age, income level, and race—with women, the young, the poor, and minority groups such as Native Americans and multi-racial families being more commonly affected. A recent Pew Study of online harassment indicated that women between the ages of 18-24 are targeted for online harassment and stalking at a higher rate than other groups. The Pew survey also notes that in the United States, African-American and Hispanic Internet users report harassment at higher levels (54% and 51%) compared to white users (34%). For more details :https://www.eff.org/deeplinks/2015/01/facing-challenge-online-harassment

[3] -John Dvorak, The Software Piracy Bluff, PC Magazine, May 12, 1992, p. 93.

9- .استغلال بواقي وكسور الإحتسابات *Salamis* : ويحدث هذا النوع من الجرائم دائماً من داخل المنشأة، وهنا يقوم المبرمج بوضع أوامر معينة لمراقبة نتائج العمليات المحاسبية، وجمع جزء من كسور العمليات المالية في حساب ما واستغلالها دون ترك أي آثار.

10- الثورات الشعبية : أن عدم الاستقرار السياسي والاقتصادي، غالباً ما يؤدي إلى الثورات الشعبية مصحوبة بالشغب والإتلاف والدمار مما قد يصيب المنشآت والمؤسسات وبالتالي غرف الحاسوب وأجهزتها ومن ثم فقدان معلومات العملاء.

البند الثالث : خرق الحماية المتصلة بالاتصالات والبيانات:

تعرَّف البرمجيات الضارة على أنها برمجيات مصممة خصيصاً لإلحاق ضرر بنظام أو تعطيله، مهاجمةً الكتمان و/أو السلامة و/أو التيسير. وهي تشمل فيروسات وديدان الحاسوب، وحصان طروادة، والبرمجيات التجسسية، وبرمجيات الإعلانات، ومعظم الجذور الخفية، وغيرها من البرامج الخبيثة[1].

والهجمات من خلال شبكة الإنترنت، هي هجوم يحاول فيه المهاجمون اختراق المواقع الإلكترونية المشروعة، باستخدام نقاط الضعف فيها، مما يؤدي إلى حقن شفرة ضارة في هذه المواقع، فيمكن أن تُستخدم بدورها لإصابة حاسوب المستخدم الزائر لتلك المواقع بالعدوى، وقد تتخذ الشفرة الضارة أشكالاً متعددة:

فيمكن أن تكون وسم *iframe* مخفياً يوجه المستخدم لزيارة موقع الهجوم، أو يمكن أن تكون تطبيقات ضارة مكتوبة بلغة برنامج حاسوبي (مثل البرامج النصية أو صغار التطبيقات).

[1]- الاتحـــاد الدولـــي للاتصـــالات، قطاع تقييس الاتصالات، لجنة الدراسات 17 – التقرير 26،مشروع التوصية الجديدة ITU-T X.1211 (X.eipwa) ،متطلبات القدرات اللازمة لمنع الهجمات من خلال شبكة الإنترنت، فبراير 2014، ص 6 .

ومن الأمثلة النمطية على نقاط الضعف في الهجمات من خلال شبكة الإنترنت، حقن لغة الاستعلام البنيوية (SQL)[1] والطلب المزوَّر العابر للموقع، على النحو الموضح في التذييل الأول.

وفي الآونة الأخيرة، تزايدت الهجمات من خلال شبكة الإنترنت تزايداً كبيراً بسبب تزايد استخدام أجهزة المستخدم النهائي الحاسوبية، والعدد المتزايد للمواقع الإلكترونية المتضمنة لبرمجيات ضارة.

وفي الهجمات من خلال شبكة الإنترنت، قد لا يكون المشرفون على المواقع على علم بأن المواقع قد اختُرقت وحُقنت بشفرات ضارة وأنها تُستخدم لنشر الشفرات الضارة. وعلاوة على ذلك، لا يدرك المستخدمون أن حواسيبهم معرضة للإصابة بشفرات ضارة من المواقع التي زاروها،وإذ يمكن منع بعض الحوادث بتثبيت برمجيات مكافحة الفيروسات، فإن ذلك لا يقدم حلولاً نهائية[2].

و لهذا ينبغي تصميم نظام الحماية من هجوم من خلال شبكة الإنترنت، ليكون متيناًوقادراً على استيعاب مختلف المقاييس وعلى النهوض من العثرات.

---

[1]–لغة الاستعلامات البنيوية أو البنائية، بالإنجليزية Structured Query Language أوSQL لغة قواعد البيانات: هي لغة برمجة غير إجرائيةNon Procedural Language ،هي لغة للتعامل والتحكم مع قواعد البيانات المترابطة من خلال التعامل مع تراكيب البيانات وإجراء عمليات إدخال البيانات والحذف والفرز والبحث والتصفية و التعديل وخلافه،تركيب لغة الاستعلامات البنائية،تبعًا لوظائفها التي تقوم بها إلى ثلاثة أقسام رئيسة هي:

- لغة تعريف البياناتData Definition Language DDL
- لغة معالجة البياناتData Manipulation Language DML
- لغة التحكم بالبياناتData Control Language DCL

http://egy-tech.forumegypt.net/t512-topic

[2]– الاتحـــاد الدولـــــي للاتصـــــالات، نفس المرجع، ص 6 .

1- هجمة البيانات *Data Attack*

ويعني ذلك سرقة وتسريب البيانات والمعلومات، كالبيانات الشخصية للعملاء وأرقام الحسابات وارصدتهم لدى البنوك وذلك بغرض استغلالها وبيعها أو بغرض الابتزاز ويتم ذلك باستخدام وسائل وطرق عديدة متمثلة في الآتي:

- النسخ غير المصرح به للبيانات *Unauthorized Coping of Data*

وهي العملية التي تستتبع عادة الدخول غير المصرح به للنظام، حيث يتم الاستيلاء على البيانات والمعلومات عن طريق النسخ لكافة أنواع البيانات والمعلومات والبرمجيات وخلافها.

- القنوات السرية *Covert Channels*

هي عملياً عبارة عن نقل المعلومات بانتهاك أمن وحماية النظام وتتمثل في اعتداءات التخزين، [1]حيث يخفي المنتهك بيانات أو برمجيات أو معلومات مستولى عليها – كأرقام بطاقات الائتمان – في مواضع معين بالذاكرة أوالقرص الصلب بحيث يتم استخدامها لاحقاً، اما القنوات السرية المتزامنة فتتمثل في برامج النظام بحيث يتم التعامل مع التغير من خلال برامج أخرى وتتعدد أغراض الاخفاء، فقد تكون تمهيداً لهجوم لاحق أو تغطية اقتحامات سابقة أو مجرد تخزين لبيانات غير مشروعة.

– **هجمات البرمجيات*Software Attack*** : يعتبر الهجوم البرمجي احد الأشكال المألوفة لمهددات السرية ويحدث عندما يقوم فرد أو مجموعة من الأفراد بتصميم برمجيات ضارة لإحداث ضرر بنظام معين،ويشار إلى هذه البرمجيات في معظم الأحوال بالـ Malware or *Malicious Code*،وفيها يقوم المهاجم باستخدام برامج معينة في تنفيذ الهجمات – وهي الان

[1] – http://www.answers.com.

متوفرة في مواقع عديدة بالإنترنت، وقد لا تتطلب مهارات عالية –سواء كانت هذه البرامج برامج نقل بيانات أو برامج إتلاف أو برامج للمشاهدة والتحليل.[1]

– المصائد والأبواب الخلفية *Traps and Backdoors*

وهي ثغرة أو منفذ في برنامج ما أو برامج تشغيل النظم، والهدف من ايجاد هذه الثغرات أساساً، هو استخدامها في حالات معينة من قبل المختصين لمعالجة مشاكل النظم، كما ان بعضها تزرع في برمجيات عامة عمدا للاختراق فيما بعد للمواقع، كما حدث مع بعض نظم مايكروسفت وباعترافهم وهي ميزة أو صفة في نظام ما يؤدي سوء استغلالها إلى تجاوز كل السياسات الرقابية الموضوعة علي النظام، وتستغل من قبل مرتكبي جرائم الحاسوب، ومثل هذه الثغرات تشكل تهديداً كبيراً للمؤسسات المالية والبنوك.

أ – الهجمات والتلاعب بنقل معلومات عبر أنفاق النقل *Tunneling Session*

وهي طريقة تقنية مشروعة لنقل المعلومات عبر الشبكات غير المتوافقة، لكنها تصلح طريقة اعتداء عندما تستخدم حزم المعطيات المشروعة لنقل معلومات غير مشروعة.

ج– الهجمات الوقتية *Timing Attack*

هي هجمات تتم بطريقة تقنية معقدة للوصول غير المصرح به إلى البرامج والمعلومات، وتقوم جميعها علي فكرة استغلال وقت تنفيذ الهجمة متزامناً مع فواصل الوقت التي تفصل العمليات المرتبة والمجدولة للنظام، وتضم في نطاقها العديد من الأساليب التقنية لتنفيذ الهجوم، منها إساءة إستغلال الأوضاع أو الانماط العادية للأداء والكيفية في النظام *Race condition*والهجمات غير المتزامنة أو غير المتوافقة المتصلة باستغلال ترتيب تنفيذ العمليات الاعتيادية *Asynchronous attacks.*

[1]– ذياب البداينة، الأمن وحرب المعلومات، ط 1، دار الشروق، عمان، 2002م، ص 29،كذلك محمود غيث عيسي بوحروره، أمن المعلومات، المركز العالي للمهن الشاملة، إجدابيا، قسم هندسة الحاسوب،ليبيا،2012 ،ص8

ح- حصان طروادة *(Trojan Horse)*

هو برنامج تجسسي يقوم بعمل معين، يحدده الشخص الذي صممه او زرعه في جهاز الضحية، يمكنه من الحصول على المعلومة التي يريدها [1].

- بداية كان تصميم هذه البرامج لأهداف نبيلة كمعرفة ما يقوم به الأبناء أو الموظفون على جهاز الحاسب، في غياب الوالدين أو المدراء وذلك من خلال ما يكتبونه على لوحة المفاتيح، الا انه سرعان ما اسيئ استخدامه، وتعد هذه البرامج من أخطر البـــرامـــــج المستخدمة من قبل المتسللين، وذلك يرجع إلى أنه يتيح للدخيل الحصول على كلمات المرور *(passwords)* وبالتالي الهيمنة على الحاسب الآلي بالكامل، كما أن المتسلل لن يتم معرفته أو ملاحظته كونه يستخدم الطرق المشروعة التي يستخدمها مالك الجهاز، كما تكمن الخطورة ايضا في أن معظم برامج حصان طروادة لا يمكن ملاحظتها بواسطة مضادات الفيروسات[2]،اضافة إلى أن الطبيعة الساكنة لحصان طروادة يجعلها اخطر من الفيروسات، فهي لا تقوم بتقديم نفسها للضحية مثلما يـــقـــوم الفيروس الذي دائما ما يمكن ملاحظته من خلال الإزعاج أو الأضرار، التي يقوم بها للمستخدم وبالتالي فإنه لا يمكن الشعور بهذه الاحصنة أثناء أدائها لمهمتها التجسسية وبالتالي فإن فرص إكتشافها والقبض عليها تكاد تكون معدومه.

خ-البرمجيات الخبيثة *Malicious Codes*

البرمجيات الضارة أو الخبيثة هي مهددات مزروعة[3] *(Planting Threats)*في النظم والبرامج وتستغل للتدمير، وتتمثل في الفيروسات وحصان طروادة والقنابل المنطقية والموقوتة، وتستغل هذه البرامج لتدمير النظم أو البرمجات أو المعلومات والبيانات أو الملفات أو الوظائف، أو تستثمر للقيام بمهام غير مشروعة كالاحتيال أو غش النظام أو سرقة البيانات والمعلومات المهمة كأرقام وكلمات السر، والحقيقة أن هذه المسميات ليست

[1]- ضياء مصطفى عثمان، السرقة الالكترونيّة، دراسة مقارنة، دار النفائس،2011،ص 73.

[2] - nanoart 2000 online: www.nanoart.f2s.com /hack/15.11.2000.

[3]- خالد بن سليمان الغثير، محمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، مركز التمييز لأمن المعلومات، جامعة الملك سعود، ط1 ،2009،ص57.

تسميات مترادفة للفيروسات، الشائعة بل أنها تختلف عن بعضها البعض من حيث تركيبها ومن حيث طريقة إحداث التجسس وأحياناً أسلوبها في الهجوم، والهدف من تركيبها أو زرعها.

- والبرامج الخبيثة تتمثل في:

1. الفيروس ***Virus*** :

هو عبارة عن برنامج حاسوب مثل أيِ برنامج تطبيقي آخر، [1] ولكن يتم تصميمه بواسطة أحد المخرِبين بهدف محدد، هو إحداث أكبر ضرر ممكن بنظام الحاسوب؛ ولتنفيذ ذلك يتم إعطاؤه القدرة على ربط نفسه بالبرامج الأخرى، وكذلك إعادة إنشاء نفسه حتى يبدو كأنه يتكاثر ويتوالد ذاتيا، مما يتيح له القدرة على الإنتشار بين برامج الحاسب المختلفة، وكذلك بين مواقع مختلفة في ذاكرة الحاسب حتى يحقق أهدافه التدميرية [2].

2. الديدان:***Worms :***

هو برنامج ينتقل غاليا عبر البريد الالكتروني، و يمتاز بقدرته على التنقل عبر شبكات الانترنت لغرض تعطيلها أو التشويش عليها عن طريق شل قدرتها على تبادل البيانات[3].

3. القنبلة الموقوتة :***Time Bomb :***

عبارة عن برامج تزرع لتدمير نظام ما في وقت محدد وغالباً ما تزرع مثل هذه البرامج من قبل الموظفين الذين يشعرون بالتهديد في وظائفهم.

[1]- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر و التوزيع ،2011،ص 75 و ما بعدها

[2] -Warwick Ford, Computer communications security, 1994, P18.

[3]- ضياء مصطفى عثمان، المرجع السابق، ص 74.

4. القنبلة المنطقية ***Logic Bomb***:

وهذه تماماً كالقنبلة الموقوتة إلا إنها تختلف من حيث أنها تقدح بتحقيق أمر ما، كأن لا يضمن إسم أو رقم الشخص زارع القنبلة في قائمة المرتبات، أو أن يضمن في قائمة المفصولين[1]

5. المصيدة ***Phishing***

و تعني اصطياد المعلومات من قبل القرصان باستخدام برامج لإلتقاط معلومات الضحايا، وذلك بخداع الضحية عن طريق برامج معينة، للقيام بنسخ صفحات موقع ما وليكن بنك بصورها وتصاميمها، ومن ثم إنشاء موقع على الإنترنت مشابه تماماً لموقع البنك وباسمً قريب جداً لاسم هذا الموقع، ومن ثم ارسال بريد ***إلكتروني E-mail*** يدعو فيه الضحية لتحديث معلومات حسابه الإلكتروني، مع وصلة ***Link*** إلى موقع البنك المزيف وسيجد الضحية نفسه مدعواً لإدخال اسم الدخول وكلمة السر، وبعد ذلك تقوم العصابة بحفظ معلومات الدخول ثم السطو على حساب الضحية فيما بعد، ثم لإنهاء العملية، إما أن يشاهد الضحية رسالة قصيرة تفيدك بأن هناك مشكلة في الدخول أو سيقوم الموقع المزيف بتحويل معلومات الدخول إلى صفحة البنك الحقيقية، باستخدام تقنيات معروفة في برمجة صفحات الإنترنت وسيجد الضحية نفسه أمام حسابه الحقيقي في البنك و لكن معلومات حسابه الشخصي تكون قد سرقت [2].

وسرقة المعلومات: تتم بان يقوم المجرم بزرع برامج من نوع حصان طروادة الذي يقوم بمتابعة حركة لوحة المفاتيح والفأرة ***(key logger)*** وتقوم بتسجيل كل ما تطبعه على لوحة المفاتيح، ثم ترسل هذه المعلومات بواسطة الإنترنت إلى كمبيوتر المجرم.

---

[1] Jargon-dictionnaire informatique , de bombe logique
– http//linux France. org/prj/jargonf/b/bombe-logique.htm

[2] –محمد أمين الشوابكة، جرائم الحاسوب والإنترنت–الجريمة المعلوماتية،دار الثقافة للنشر و التوزيع،الأردن،2011،ص 237 و ما بعدها .

لبند الرابع : الهجمات والمخاطر المتصلة بعمليات الحماية

والمعني هنا المخاطر والمهددات التي يتعرض لها نظام الحماية المستخدمة[1]، لحماية النظم وبتعرض نظام الحماية للهجوم والإختراق، تصبح كل أو بعض المعلومات والبرمجيات تحت سيطرة المهاجم، وبالتالي تنفيذ الأغراض التي دخل من أجلها للنظام سواء كان ذلك سرقة أو تخريباً أو تهديد، وهذه المخاطر في حقيقة الأمر تمثل كافة أنواع المخاطر والهجمات ولكن من زاوية تقنية.

ونورد فيما يلي خمسة أنواع من المخاطر وهي:

1- العبث بالبيانات *Data Diddling*

وهو استخدام يتعلق بالغش والخداع والإيهام والتقليد والمحاكاة والسرقة، والفكرة هنا تنبني على استخدام تقنيات لتزوير العنوان المرفق مع حزمة البيانات المرسلة، بحيث يفهم النظام على أنه عنوان صحيح، ويسمح النظام لحزمة البيانات بالمرور باعتبارها حزمة مشروعة وصحيحة.

2- تشمم كلمة السر *Password Sniffing*

عادة ما يتم كشف كلمات السر بطريقة التخمين أو تنفيذ معادلات، ولكن هنا يتم الكشف عنها باستخدام برامج يمكنها أن تتشمم أو تلتقط كلمات السر، خلال تجوالها في جزء من الشبكة أو أحد عناصرها بحيث تقوم هذه البرامج بجمع المعلومات، عندما يطبع المستخدم كلمة السر.

3- المسح والنسخ*Scanning*.

[1] -Franziska Boehm,information sharingand data protection in the area of freedom ,security and justice,towards harmonised data protection principles for information exchange, at Eu –level,Springer,Verlag,berlin ,Heidelberg,2012 ,p371.

وهو اسلوب يستخدم فيه برنامج (الماسح *ware dialer* –او *demon dialer* (*processes*الذي هو برنامج احتمالات يقوم على فكرة تغيير التركيب او تبديل احتمالات المعلومة، ويستخدم تحديدا بشان احتمالات كلمة السر او رقم هاتف المودم او نحو ذلك، وابسط نمط فيه عندما تستخدم قائمة الاحتمالات لتغيير رقم الهاتف بمسح قائمة أرقام كبيرة للوصل الى احدها الذي يستخدم موديم للاتصال بالإنترنت، او اجراء مسح لاحتمالات عديدة لكلمة سر للوصل الى الكلمة الصحيحة التي تمكن المخترق من الدخول لنظام، ومن جديد فان هذا اسلوب تقني يعتمد واسطة تقنية هي برنامج (الماسح) بدلا من الاعتماد على التخمين البشري.

4- هجومات استغلال المزايا الإضافية *Excess Privileges*

الفكرة هنا تتصل بواحد من أهم استراتيجيا الحماية، فالأصل أن مستخدم النظام تحديدا داخل المؤسسة–محدد له نطاق الاستخدام ونطاق الصلاحيات بالنسبة للنظام، و لكن ما يحدث في الواقع العملي، أن مزايا الاستخدام يجري زيادتها دون تقدير لمخاطر ذلك أو دون علم من الشخص نفسه انه يحظى بمزايا تتجاوز اختصاصه ورغباته، في هذه الحالة إن أي مخترق للنظام لن يكون فقط قادرا على تدمير أو التلاعب ببيانات المستخدم الذي دخل على النظام من خلال اشتراكه أو عبر نقطة الدخول الخاصة به، انه ببساطة سيتمكن من تدمير مختلف ملفات النظام، حتى غير المتصلة بالمداخل الذي دخل منه لأنه استثمر المزايا الإضافية، التي يتمتع بها المستخدم الذي تم الدخول عبر مدخله، وهذا وحده يعطينا التصور لأهمية إستراتيجية امن المعلومات، وحمايتها في المنشاء فان تحديد الامتيازات والصلاحيات قد يمنع في حقيقته من حصول دمار شامل، ويجعل الاختراقات غير ذي اثر، ولن تسمح الاستراتيجيات الواعية للقول أن المستخدم الفلاني لديه مزايا لا يعرف عنها بل لن تسمح بوجودها أصلا[1] .

5- تجاوز الرقابة (*Bypassing Controls*)

يقوم المهاجم أو المخترق بقراءة ملفات التحكم بالنظم ومعرفة نقاط الضعف واستغلال الضعف الموجود في النظام، بقراءة ملفات التحكم وبمتابعة مسار النظام والحصول علي

[1]– منى تركي الموسوي، الخصوصية المعلوماتية و اهميتها و مخاطر التقنيات الحديثة عنها، مركز بحوث السوق و حماية المستهلك، مجلة كلية بغداد للعلوم الاقتصادية ،جامعة بغداد، العدد الخاص بمؤتمر الكلية ، ص 26 و ما بعدها .

صلاحيات بطريقة غير مشروعة، وهنا يمكن أن يقوم بتنفيذ القيود المالية على حسابات العملاء و/أو الحسابات الوسيطة، بتبديل وتغيير المعلومات سواء بالإضافة أو الحذف أو التعديل، ودون ترك أي آثار لجريمته كما يمكنه تخريب النظام وإلغاء ملفاته وإتلاف بيانات العملاء.

المطلب الثاني :الحماية القانونية للمصنفات الرقمية

إن الاعتداء على البرامج ناتج بشكل رئيس بسبب ارتفاع سعر النسخة الأصلية مقارنة بالنسخ المقلدة، التي تحتاج إلى تكاليف زهيدة، بالإضافة إلى جانب ذلك اعتقاد الدول النامية و دول العالم الثالث، بضرورة الحصول على ما تنتجه الدول المتقدمة من برامج، و إن ذلك كله من اجل العمل على تقليص الهوة بين الدول المتقدمة بتقنياتها و الدول المستوردة و هي الدول النامية .

و نتيجة لهذا انتشر ما يسمى بسرقة البرامج، و التي تعني نسخ برامج الحاسب الآلي المشمولة بحق النشر و التأليف، دون إذن أو ترخيص من أصحابها، و يتم ذلك بنسخ برنامج من قرص مرن لقرص آخر، أو تحميل البرامج على جهاز الحاسب الآلي من شبكة المعلومات و عمل نسخة منه.

تنبع أهمية حماية البرامج من القيمة الاقتصادية لبرامج الحاسب الآلي التي نتجت من استثمارات مكلفة كما أن :

- إن توفير الحماية القانونية لهذه البرامج يؤدي إلى أن يتم تسويق هذه البرامج دون مبالغة في سعرها، إذ المبالغة في السعر احد أهم أسباب الاعتداء[1] .
- إن توفير الحماية القانونية للمبدعين يدفعهم إلى أن يستمروا في إبداعاتهم دون خشية من الفقر و الحاجة، إذ في حال إحساس المبدع أن جهوده ستسرق، و عوائده المالية سيستفيد منها غيره دون مقابل، فانه سيتوقف عن إبداعه و يبحث عن مصدر رزق أخر لطالما انه محروم من التمتع بحقوقه المالية و الأدبية هي ابسط حقوقه، عليها أو تزويرها، و بالتالي فمن الواجب أن يتم مسايرة التقدم المتسارع لهذه البرامج و توفير الحماية الفقهية و القانونية لها .

[1]- ضياء مصطفى عثمان، المرجع السابق، ص 131 و كذلك نوري حمد خاطر، شرح قواعد الملكية الفكرية، حقوق المؤلف والحقوق المجاورة، العين، الإمارات، 2008، ص190و ما بعدها .

ورد نص في المادة العاشرة /1 من اتفاقية التريبس ببسط الحماية على برامج الحاسب الآلي (الكمبيوتر) سواء أكانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها من الأعمال الأدبية التي تنبسط عليها الحماية بموجب اتفاقية برن 1971 .

كذلك فقد نصت المادة 2/10 على أن تتمتع بالحماية أيضا البيانات المجمعة أو المواد الأخرى، سواء أكانت في شكل مقروء آليا أو أي شكل آخر، إذا كانت تشكل خلقا فكريا نتيجة انتقاء أو ترتيب محتوياتها، مع التحفظ بأن هذه الحماية لا تشمل البيانات أو المواد في حد ذاتها، مع عدم الإخلال بحقوق المؤلفين المتعلقة بهذه البيانات أو المواد[1].

الفرع الأول : الطبيعة القانونية لبرامج الحاسوب.

لقد نشأ خلاف فقهي في نهاية السبعينيات من القرن المنصرم، حول الطبيعة القانونية لبرامج الحاسوب، وتمحور الخلاف حول نوع الحماية القانونية التي يجب أن تقرر لبرامج الحاسوب فيما إذا كان لابد من حمايتها تحت قانون براءات الاختراع، أو الأسرار التجارية، فذهب الاتجاه الأول في حججه إلى أنها ترتبط بالآلات، وباستخدامها في هذا الغرض، وما ينطوي عليه إعدادها من سرية وجدية، أيد هذا الاتجاه إلى أن تكون محمية بنطاق قانون براءات الاختراع، بينما ذهب أصحاب الاتجاه الثاني إلى أنها يجب أن تكون محمية بنطاق الأسرار التجارية لما لتلك الأسرار من قيمة تجارية كبيرة اذا ما تم نشره، وأن برامج الحاسوب تمتاز بكونها سرية في وظائفها وبطرق تطويرها، وبالتالي فإن قانون حماية الأسرار التجارية من يوفر الحماية القانونية لها[2].

وبقي هذا الخلاف قائماً إلى تاريخ جويلية من سنة 1978حيث صُدر تقرير من ***(CONTU: NATIONAL COMMISSION ON NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS)*** وهي اللجنة الوطنية التي شكلت بقرار من الكونجرس الأمريكي

[1] – حسن جميعي ،المرجع السابق، ص 16 .

[2]– يونس عرب، نظام الملكية الفكرية لمصنفات المعلوماتية، المركز العربي للقانون والتقنية العالمية، متاحة على الموقع التالي: www.arablawinfo.comص 20 .

لمراجعة قانون حق المؤلف الأمريكي، والتي أعدت تقرير قدمته للكونجرس تضمن عدة توصيات كان من بينها؛ أنها أوصت بأن تكون برامج الحاسوب محمية بنصوص قانون حق المؤلف، وأهم الحجج التي برروا فيها هذا الفكر الجديد، كانت من تعريفهم لبرنامج الحاسوب بأنه:" مجموعة من الجمل أو التعليمات لتستخدم بشكل مباشر أو غير مباشر في الحاسوب وذلك للحصول على نتيجة معينة"، وبهذا فإنهم اعتبروا برامج الكمبيوتر ضمن حقوق المؤلف، لأنها تستند إلى العمل الذهني المكتوب مثلها بذلك مثل المؤلفات الكتابية الأخرى، أي أن العلة بحماية المؤلفات توافرت لتلك البرامج[1].

وكانت تلك التوصيات ذات وقع كبير على المستوى العالمي، وقدمت لكل من المبرمجين ومشرعي تلك الدول وسائل حماية جديدة تضمن حقوق أصحاب تلك البرامج من أي عبث، وبهذا فان كثيراً من مشرعي تلك الدول ذهبوا إلى تبني تلك التوصيات في تشريعاتهم المحلية، أولهم المشرع الأمريكي، وكذلك المشرع الياباني وغيرها من الدول الأوربية في سنة 1980[2]،الأمر الذي حسم الجدل الدائر حول هذه المسألة، وجاءت اتفاقية ترابيس بمادة رقم 10 الفقرة الأولى التي نصت على " تتمتع برامج الحاسوب ،سواء أكانت بلغة المصدر أو بلغة الآلة بالحماية، باعتبارها أعمالاً أدبية (بموجب معاهدة برن 1971)"، وكذلك معاهدة الويبو بشأن حق المؤلف في مادتها رقم 4 التي أكدت على أن برامج الحاسوب هي مصنفات أدبية، لينتهي الخلاف تماما بشأن حماية برامج الكمبيوتر وتحسمه التشريعات المحلية والاتفاقات الدولية لصالح قانون حقوق المؤلف.

ومن خلال ذلك فإن المعاهدات الدولية، متبوعة بالتشريعات المحلية للدول التي وقعت ودخلت بتلك المعاهدات، شملت في قوانينها الداخلية برامج الحاسوب تحت قوانين حق المؤلف

---

[1] -Final report of the national commission on new tehnological uses of copyrighted works (July 31, 1978): Sections on Software Copyrights,p 61.

[2] -Alan Story, Intellectual Property and Computer Software, Lecturer in Intellectual Property Law, University of Kent, United Kingdom, Published by International Centre for Trade and Sustainable Development (ICTSD), International Environment House, p 11.

باعتبارها أعمالاً أدبية أو تتحد مع الأعمال الأدبية بنفس العلة، ذلك أنها اعتبرت برنامج الحاسوب وتلك الصياغة اللغوية المكتوبة على شكل تعليمات، جديرة بالحماية القانونية.

الفرع الثاني: الحماية بموجب قانون خاص.

إعتمادا على الطبيعة الخاصة لبرامج الحاسب الآلي سواء من حيث الخصائص الفنية او متطلبات الحماية، فقد أدى ذلك إلى ظهور القول بان برامج الحاسب الآلي، بحاجة إلى نصوص و قوانين خاصة للحماية و ان مجرد تعديل النصوص لا يكفي[1].

و قد تأيد هذا القول بما يلي :

أولا: إن كل ما قيل حول إمكان تمتع برامج الحاسب الآلي بالحماية الجزائية بموجب نصوص قانون براءات الإختراع، الرد المنطقي على ذلك، ثم تقويض حجج الحماية بالنظر إلى الطبيعة الخاصة لبرامج الحاسب الآلي من جهة، و اختلافها عن الطبيعة الخاصة للاختراعات من جهة أخرى، يدفع نحو القول بضرورة وجود قانون خاص كاف لبسط الحماية الجزائية على برامج الحاسب الآلي .

ثانيا: انه وإن انطبقت على برامج الحاسب الآلي وصف المصنفات وفقا لمفهومها في قانون حق المؤلف، باعتبارها تأتي تعبيرا عن أفكار مؤلفيها، إلا أنها رغم ذلك تختلف عن سائر المصنفات المحمية بموجب قانون حماية حق المؤلف من حيث الوظائف التي تؤديها.

فبرامج الحاسب الآلي و إن كانت وسائل لنقل المعلومات، و طريقة لغرض الأفكار والتصورات المعنية بقوالب مفهومة مقروءة، إلا أنها بالإضافة إلى ذلك و بمساعدات فنية خاصة كالشرائح الالكترونية تقوم بوظائف تشغيل الحاسب الآلي، على نحو تمكنه من أداء الوظائف و القيام بخدمات تطبيقية أخرى، و هي بهذا تبتعد على سائر المصنفات المحددة بقانون حماية حق المؤلف، و التي لا تتمتع بهذه الخاصة، كما تبتعد عن فلسفة الحماية المقصودة من قانون حماية حق المؤلف.

[1]- جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية"، دار الثقافة للنشر و التوزيع، ط 1، 2010، ص ص- 184-185 .

فالكتاب قد يكون حاوية لمجموعة من التعليمات أو المعلومات حول القيام بشيء معين، و البرامج قد تكون كذلك مجموعة تعليمات للقيام بعمل معين، غير أن الكتاب يخاطب الإنسان مباشرة، فيما يقوم الآخر بعمله داخل مستخلصات الحاسب الآلي، بحيث تؤثر فيه و تعطيه آليات القيام بعمل ما، أو أداء خدمة ما، فكانت النتائج و الأحداث مختلفة فيما بين المصنفات و البرامج، فالحقيقة إن البرامج الحاسب الآلي لا تقف عن حد الأفكار و المعلومات، محتوى كل مصنف خطي عادي لضعفها من جهة و لاختلافها و عدم قدرتها على التماشي مع طبيعة ومراحل برامج الحاسب الآلي، و لهذا كان الحل باقتراح قوانين خاصة، تعالج الحماية في ضوء ما ورد سابقا من مفهوم و طبيعة لبرامج الحاسب الآلي[1] .

ثالثا :إن نطاق الحماية التي يقرها قانون حماية حق المؤلف للمصنفات الواردة فيه يعتبر قاصرا إذ ما قورن بنطاق و حجم و شكل الاعتداءات التي تتعرض لها برامج الحاسب الآلي في الواقع فإذا كانت الحماية التي توفرها نصوص قانون حماية حق المؤلف تطال الاعتداءات المباشرة الواقعة على حق المؤلف أدبية كانت أو مادية، فان برامج الحاسب الآلي تتعرض لأصناف أخرى من الاعتداءات، لا تقع تحت هذا النمط من حيث إعادة كتابة البرنامج بلغات أخرى و تحقيق الاحتكار بطرق شتى، و بالتالي تصبح هذه الاعتداءات خارج نطاق العقاب، باعتبارها لا تمثل اعتداء مباشرا على حق المؤلف في المصنف وفقا لنصوص القانون .

رابعا: إن برامج الحاسب الآلي تشهد تطورا متسارعا و نموا تكنولوجيا يطال الطبيعة و الأسلوب، بالإضافة إلى تطورات سائر مشتملات التكنولوجيا الأخرى، الأمر الذي يعظم المخاطر، ويوسع صور الإعتداءات، وبالتالي فان الأمر يحتاج إلى قانون خاص يواكب ذلك كله، ويكون قادرا على استيعاب كافة التطورات و المستجدات و ملاحقتها دون ارتباط بمصنفات أخرى لا تحتاج إلى ذلك كله .

خامسا: إن إدماج برامج الحاسب الآلي ضمن نصوص قانون حق المؤلف يستدعي تعديل و تطوير مصطلحات و مفاهيم عديدة لا يبحثها ذلك القانون، ذات علاقة بالمصنفات و هو أمر يصعب تصوره، وفقا لرأي أصحاب هذا الاتجاه .

[1] – J.P Barlow, Selling Wine Without Bottels, in Hugenholtz, P.B.(ed.), The Future of Copyright in a Digital Environnement, The Huge, Kluwer ,1996, pp 170-185

تماشيا مع هذا تبنت بعض الدول نهجا بموجبه وضعت قانونا خاصا لحماية برامج الحاسب الآلي، و لم تكتف لا بنصوص قانون حق المؤلف و لا بالتعديل عليها، ومن ذلك كوريا الجنوبية حيث أصدرت قانونا خاصا لبرامج الحاسب الآلي في 31/12/1986 روعي فيه الطبيعة الخاصة لهذه البرامج .

وكذلك الدنمارك في قانونها الصادر عام 1986، [1]كما و عالجت المملكة المتحدة سائر الاعتداءات التي موضوعها برامج الحاسب الالي ضمن قانون خاص هو قانون إساءة استخدام الحاسب الآلي لسنة 1990 .

وتبع ذلك الولايات المتحدة الأمريكية التي عالجت الاحتيال و جرائم الاعتداء على برامج الحاسب الآلي ضمن قانون خاص عام 1986 .

أ . **التشريع الفرنسي :**

عدلت فرنسا من قانون حماية حق المؤلف النافذ المفعول لديها، بان أضافت برامج الحاسب الآلي إلى مجموعة المصنفات المحمية بموجبه برامج الحاسب الآلي [2] ،حيث صدر القانون رقم 85/660 المعدل لقانون حق المؤلف الفرنسي بتاريخ 3/6/1985و الذي تبنى الطبيعة الخاصة لبرامج الحاسب الآلي و التي تفرده عن سائر المصنفات الأخرى والتي توجب بعض ميزات الحماية خصوصا مدة الحماية، حيث أنقصت مدة الحماية العامة و جعلت مدة حماية خاصة لبرامج الحاسب الآلي بموجب هذا القانون بلغت خمسة و عشرين عاما [3].

---

[1] -The Act on the Protection of Semiconductor Products, Law No. 778 of 9 December 1987 . Law No. 153 of 14 January 1988

[2] - Loi n ° 85-660 du 3 juillet 1985. Loi relative à la protection des topographies des produits semi-conducteurs, Loi n ° 87 890 du 4 novembre 1987.

[3]- جلال محمد الزعبي، أسامة أحمد المناعسة، المرجع السابق، ص 189 .

ب .**التشريع الأمريكي**[1] **:** قانون الكونغرس الأمريكي عام 1980 بتعديل نصوص قانون حق المؤلف، بالإضافة برامج الحاسب الالي صراحة، و اعتبارها مصنفا من ضمن المصنفات المستحقة للحماية بموجب نصوصه. وقد كان تدخل المشرع الأمريكي بموجب ذلك في إطارين:

*الإطار الأول: إدراج برامج الحاسب الآلي ضمن المصنفات .

*الإطار الثاني : وضع تعريف خاص لبرامج الحاسب الآلي غير التعريف الأصلي العام المتعلق بسائر المصنفات الأخرى .

فقد عرف القانون برامج الحاسب الآلي، باعتبارها مصنفات فكرية بأنها مجموعة العبارات و التعليمات التي تستعمل بطريقة مباشرة أو بطريقة غير مباشرة في الحاسب الآلي،

و تبسط بموجبها الحماية الجزائية عليها غير أن هذا لم يكن كافيا فكان أن عدل القانون حق المؤلف ليضيف بصراحة برامج الحاسب الآلي ضمن نصوص قانون حق المؤلف لبسط هذه الحماية .

و قد سايرت هذا الاتجاه معظم قوانين حق المؤلف الدولية ، فقد استجابت المكسيك [2]و أيرلندا و استراليا [3]و سنغافورا و دول كبرى أخرى لطبيعة البرامج وصفتها الخاصة ، فعدلت نصوص قوانين حماية حق المؤلف لديها بما يكفل بسط الحماية اللازمة لبرامج الحاسب الآلي .

كما ظهرت تطبيقات القضاء و اعتماده على نصوص قانون المؤلف بصيغتها المعدلة، و اعتبارها الوسيلة الأفضل لحماية برامج الحاسب الآلي من سائر الاعتداءات الجائزة عليها [4].

---

[1] -The Computer Software Copyright Act 1980 amending the Copyright Act 1974 (17 U.S.C) 101, 117

- The Piracy and Counterfeiting Amendment Act of 24 May 1982 (17 U.S.C. § 506) and the Copyright Act as amended 1980 .17 U.S.C. 502.
- The Semiconductor Chip Protection Act of 8 November 1984.

[2] -The Copyright Amendment Act No. 114 of 8 October 1984.

[3] -The Copyright Amendment Act 1984 on Informatics.

[4]- جلال محمد الزعبي، أسامة أحمد المناعسة ، نفس المرجع، ص 190 .

ج . **التشريع المغربي** :أقرت أغلب التشريعات حماية برامج الحاسب الآلي بقانون حق المؤلف، بحيث أدرجت برامج الحاسب الآلي ضمن المصنفات الفكرية الخاضعة لنصوص قانون حق المؤلف[1]، فلم يعد الأمر كما كان من قبل متعلقا بالبحث عن مدى اعتبار برنامج الحاسب الآلي مصنفا مبتكرا أم لا، فقد تم حسم الأمر من خلال مواقف المشرع المغربي الصريحة بالنص على حماية برامج الحاسب الآلي بقانون حق المؤلف ومنها القانون المغربي رقم 00-2 المتعلق بحقوق المؤلف والحقوق المجاورة[2]، وتبقى جريمة تقليد هذه البرامج من أهم صور الاعتداء على حقوق مؤلفيها. وقد بين المشرع المغربي أحكام هذه الجريمة من خلال الفصول 575 حتى 579 من القانون الجنائي المغربي.

أما بخصوص العقوبات فان العقوبة في صورتها العادية هي الغرامة من 120 إلى 10000 درهم تطبيقا للمادتين 575و576 ، سواء تم نشر المؤلفات المقلدة بالمغرب أو خارجه، أو تم عرضها للبيع أو استيرادها أو تصديرها، وتطبق نفس العقوبات في حالة إنتاج أو عرض أو إذاعة مؤلف أدبي محمي قانونا.

أما المادة577 فقد عالجت حالة الاعتياد(الحبس من ثلاثة شهور إلى سنتين والغرامة من 500 إلى 20000 درهم)،ثم حالة العود إلى ارتكاب الجريمة بعد الحكم عليه من اجل جريمة الاعتياد(الحبس والغرامة يمكن أن ترفع إلى الضعف مع إمكانية الإغلاق الكلي أو الجزئي لمحل المقلد أو شركائه).

---

[1]- كانت هذه الحماية مثار جدل كبير في فرنسا قبل تدخل المشرع الفرنسي بالنص عليها صراحة القانون رقم 85-660 الصادر في 3 يوليه 1985 ، وكان الفقه والقضاء هناك منقسمين حول امتداد حماية حق المؤلف إلى برامج الحاسب الآلي بسبب الاختلاف حول توافر شروط المصنف المحمي في برامج الحاسب الالي : انظر على سبيل المثال.

A. Lucas , Les programmes d'ordinateurs comme objets de droits intellectuelles ,JCP ,1982,1,Doct,3081.

J. Huet , La modification du droit sous l'influence de l informatique, aspect de droit privé,JCP,1983,1,Doct,3095.

J.L. Goutal , La protection juridique du logiciel,D.1984,Chron,p197

M. Vivant, Informatique et propriété intellectuelle,JCP,1984,1 Doct,3081.

وانظر في عرض هذا الخلاف بالتفصيل الدكتور، محمد حسام لطفي ،الحماية القانونية لبرامج الحاسب الآلي ، دار الثقافة للطباعة والنشر ،القاهرة ،1987 ص 87 وما بعدها.

[2]- ظهير شريف رقم 1.00.20 صادر في 9 ذي القعدة 1420 ،المؤرخ في 15 فبراير 2000، بتنفيذ القانون رقم 2.00 المتعلق بحقوق المؤلف والحقوق المجاورة .

الفرع الثالث : موقف المشرع الجزائري من حماية البرمجيات

مما لاشك فيه أن ما يطلق عليه ثقافة الملكية الفكرية من الأمور المغيبة في الجزائر، شأنها في ذلك شأن سائر الدول النامية.

وإذا كان هذا هو الشأن في تلك القضية بوجه عام، فإنها أكثر وضوحاً فيما يتعلق ببرامج الحاسب الآلي نظراً لحداثتها من ناحية ولعجز كثيرين – ليس من العامة فحسب بل من المتخصصين أيضاً – عن الاقتناع بأن برنامج الحاسب يعدّ من قبيل المصنفات الأدبية من ناحية أخرى.

ومازال الكثيرون يتساءلون حتى الآن عن العلاقة بين برنامج الحاسب والكتاب أو قطعة الموسيقى، ولماذا لا تتم معاملة البرنامج باعتباره اختراعاً تتم حمايته بنظام براءات الاختراع؟ حقيقة أن هذا الأمر قد تمّ حسمه باتفاقية "تريبس" والتزام الدول الموقعة عليها بتعديل تشريعاتها للتوافق مع نص المادة العاشرة من الاتفاقية التي أسبغت على برامج الحاسب الحماية المقررة للمصنفات الأدبية[1]، ولكن تبقى العقبة الأساسية في كيفية إقناع الأشخاص الذين يتعاملون مع هذه البرامج بتلك الحقيقة.

ومن ثمَّ فمن المناسب أن نشير هنا إلى تجربة إحدى الدول المتقدمة في مجال التكنولوجيا وهي اليابان، ففي التقرير السنوي لإتحاد منتجي برامج الكمبيوتر ***Business (BSA) Software Alliance***عام 1995قدرت خسائر اليابان من جراء قرصنة البرامج بـــ 1.1 بليون دولار.

ومن هنا ثار التساؤل عن كيفية تطبيق قوانين حماية الملكية الفكرية والتعاون بين الأجهزة الحكومية والمؤسسات الصناعية في هذا الخصوص.

والحقيقة أنه يمكن أن يطلق على التجربة اليابانية في هذا الخصوص تجربة "إنشاء وعي شعبي مضاد لعمليات القرصنة"، حيث قامت أجهزة الإعلام بدور فعال في إيضاح الصورة لدى

[1]– و من هذه التشريعات ، التشريع المصري في المادة 2 من القانون رقم 38 لسنة 92م والمعدل بالقانون رقم 29 لسنة 1994م، والأردني في المادة 8/3 من قانون حماية المؤلف رقم 22 لسنة 1992م، والتونسي في المادة 1 من قانون الملكية الأدبية والفنية رقم 36 لسنة 1994م، والسعودي في المادة 3/10من نظام حماية حقوق المؤلف، والقطري في المادة 10/2 من قانون حماية المصنفات الفكرية وحقوق المؤلف، رقم 25 لسنة 1995م، البحريني في المادة 2/ي من قانون حماية حقوق المؤلف رقم 10 لسنة 1993م.

الناس وما يؤدى إليه استخدام البرامج المنسوخة أو المقلدة من إضرار بالاقتصاد الياباني مما ترتب عليه تقليص الخسائر في السنوات التالية، ولقد كان دور التوعية واقعياً، حيث فرق بين قيام شركات أو مجموعات بنسخ وتزوير البرامج وبين الأفراد الذين يقومون بعملية نسخ لإهدائها لأصدقائهم أو لاستخدامهم الشخصي.

أما عن موقف الدول العربية من الاتفاقيات الدولية في مجال الملكية الفكرية، فيمكننا القول أن غالبية الدول العربية هي أعضاء في أهم ثلاثة اتفاقيات وهى اتفاقية "إنشاء المنظمة العالمية للملكية الفكرية" واتفاقية "بيرن للملكية الأدبية" واتفاقية "باريس للملكية الصناعية"، أما الاتفاقيات الأخرى والتي تندرج تحت أي من هذين الموضوعين (الملكية الأدبية أو الصناعية) فإن عدد الدول العربية المنضمة قليل جداً، وبالعموم تحتل مصر المركز الأول بين الدول العربية في عدد الاتفاقيات التي انضمت إليها وتبلغ 11 اتفاقية من أصل 24 - عدا تربس - ثمّ المغرب 10 اتفاقيات، في تونس 9 اتفاقيات، ثمّ الجزائر 8 اتفاقيات[1]، في لبنان 6 اتفاقيات.

الفرع الرابع : حماية البرمجيات وقواعد البيانات من التقليد في تشريع 03-17 [2]

لم تستطيع الوسائل التقنية الحديثة بكل سطوتها وتقدمه أن تحول دون تقليد البرنامج المحصَن الأصيل، [3]فلا يوجد حتى الآن من البرامج ما يمتنع عن التقليد او النسخ مهما كانت

[1] - بدأ نفاذ الاتفاقيات التي تديرها wipo في الجزائر: اتفاقية روما بتاريخ 22ابريل 2007،معاهدة الويبو بشان حق المؤلف بتاريخ31 يناير 2014، اتفاقية إنشاء المنظمة العالمية للملكية الفكرية في 16 ابريل 1975، اتفاقية برن لحماية المصنفات الأدبية و الفنية في 19 ابريل 1998، معاهدة الويبو بشان التسجيل الصوتي بتاريخ 31 يناير 2014.

[2] - القانون رقم 03-17 مؤرخ في 9 رمضان عام 1424 الموافق 4 نوفمبر عام 2003, يتضمن الموافقة على الأمر رقم 03-05 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 19يوليو عام 2003 والمتعلق بحقوق المؤلف والحقوق المجاورة.

[3] - شرط الأصالة لحماية المصنفات الواردة في نص المادة الرابعة من الأمر رقم 97-10 المؤرخ في 06 مارس 1997م، المتعلق بحقوق المؤلف والحقوق المجاورة وهي كالتالي:

- المصنفات الأدبية المكتوبة مثل المحاولات الأدبية، والبحوث العلمية والتقنية، والروايات، والقصص، والقصائد الشعرية، ومصنفات وقواعد البيانات، والمصنفات الشفوية مثل المحاضرات والخطب وباقي المصنفات التي تمثلها.
- كل مصنفات المسرح والمصنفات الدرامية، والدرامية الموسيقية والإيقاعية والتمثيليات الإيمائية.
- المصنفات الموسيقية بالغناء أو الصامتة.
- المصنفات السينمائية أو المصنفات السمعية البصرية الأخرى سواء كانت مصحوبة بأصوات أو بدونها.
- مصنفات الفنون التشكيلية والفنون التطبيقية مثل: الرسم، والرسم الزيتي، والنحت، والنقش، والطباعة الحجرية وفن الزرابي.

وسيلة التقنية المستخدمة في تحصينه، لذلك لا مناص من ضرورة البحث عن وسائل قانونية لحماية البرامج من التقليد[1]، لهذا السبب نجد ان المشرع الجزائري قد جرّمَ أعمال القرصنة (piracy)[2]

الواردة على المصنفات الأدبية والفنية، بما فيها برامج الحاسوب وعاقبَ مُرتكبها فقد اعتبرها من الحقوق المحمية دستوريا ،إذا تفحصنا مختلف الدساتير فنلاحظ أن دستور سنة 1976 ودستور 1989 فقد تطرقا كليهما إلى ضرورة حماية عصارة الأفكار العلمية وتصنيفها كحق دستوري محفوظ، حيث نص دستور 22 فيفري 1976 في مادته 54: "على حرية الابتكار الفكري والفني والعلمي للمواطن مضمونه في إطار القانون"، أما الدستور 23 فيفري 1989 فقد جاء بنفس ما جاء به سلفه إلا أنه أضاف: " لا يجوز حجز أي مطبوع أو تسجيل أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي."

الأمر رقم 03-05 مؤرخ في 19 جمادى الأولى عام 1424 الموافق لـــ 19 جويلية سنة 2003والمتعلق بحقوق المؤلف والحقوق المجاورة، والملغي للأمر رقم 97-10[3] حيث نجده في مادته الرابعة استبدل مصطلح قواعد البيانات بمصطلح برامج الحاسوب، حذف مصطلح قواعد البيانات من المادة سبعة وعشرون المتمثلة في الحقوق المادية وأحتفظ بمصطلح برامج

- الرسوم والرسوم التخطيطية والمخططات، والنماذج الهندسية المصغرة للفن والهندسة المعمارية والمنشآت التقنية.
- الرسوم البيانية والخرائط والرسوم المتعلقة بالطوبوغرافيا أو الجغرافيا أو العلوم.
- المصنفات التصويرية والمصنفات المعبر عنها بأسلوب بماثل التصوير.
- مبتكرات الألبسة للأزياء والوشاح.

[1] – مصطفى محمد عرجاوي، المرجع السابق، ص376.

[2] – القرصنة في الجزائر

أظهرت دراسة حول قرصنة البرمجيات عالميا، أن القيمة التجارية للبرمجيات المقرصنة حول العالم بلغت 63.4 مليار دولار في عام 2011. وكشفت دراسة حديثة لمؤسسة (بزنيس سوفتوير اليانس) أحد المدافعين عن قطاع البرامج المعلوماتية، أن القرصنة المعلوماتية في الجزائر بلغت 84% لهاية العام 2011 ما يعادل 83 مليون دولار كخسارة تجارية للجزائر وذكرت الدراسة أن 57% من مستعملي الحاسوب أقروا بأنهم اكتسبوا برامج معلوماتية بطريقة غير شرعية وبأنهم قاموا بالقرصنة في أغلب الأوقات ما أدى إلى ارتفاع معدل القرصنة المعلوماتية إلى 84% العام 2011 حيث لم تتغير مقارنة بالسنوات التي سبقتها ما عدا سنة 2010 حيث انخفضت رمزيا بنسبة 1%[2] وذلك على النحو التالي:2007 / 84%-2008 / 84%-2009 / 84%-2010 / 83%-2011 / 84%.

[3] – الأمر رقم 97-10 ،المؤرخ في 06 مارس 1997م المتعلق بحقوق المؤلف والحقوق المجاورة ، المؤرخة في 12 مارس 1997م، ج.ر.ر13،الملغى بموجب الأمر رقم 03-05 مؤرخ في 19 جمادى الأولى عام 1424 الموافق لـــ 19 جويلية سنة 2003والمتعلق بحقوق المؤلف والحقوق المجاورة.

الحاسوب، وأضيف مصطلح معالجة معلوماتية في الأمر 03-05 عوض العبارة السابقة من نفس المادة في الأمر رقم 97-10 وهي كالآتي:" إبلاغ المصنف إلى الجمهور بأية منظومة معالجة معلوماتية"، وأضيفت العبارة التالية في نفس المادة من الأمر 03-05 وهي كالتالي" لا تطبق حقوق التأجير المنصوص عليها في هذه المادة على تأجير برنامج الحاسوب عندما لا يكون البرنامج الموضوع الأساسي للتأجير". غير البندين 4 و8 من المادة 27 من الأمر 97-10 إلى الفقرتين 5 و4 من المادة 22 من الأمر 03-05 المتضمنين في المادة اثنان وثلاثون .

أما فيما يخص الاستثناءات والحدود فإننا نجد في المادة الواحدة والأربعون 41 أنه قد أضاف استثناءات أخرى تمثلت في الاستنساخ الخطي لكتاب كامل أو مصنف موسيقي في شكل خطي واستنساخ قواعد البيانات في شكل رقمي، واستنساخ برامج الحاسوب إلا في الحالات المنصوص عليها في المادة 52 من هذا الأمر.

وفي المادة 54 من الفصل الرابع جعل الحقوق المادية تحظى بالحماية لفائدة المؤلف طوال حياته، ولفائدة ذوي حقوقه مدة خمسين سنة [1]، وتناول الأمر في بابه السادس الإجراءات والعقوبات المتخذة في حال الاستنساخ غير المشروع للمصنف بما يخالف حقوق المؤلفين والحقوق المجاورة إذ جعل في فصله الأول من المادة 143 إلى 150 من نفس الباب أنه يمكن للمتضرر برفع دعوى قضائية لتعويض الضرر، أما الفصل الثاني والذي تناول الأحكام الجزائية، فقد أعتبر كل مقلد من يقوم باستنساخ أو بيع أو تأجير أو استيراد وتصدير مصنف مقلد، قد ارتكب جنحة ويعاقب بالحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة مالية من 500.000دج إلى 1000.000 دج سواء تمت عملية النشر في الجزائر أو في الخارج[2].

أسباب عديدة تمت الاشارة اليها أعلاه مجتمعة، جعلت حماية البرمجيات تطرح بحدة، خاصة مع تطور تقنيات الحواسيب، وتنوع أشكال القرصنة والتقليد بشكل كبير، وكان لا

[1] و هذا ما نجده في اتفاق تريبس، الذي يلزم بأن تستغرق مدة الحماية أيا كانت معايير تحديدها غير المبنية على عمر شخص طبيعي 50 سنة على الأقل ،اعتبارا من تاريخ أول نشر مرخص للمصنف،أو 50 سنة اعتبارا من تاريخ ابتكاره. على أن هذه القاعدة لا تنطبق على المصنفات الفوتوغرافية أو مصنفات الفنون التطبيقية.

[2] – ميلود، العربي بن حجار .تشريعات الملكية الفكرية في حقل حماية البرمجيات بالجزائر -.Cybrarians Journal -. و 26، سبتمبر http://journal.cybrarians.info/2011

مناص من تدخل المنظمات الدولية والحكومات الوطنية لحماية ثمار الجهد الإنساني من الاستغلال والتشويه أو السطو والسلب.

ان المشرع الجزائري غيّر بعض الأمور الطفيفة جدا في الأمر97-10 المتعلق بحقوق المؤلف و الحقوق المجاورة، والملغى بموجب الأمر05/03 إلا انه ضمن هذا الأخير في كل المادتين 4 و 5 احد هذه المصنفات بشكل حصري واشاري دون تفصيل فيه وهما كل من برامج الحاسب الآلي وقواعد البيانات، كما انه خلق بعض اللبس ان صح التعبير في المادة 4 عند قوله

"وبرامج الحاسب الآلي والمصنفات الشفوية مثل المحاضرات والخطب والمواعظ وباقي المصنفات التي تماثلها " فعبارة " تماثلها" هل يقصد بها هنا لمصنفات التي تماثل برامج الحاسب الآلي ؟ أم الهاء تعود على الخطب والمحاضرات والمواعظ ؟ هذا من جهة .

ومن جهة أخرى نجد ان حقوق المؤلف عرضة للعديد من الاعتداءات بمختلف أشكالها وعلى اختلاف درجات الأضرار التي تلحقها بالمؤلفين محل الضرر، ولردع مثل هذه الاعتداءات استوجب ذلك على المشرع ان يوفر طرقا أكثر فاعلية وقابلة للتطبيق، حتى تحمى هذه الحقوق بشكل اكبر وفعال، وكذلك بتضافر الجهود مع المعلوماتيين التقنيين لتوفير السبل التقنية الفعالة، للحماية في ظل بيئة رقمية جد متطورة، ولأجل ذلك وضع المشرع وسائل وقائية للحماية بالإضافة إلى الوسائل الموضوعية، من حماية جزائية وكذلك مدنية[1].

[1]- ونسه ديالا عيسى، حماية حقوق التأليف على شبكة الانترنيت، المنشورات الحقوقية، بيروت، 2010، ص126 .

المبحث الثاني: جرائم تقنية المعلومات

تعد الجرائم المعلوماتية[1] صنفاً مستحدثاً من الجرائم التي تتحدى القواعد التقليدية للتجريم و العقاب، التي تقتضي ضرورة تحقق أركان الجريمة طبقاً لمبدأ شرعية الجرائم و العقوبات، علما أنه إذا ما تأخرت القوانين والتشريعات اللازمة لمواجهة هذه الظاهرة الإجرامية، الجديدة، فسوف نواجه عشوائية سيبيرية كتلك العشوائية العمرانية التي تنتج عن تأخر قوانين التطوير العمراني.

المطلب الأول : حرب المعلومات

شهد العالم ثورة من نوع غير مألوف اصطلح على تسميتها بثورة المعلومات، كان بطلها جهاز الحاسب الآلي الذي تطور دوره بحيث تعدى إجراء العمليات الحسابية المعقدة ليشمل قضايا تُهم الناس في جميع معاملاتهم بما فيها قضايا الاتصالات مرورا بالمعلوماتية التوثيقية والذكاء الإصطناعي... الخ [2]

و ليس هناك من إجماع واسع على تعريف محدد ودقيق لمفهوم الحرب الإلكترونية الآن[3]، وعلى الرغم من ذلك، فقد اجتهد عدد من الخبراء من ضمن اختصاصاتهم في تقديم تعريف يحيط بهذا المفهوم، فعرّف كل من "ريتشارك كلارك" و"روبرت كناكي" الحرب إلكترونية، على أنها "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها.

كما يمكن تعريفها "حرب المعلومات" هي مجموع النشاطات المتخذة بهدف احراز التفوق المعلوماتي ،بجمع و معالجة معلومات و انظمة معلومات العدو، مع حماية البيانات و أنظمة المعلومات الصديقة "[4]

---

[1]- أوّل ظهور لمصطلح الجرائم الالكترونية سنة 1998 في مؤتمر بأستراليا و في 2001/11/27 عقد المؤتمر الأوروبي لمكافحة الجريمة عبر الانترنت، و قد عقد مؤتمر الأمن العربي حول الجريمة الالكترونية للدولة العربية سنة 2002.

[2]- *François-Bernard Huyghe*, L'ennemi à l'ère numérique : Chaos, information, domination, *P.U.F., 2001, p 216*

[3]- هشام سليمان، تكنولوجيا المعلومات والاتصال، مجلة علوم وتكنولوجيا،ط2،2001، ص 25 .

[4] -Loup Francart. Infosphère et intelligence stratégique, IHEDN, Economica, Paris, 2002, p 52.

فيما يعرّف آخرون مصطلح الحرب الإلكترونية بأنها "مفهوم يشير إلى أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي" ولأن مثل هذه التعريفات فضفاضة ولا تعبّر بدقّة عن فحوى الموضوع، يقترح آخرون أن يتم التركيز بدلا من ذلك على أنواع وأشكال النزاع التي تحصل في الفضاء الإلكتروني، ومنها:

الفرع الأول : القرصنة الإلكترونية

تقع في المستوى الأول من النزاع في الفضاء الإلكتروني،[1] تعد عملية القرصنة الالكترونية إحدى أخطر الظواهر الجديدة التي صاحبت التطور الإلكتروني على مدى السنوات القليلة الماضية في الجزائر.

ففي المجال القانوني وخبراء في التقنيات الحديثة لتكنولوجيات الإعلام والاتصال أكد مختصون، أن المؤسسات الجزائرية الاقتصادية والإدارية غير مؤمّنة بشكل كامل ضد القرصنة والاعتداءات الإلكترونية، بما في ذلك الإدارات العمومية أو البنوك والمؤسسات المالية، الأمر الذي يهدد مصير نشاطها الاقتصادي[2].

إن القانون الجزائري على الرغم من تجريمه لفعل القرصنة الالكترونية أو الاعتداء على معلومات حساب شخصي أو تابع لمؤسسة معينة، منذ صدور قانون 2004، إلاّ أن التشريع لم يخض في التفاصيل، وإنما اكتفى بوضع الخطوط العريضة للفعل المجرم.

---

[1]- قانون وقف القرصنة على الإنترنت Stop Online Piracy Act أو "SOPA" اختصارا،هو قانون تم اقتراحه في الكونغرس الأمريكي بتاريخ 26أكتوبر لعام 2011 عن طريق النائب لامار سميث لمنع أعمال ونشاطات القرصنة على الإنترنت .يسعى القانون لإغلاق جميع مواقع الإنترنت (مثل مواقع التورنت أو مواقع التحميل والمشاركة) التي تنشر مواد محفوظة الحقوق أو مواد تساعد على القرصنة نهائياً ولن يتمكن صاحب الموقع من استرجاعه وقد يصل الأمر إلى سجن صاحبه مدة أقصاها خمس سنوات في السجن. القانون يهدف لتوسيع قدرة إنفاذ قانون الولايات المتحدة لمكافحة الاتجار على الإنترنت في مجال الملكية الفكرية حقوق الطبع والنشر والسلع المقلدة.

Margaret Rouse, Stop Online Piracy Act (SOPA) and PIPA ,Continue reading about SOPA:

- The United States House of Representatives website has more information about SOPA

[2]- سعيد بشار، المؤسسات الجزائرية غير مؤمّنة ضد القرصنة، مقال كتب بتاريخ 13 ابريل 2014،متاح على الموقع التالي : http://www.elkhabar.com

ويعرف الإختراق في مجال الكمبيوتر والشبكات بأنه القدرة علي الوصول لجهاز أو شبكة أو موقع معين بطريقة غير مشروعة عن طريق الثغرات الأمنية الموجودة في نظام الحماية الخاص بالهدف، كالدخول على أجهزة الآخرين عنوة أو التلصص داخل شبكاتهم.[1] ويعتبر البعض أن الإختراق تفوق علمي وإنجاز يدعو إلى الفخر لمن قام به، بينما يرى البعض الآخر أنه جريمة ويحمل عدة دوافع منها سياسية او اقتصادية وتجارية، ثمة صراع تكنولوجي مقنع في صورة تنافس تجاري بين الشركات الكبرى، حيث يسعي كل طرف للتجسس على مخترعات الآخر، والوقوف على مدى الإنجاز التي حققته الشركات المنافسة. وهناك دوافع سياسية ايضاً حيث يقوم البعض بعمليات الاختراق علي سبيل التباهي والفخر وإثبات الذات من دون وجود أي دافع تجاري أو سياسي، وقد يكون بغرض السطو والكسب المادي غير المشروع أو من أجل الانتقام الشخصي.

الفرع الثاني : التجسس الإلكتروني و الاحتيال المعلوماتي

ويقعان في المستوى الثاني والثالث وغالبا ما يستهدفان الشركات والمؤسسات في القطاعين العام و الخاص.

---

[1] -En France, l'article 323-1 du nouveau code pénal, sanctionne l'intrusion dans un système automatisé. L'alinéa 2 de cet article aggrave même la sanction lorsque l'intrusion a eu pour effet de falsifier ou de supprimer des données.

-Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende. Article 323-1 Modifié par LOI français n°2015-912 du 24 juillet 2015 - art. 4 - Loi français n° 92-685 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les biens.

يعدّ التجسس المعلوماتي[1] واحداً من الجرائم التي تُرتكب من خلال أنظمة الحاسوب وشبكة الإنترنت، ويتمثّل أسلوب التجسس باستخدام قراصنة المعلوماتية أساليب فعّالة للحصول على كلمات المرور بطريقة غير مشروعة، وتُقدّر خطورة التجسس بحسب أهمية المعلومات المستهدفة، التي يمكن أن تكون معلومات عسكرية أو اقتصادية أو معلومات خاصة ببطاقات الائتمان وغير ذلك من المعلومات[2].

وقد اتجهت بعض التشريعات إلى تجريم التجسس المعلوماتي بنصوص خاصة، ومن هذه التشريعات على سبيل المثال، المادة 370 من قانون العقوبات اليوناني التي تعاقب "كل من يقوم – على نحو غير مشروع – بنسخ أو طباعة أو استعمال أو إفشاء معلومات مبرمجة أو برامج حواسيب، إذا كانت تحتوي على أسرار تتعلق بالدولة، أو أسرار علمية، أو أسرار مهنية، أو أسرار تتعلق بالمؤسسات الاقتصادية، أو اعتدى بأي وسيلة أخرى على مثل هذه المعلومات".

أما الإحتيال المعلوماتي، فهو يعد واحداً من أهم الجرائم التي تركب في مجال تكنولوجيا المعلومات، سواء من حيث حجم الجريمة أو مقدار الخسائر الناجمة عنها، فقد شكّلت المواقع الإلكترونية العائدة للمصارف، وسهولة التحويل الإلكتروني، وانتشار أجهزة الصرف الآلي، مجالاً خصباً للاحتيال المعلوماتي.

والاحتيال المعلوماتي يقصد به «التلاعب العمدي بمعلومات وبيانات تمثّل قيماً مادية يختزنها نظام الحاسوب، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب بالأوامر والتعليمات التي تحكم عملية البرمجة، أو أية وسيلة أخرى من شأنها التأثير على الحاسوب

[1]– حسن بن أحمد الشهري،ا لأنظمة الالكترونية الرقمية المطورة لحفظ و حماية سرية المعلومات من التجسس، المجلة العربية للدراسات الأمنية و التدريب، جامعة نايف العربية للعلوم الأمنية، المجلد 28، العدد 56،الرياض،ص11 و ما بعدها .

[2]– داود حسن طاهر، نظم المعلومات، أكاديمية نايف الأمنية،الرياض،1999،ص 95.

حتى يقوم بعملياته بناء على هذه البيانات أو الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع وإلحاق الضرر بالغير»[1].

ومن أبرز صور الاحتيال المعلوماتي، الاستيلاء على أموال المصارف عبر الإنترنت، والاحتيال التجاري، عن طريق عدم تسليم البضائع للمشتري بعد شرائها ودفع ثمنها عبر الإنترنت، والاحتيال عن طريق الأوراق المالية، وذلك من خلال نشر المعلومات الكاذبة عن أسهم بعض الشركات، بهدف الترويج لها، والاحتيال بأسلوب انتحال الصفة، كإنشاء المواقع الإلكترونية المشابهة لمواقع الشركات التجارية، والاحتيال عن طريق البريد الإلكتروني، كإرسال رسالة الكترونية تتضمن جائزة وهمية مقابل بعض الأجور التي يتوجب على المرسل إليه تحويلها إلى الجهة المرسلة.

الفرع الثالث : الإرهاب الإلكتروني

ويقع في المستوى الرابع من النزاع في الفضاء الإلكتروني، ينطلق الإرهاب بجميع أشكاله وشتى صنوفه من دوافع متعددة, ويستهدف غايات معينة،ويتميز الإرهاب الإلكتروني عن غيره من أنواع الإرهاب بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والوسائل الإلكترونية

[1]- قامت معظم التشريعات بتجريم الاحتيال المعلوماتي بنصوص خاصة، ومن هذه التشريعات على سبيل المثال، القسم 1030 من القانون الفيدرالي للولايات المتحدة الأمريكية، والمادة 263 من قانون العقوبات الألماني:

Quiconque avec l'intention d'obtenir pour lui-même ou une tierce personne illégales dommages d'avantages matériels dont la propriété d'un autre en influençant le résultat d'un traitement de données opérationnelles grâce à une configuration incorrecte d'un programme, l'utilisation de données incorrectes ou incomplètes, l'utilisation non autorisée de données ou d'autres influence non autorisée sur le cours du traitement est passible d'un emprisonnement maximal de cinq ans ou d'une amende.

1. L'article 263 (2) à (7) sont applicables mutatis mutandis.
2. Quiconque prépare une infraction en vertu du paragraphe (1) ci-dessus par l'écriture de programmes informatiques dans le but de tout ce qui est de commettre cherchant à agir, ou les achète pour lui-même ou d'une autre, offre à la vente, ou détient ou les fournit à un autre doit être passible d'un emprisonnement ne dépassant pas trois ans ou d'une amende.
3. Dans les cas visés au paragraphe (3) ci-dessus l'article 149 (2) et (3) sont applicables mutatis mutandis. Citation complète: Code criminel dans la version promulguée le 13 Novembre, la loi de 1998 Federal Gazette [Bundesgesetzblatt] I p. 3322, modifié en dernier lieu par l'article 1 de la loi du 24 Septembre 2013, Journal officiel fédéral I p. 3671 et avec le texte de l'article 6 (18) de la loi du 10 Octobre 2013, Journal officiel fédéral I p 3799.

التي جلبتها حضارة التقنية في عصر المعلومات، لذا فإن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف الإرهابيين .[1]

وغني عن البيان أن الإرهاب الإلكتروني يشير إلى عنصرين أساسيين هما: الفضاء الافتراضي *Cyber Space* والإرهاب *Terrorism* إضافة إلى ذلك هناك كلمة أخرى تشير إلى الفضاء الإلكتروني وهي العالم الافتراضي *Virtual World* والذي يشير إلى التمثيل الرمزي والزائف والمجازي للمعلومات، وهو المكان الذي تعمل فيه أجهزة وبرامج الحاسوب والشبكات المعلوماتية، كما تتنقل فيه البيانات الإلكترونية، ونظراً لارتباط المجتمعات العالمية فيما بينها بنظم معلومات تقنية عن طريق الأقمار الصناعية وشبكات الاتصال الدولية، فقد زادت الخطورة الإجرامية للجماعات والمنظمات الإرهابية، فقامت بتوظيف طاقتها للاستفادة من تلك التقنية واستغلالها في إتمام عملياتها الإجرامية وأغراضها غير المشروعة.

كما أصبح من الممكن اختراق الأنظمة والشبكات المعلوماتية, واستخدامها في تدمير البنية التحتية المعلوماتية، التي تعتمد عليها الحكومات والمؤسسات العامة والشركات الاقتصادية الكبرى، وهناك ما يشير إلى إمكانية انهيار البنى التحتية للأنظمة والشبكات المعلوماتية في العالم كله، وليس في بعض المؤسسات والشركات الكبرى أو في بعض الدول المستهدفة، فالإرهاب الإلكتروني أصبح خطراً يهدد العالم بأسره، ويكمن الخطر في سهولة استخدام هذا السلاح الرقمي مع شدة أثره وضرره، حيث يقوم مستخدمه بعمله الإرهابي وهو مسترخ في مترله أو في مكتبه أو في غرفته الفندقية، وبعيداً عن أنظار السلطة والمجتمع.

الطاقة والماء، أو اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية.

وتأسيساً على ما سبق يمكننا القول بأن الإرهاب الإلكتروني هو إرهاب المستقبل، وهو الخطر القادم، نظراً لتعدد أشكاله وتنوع أساليبه واتساع مجال الأهداف التي يمكن من خلال وسائل الاتصالات وتقنية المعلومات مهاجمتها في جو مريح وهادئ، وبعيد عن الإزعاج والفوضى،مع توفير قدر كبير من السلامة والأمان للإرهابيين.

[1]- محمد أمين الرومي، جرائم الكمبيوتر و الانترنيت، دار المطبوعات الجامعية،2003، ص 182.

الفرع الرابع : الحرب الإلكترونية

وهي المستوى الأخطر للتراع في الفضاء الإلكتروني، وتعتبر جزءا من الحرب المعلوماتية بمعناها الأوسع.[1]

وهناك جدل واسع حول تحديد مفهوم حرب المعلومات فغالباً ما يتم ربطه بالمجال العسكري، بالرغم من شمول المعنى إلا أننا نستطيع القول بأن "حرب المعلومات *(information warfare)*هو: استخدام نظم المعلومات لاستغلال وتخريب وتدمير وتعطيل معلومات الخصم، وعملياته المبنية على المعلومات ونظم معلوماته وشبكات الحاسب الآلي الخاصة به، وكذلك حماية ما لدي من كل ذلك من هجوم الخصم؛ لإحراز السبق والتقدم على نظمه العسكرية والاقتصادية". وتنقسم حرب المعلومات إلى ثلاث مستويات: شخصية، مؤسسية، وعالمية.[2]

ومن المتوقع أن تصبح الحرب الإلكترونية نموذجا تسعى إليه العديد من الجهات نظرا للخصائص العديدة التي تنطوي عليها، ومنها:

---

[1]- هناك من الجرائم الافتراضية يكون الهدف أو الدافع من وراء ارتكابها دوافع سياسية تتمثل في تهديد الأمن القومي والعسكري وظهور ما يعرف بحرب المعلومات و التجسس الإلكتروني والإرهاب الإلكتروني. وكانت تقارير صحافية ذكرت في منتصف 2009 قيام جهات صينية غير معروفة باختراقات كبيرة على شبكة الإنترنت طالت مئات الحواسيب في زهاء 103 بلدان. وكانت عملية الاختراق منظّمة واستهدفت بشكل خاص مجموعة من أجهزة الحاسب الآلي التي تخص جهات ديبلوماسية وأمنية وشخصيات عالمية. وكشف عن بعض تفاصيل هذا الحادث لوسائل الإعلام مركز أبحاث كندي يعمل في مجال المعلوماتية باسم" مرصد حرب المعلومات". وذكر المركز الكندي أن شبكة تجسس الكترونية تعمل من الصين تمكنت من اختراق 1295 جهاز حاسب آلي في 103 بلد. لمزيد من التفاصيل حول هذا الموضوع أنظر : http://ucipliban.org

[2]- هشام سليمان، حرب المعلومات الوجه الجديد للحروب،2001 .
http://www.islamonline.net/servlet/Satellite.

1. حروب الإنترنيت هي حروب لا تناظرية (*Asymmetric*): فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب، يعني أنّه ليس هناك حاجة لدولة ما مثلا أن تقوم بتصنيع أسلحة مكلفة جدا، كحاملات الطائرات والمقاتلات المتطورة لتفرض تهديدا خطيرا وحقيقيا على دولة مثل الولايات المتّحدة الأمريكية على سبيل المثال[1].

2. تمتّع المهاجم بأفضلية واضحة: في حروب الإنترنيت يتمتع المهاجم بأفضلية واضحة وكبيرة على المدافع، فهذه الحروب تتميز بالسرعة والمرونة والمراوغة، وفي بيئة مماثلة يتمتّع بها المهاجم بأفضليّة، من الصعب جدا على عقليّة التحصّن لوحدها أن تنجح، فالتحصين بهذا المعنى سيجعل من هذا الطرف عرضة لمزيد من محاولات الاختراق وبالتالي المزيد من الضغط.

3. فشل نماذج "الردع" المعروفة: يعد مفهوم الردع الذي تمّ تطبيقه بشكل أساسي في الحرب الباردة غير ذي جدوى في حروب الإنترنيت، فالردع بالانتقام أو العقاب لا ينطبق على سبيل المثال على هذه الحروب، فعلى عكس الحروب التقليدية حيث ينطلق الصاروخ من أماكن يتم رصدها والرد عليها، فإنه من الصعوبة بمكان بل ومن المستحيل في كثير من الأحيان تحديد الهجمات الإلكترونية ذات الزخم العالي.

بعض الحالات قد تتطلّب أشهرا لرصدها، وهو ما يلغي مفعول الردع بالانتقام وكثير من الحالات لا يمكن تتبع مصدرها في المقابل، وحتى إذا تم تتبع مصدرها وتبين أنها تعود لفاعلين غير حكوميين، فانه في هذه الحالة لن يكون لديهم أصول أو قواعد حتى يتم الرد عليها.

4. المخاطر تتعدى استهداف المواقع العسكرية: لا ينحصر إطار حروب الإنترنيت باستهداف المواقع العسكرية، فهناك جهود متزايدة لاستهداف البنى التحتية المدنية والحسّاسة في البلدان المستهدفة، وهو أمر أصبح واقعيا في ظل القدرة على استهداف شبكات الكهرباء والطاقة

---

[1]- مونتغمري، الحرب عبر التاريخ، ترجمة فتحي نسيب نمر، مكتبة الانجلو مصرية، مصر، 1967، ص 59.

و يرجى مراجعة، الموقع التالي : http://www.wired.comو أيضا، يحيى اليحياوي، الإرهاب والحروب الإعلامية الأولى ،جريدة العلم،2002 ،ص1،كذلك حرب المعلومات ومستقبل التجسس، قراءات استراتيجية، مركز الدراسات السياسية والاستراتيجية، ورد في/ http://www.ahram.org وايضا: جلال المندلاوي، ماذا يدور خلف السور العظيم، مجلة خالد العسكرية، تقارير،2004، ص ص1-2 .http: www.islamonlin.net.

وشبكات النقل والنظام المالي والمنشآت الحساسة النفطية أو المائية أو الصناعية، بواسطة فيروس يمكنه إحداث أضرار مادّية حقيقية تؤدي إلى انفجارات أو دمار هائل.

كما شاعت في السنوات الأخيرة طائفة جديدة من الجرائم التي تستهدف المعلومات وبرامج الحاسوب، كالدخول غير المصرح به إلى أنظمة الحاسوب والشبكات، والاستيلاء على المعلومات أو إتلافها عبر تقنيات الفيروسات وغيرها من وسائل التدمير المعلوماتي أو جرائم قرصنة البرمجيات والاعتداء على حقوق الملكية الفكرية لمؤلفيها وجهات إنتاج هذه البرامج

وشاعت أيضاً الجرائم التي تستخدم الحاسوب وشبكات الاتصال كوسيلة لارتكاب أنشطة إجرامية تقليدية كالاحتيال عبر الحاسوب والتزوير باستخدام التقنيات الحديثة، كما في جرائم توزيع المحتوى غير القانوني والضار عبر مواقع الإنترنت وجرائم المقامرة والأنشطة الإباحية عبر الإنترنت أو استثمار مواقع الإنترنت كمخازن للبيانات الجرمية ومواضع لتنسيق أنشطة الجريمة المنظمة وجرائم غسيل الأموال الإلكترونية[1].

وفي خضم هذا النشاط الإنساني عبر الشبكة المعلوماتية برزت أهمية هذا البحث وهذا خاصة عندما عليها المشرع الجزائري بقانون رقم 15-2004 المؤرخ في 10نوفمبر2004[2]من قانون العقوبات في القسم السابع تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات وذلك في المادة 394الى المادة 394مكرر7 .

[1]- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية،القاهرة،ط1، 1992م، ص 15 ،كذلك حسن طاهر دوود، جرائم نظم المعلومات ،أكاديمية نايف العربية للعلوم الأمنية،ط1،الرياض،2000 ص 23، كذلك محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994، ص 80.

[2]- قانون رقم 04-15 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966والمتضمن قانون العقوبات،ج.ر.71.

المطلب الثاني : العدوان على البيئة المعلوماتية

لقد أصبح العالم يعيش ثورة هائلة في مجال المعلومات والاتصالات أتاحت للبشر قدراً هائلاً من المعرفة لم يكن متاحاً من قبل، كما وفَّرت هذه التقنية الجديدة فرصاً للمؤسسات والشركات والمصارف والحكومات، لتقديم خدماتها بشكل غير مسبوق.

وإذا كان ذلك هو الوجه المضيء لهذه التقنية، فإن الوجه الآخر تمثل في إمكانية العدوان والاختراق وممارسة الإتلاف والتخريب والتجسس، الأمر الذي فرض ضرورة توفير قدر من الحماية يتناسب مع مستوى أهمية المعلومات في البيئة الرقمية.[1]

وبما أن هذه البيئة لها رواد عديدون جدا، وجد بعض المجرمين التقنيين في البيئة التقنية مرتعا خصبا لهم، وخصوصا أن طبيعة هذه البيئة توفر لهم الكثير من الضمانات التي تدعوهم إلى اعتقاد صعوبة الوصول إليهم أو إلى البرمجيات التي يستخدمون، وكما هو معروف إن الجريمة سابقة لوجودها على وجود القانون، فإن التشريعات المختلفة ما زالت متخلفة عن مواكبة السرعة والتطور المضطرد الذي يسير به المجرمون، إلا أن هذه التشريعات متفاوتة في مقدار الحماية التشريعية والتغطية القانونية الخاصة لمواكبة الجريمة فبعضها يملك أسسا قانونية خاصة حول مثل هذا النوع من الجرائم ومتطورة بشكل مستمر حيث يتم تعديلها كلما ظهرت مستجدات تستوجب ذلك، ولكن بعضها الآخر لا يملك في الأصل تشريعات ناظمة لمثل هذا النوع من الجرائم.

الفرع الأول : تعريف الجريمة الالكترونية

إن التنقير في الوثائق التي تعالج جرائم الحاسوب، يُظهر أن التعريفات التي قد صِيغت لبيانِ حدودها، قد عانت من عمليات إعادة صياغة لحدودها أكثر من مرة على يد مشرعيهم، بسبب التغيرات المتسارعة في ميدان تقنيات المعلوماتية، بَيدَ أن أكثر التعريفات قَبولاً في هذا المضمار،

[1]- علي بن ضبيّان الرشيدي، العدوان على البيئة المعلوماتية خطورته ومواجهته، مجلة كلية الملك خالد العسكرية، العدد 81،2005.،متوفر على الرابط التالي : www.alyaseer.net/vb/showthread.php?t=7703

هو الذي يعتبرها **فعلاً غير مشروع، يوظِّف المعرفة العلمية السائدة في ميدان تقانة الحاسوب والمعلوماتية؛ لاقتراف إساءة أو هجوم على الغير**[1].

و من أجل مفهوم شامل للجريمة لا بد من تعريفها من الجانب الفني أو التقني و من الجانب الفقهي و بيان أنواعها .

أ- تعريـــــف الجريمة الإلكترونية من الجانب الفني.

الجريمة الالكترونية عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي[2]

- يعرفها أحمد صياني : بأنها تصرف غير مشروع يؤثر في الأجهزة و المعلومات الموجودة عليها [3]
- وهذا التعريف يعتبر جامع مانع من الناحية الفنية للجريمة الالكترونية، حيث انه لارتكاب الجريمة، [4]يتطلب وجود أجهزة كمبيوتر زيادة على ربطها بشبكة معلوماتية ضخمة .

ب- التعريف الفقهي الجريمة الالكترونية .

تعرف بأنها " :مجموعة من الأفعال و الأنشطة المعاقب عليها قانونا و التي تربط بين الفعل الإجرامي و الثورة التكنولوجية ".

و بمعني آخر هي :" نشاط جنائي يمثل اعتداء على برامج الحاسب الآلي" .[5]

قسم الفقهاء في الدول العربية الجريمة المعلوماتية(الجرائم الالكترونية) في جانبها القانوني إلى:

---

[1] -Thomas M., The Growing Threat Of Computer Crime, DETCTIVE -US Army, Summer 1990, pp.6-11.

[2] – عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية، مصر 2002 ، ص 01.

[3] - www.anaharonline.com

[4]– الجريمة عموما هي فعل غير مشروع صادر عن إرادة جنائية يقرر لها القانون عقوبة أو تدبيرا احترازيا، ولقد اشتقت كلمة الجريمة في اللغة من الجُرم وهو التعدي أو الذنب ، وجمع الكلمة إجرام وجروم وهو الجريمة، وقد جرم يجرم واجترم وأجرم فهو مجرم وجريم أنظر الشيخ أبو الفضل جمال الدين محمد بن مكرم ابن منظور، لسان العرب، دار صاد، بيروت، ص ص 604 -605 .

[5] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 06.

أولا :الجرائم التي تستعمل فيها الوسائل التكنولوجية من أجل القيام بالفعل الإجرامي مثل: تزوير أموال عن طريق الماسح الضوئي، فهذا النوع له إطاره القانوني في معظم التشريعات العالمية .

ثانيا : الجرائم التي تستخدم التقنية الحديثة لارتكابها، حيث عن طريق شبكة الانترنيت يمكن إنشاء مواقع إباحية، أو انضمام إلى مجموعات إرهابية، أو المتاجرة بالسلاح أو المخدرات ن أو المتاجرة بأسرار الناس عن طريق خرق مواقعهم أو جهاز الكمبيوتر أو انتحال الشخصية باستخدام بطاقات الائتمان.[1]

و هذا النوع من الجرائم هو الذي يهمنا، فوسط عالم إفتراضي رقمي فرضه التطور التكنولوجي قد يجد الشخص نفسه وسط تيار جارف، تختلس فيه أمواله من دون أي دليل ملموس، فمن خلال كل ما ذكر يمكن تعريف الجريمة الإلكترونية بأنها سلوك غير مشروع أو غير أخلاقي أو غير مسرح به.

وبهذا يمكن القول إن جرائم الانترنت هي امتداد لما عرف بجرائم الحاسوب ، والمقصود بجرائم الحاسوب: " كل عمل إجرامي، غير قانوني، يرتكب باستخدام الحاسوب كأداة أساسية، ودور الحاسوب في تلك الجرائم قد يكون هدفا للجريمة أو أداة لها."

وعندما ظهرت شبكة الانترنت ودخلت جميع المجالات كالحاسوب، بدءا من الاستعمال الحكومي ثم المؤسساتي والفردي، كوسيلة مساعدة في تسهيل حياة الناس اليومية، انتقلت جرائم الحاسوب لتدخل فضاء الانترنت كأداة أساسية، وكما هو الحال في جرائم الحاسوب، كذلك جرائم الانترنت قد تكون الانترنت هدفا للجريمة أو أداة لها.

والمقصود بجرائم الإنترنت[2] في نظر مكتب الشكاوى ضد جرائم الانترنت، المسماة أيضاً الجرائـــم السيبرنـــية، هو:" أي نشاط غير مشروع ناشئ في مُكوّن أو أكثر من مكونات

---

[1] - Francillon, Les crimes inormatiques et d'autres crimes dans le domaine de la technologie informatique en france Rev. int.pén, 1990, vol 64, p 293.

[2]– وجدير بالذكر أن هناك عدة تعريفات للجريمة المعلوماتية ؛ ومن هذه التعريفات :

- ماذهب إليه خبراء متخصصون من بلجيكا من أن (جريمة الكمبيوتر) هي : (كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية) . (الأستاذ عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – دراسة مقارنة – منشورات الحلبي الحقوقية ، بيروت، 2003 ، ص 32) .
- في حين يذهب الفقيه الفرنسي الأستاذ (Massa) إلى أن المقصود بالجريمة المعلوماتية (الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح. راجع: www.arablaw/Download cyber crimes_General,doc ،يونس عرب، موسوعة

الإنترنت، مثل مواقع الإنترنت، وغرف المحادثة، أو البريد الإلكتروني، ويمكن أن تشمل أيضاً أي أمر غير مشروع، بدءاً من عدم تسليم البضائع أو الخدمات، مروراً باقتحام الكمبيوتر (التسلل إلى ملفات الكمبيوتر)،وصولاً إلى انتهاك حقوق الملكية الفكرية، والتجسس الاقتصادي)سرقة الأسرار التجارية)، والابتزاز على الإنترنت، وتبييض الأموال الدولي، وسرقة الهوية، وقائمة متنامية من الجرائم الأخرى التي يسهلها الإنترنت."[1]

وهناك تعريفات انطلقت من وسيلة ارتكاب الجريمة، من بينها تعريف الأستاذ: جون فورستر، والأستاذ «*Eslied ball*»[2]الذي جاء فيه أنها: "كل فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"، ويعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية أنها : "الجريمة التي تلعب فيها البيانات الكمبيوترية و البرامج المعلوماتية دورا رئيسيا "،وقد لاقت هذه التعريفات انتقادات كون تعريف الجريمة يجب أن ينصب على السلوك المكون لها و ليس فقط على الوسيلة التي تم بها لأنه «ليس لمجرد أن الحاسب قد استخدم في جريمة ان نعتبرها من الجرائم المعلوماتية » .

القانون وتقنية المعلومات دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، منشورات إتحاد المصارف العربية، ط1، ص 213 ،علي عبد القادر القهوجي، المرجع السابق، ص 172 .

- في حين أن منظمة التعاون الاقتصادي والتنمية OCDE وضعت التعريف التالي للجريمة المعلوماتية من أنها : كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية، راجع هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الكاتبة،مصر،1995، ص 34. أحمد خليفة الملط، الجرائم المعلوماتية، الفكر الجامعي،الإسكندرية ،ط2، 2006، ص 83 وما بعدها.

[1] – جاء ضمن القرار الوزاري السعودي رقم 79 المؤرخ في 1428/03/07ه،المتضمن الموافقة على نظام مكافحة جرائم المعلوماتية، تعريف لهذه الجرائم بأنها " كل فعل يرتكب متضمنا استخدام الحاسب الالي أو الشبكة المعلوماتية، بالمخالفة لاحكام هذا التنظيم".

[2] –Tom forester, Essential proplems to HigTech Society First MIT Pres edition, Cambridge, Massachusetts, 1989, P 104.

وقد اعتمدت شخصية الفاعل كمعيار لإعطاء تعريف لهذه الجرائم، فقد اعتبرت سمة الدراية والمعرفة التقنية، كأساس لهذا[1].

ويجب الإشارة إلى أن جرائم الانترنت لا تقع على ماديات وإنما على معنويات الكمبيوتر وما يحتويه من معلومات أو ما يحوله، حتى لو كانت النتائج المحققة أو الخسائر المترتبة تتجسد في شكل مادي في كثير من الأحوال، لذلك فهو يجعل منها جرائم تخرج عن المألوف باختلافها عن الجرائم التقليدية المعروفة ضمن القسم الخاص لقانون العقوبات والتي تنطبق عليها القواعد الواردة في القسم العام منه، وهذا ما استوجب معه على الدول ان تسن تشريعات تعرف من خلالها الأفعال المجرمة، وتحددها مقابل وضع العقاب المناسب لها .

في حين لم يعرف تعديل قانون العقوبات الجزائري بموجب القانون رقم 15/04 المؤرخ في 2004/11/10 جرائم الانترنت، بل اكتفى بالعقاب على بعض الأفعال، تحت عنوان « الجرائـــــم الماسة بنظـــــام المعالجـــــة الآلية للمعطيات » .

وقد عرفت جرائم الانترنت بحسب أشكالها، فنجد أن لكل شكل تعريف خاص به، نظرا لطريقة ووسيلة ارتكابه، أو الهدف منه أو محله، وهو ما سيتعرض له ضمن أنواع جرائم الانترنت.

الفرع الثاني : الطبيعة القانونية للجريمة المعلوماتية وخصوصية مجالاتها.

يتمحور الحديث عن الطبيعة القانونية للجريمة الإلكترونية وخصوصية مجالاتها حول الوضع القانوني للبرامج و للمعلومات[2] ، هل للمعلومات قيمة في ذاتها؟ أم لها قيمة ما تمثل في أنها

[1] –كما يظهر من التعريف الذي تبنته وزارة العدل الأمريكية من دراسة وضعها معهد ستانفورد للأبحاث عام 1979و الذي جاء فيه :"أنها أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها" وكذلك تعريف David Thomsonبأنها : 'أية جريمة يكون مطلوب لاقترافها ان تتوافر لدى فاعلها معرفة بتقنية الحاسب ' الا انه تعريف قاصر حسب رأيي كون هناك بعض الفاعلين لا يملكون المعرفة اللازمة بالتقنية وقد يكون جهلهم هذا هو السبب في ارتكاب هذه الجرائم ، كما قد يتعدد الفاعلين من محرض ومساهم فلا يكون لواحد منهم أي علم بوسائل المعلوماتية.

[2]– مفتاح بوبكر المطردي، الجريمة الالكترونية و التغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، جمهورية السودان ،المنعقد في 23-25 / 9 / 2012 ، ص16.

مجموعة مستحدثة من القيم؟ ويرجع هذا التساؤل إلى ما إذا كانت المعلومات لها قيمة وتعتبر من ثمة من قبيل القيم القابلة للإستثناء، إذن يمكن الاعتداء عليها بأي طريقة كانت .

البند الأول : الطبيعة القانونية للجريمة المعلوماتية

إنقسم الفقه إلى اتجاهين:

الأول: يرى أن المعلومات لها طبيعة من نوع خاص.

الثاني: يرى أن المعلومات ما هي إلا مجموعة مستحدثة من القيم، ولنرى ذلك بشيء من التفصيل.

أ- المعلومات لها طبيعة قانونية من نوع خاص.

يرى هذا الاتجاه التقليدي، أن المعلومات لها طبيعة من نوع خاص وذلك انطلاقا من حقيقة مسلم بها هي أن وصف القيمة يضفي على الأشياء المادية وحدها بمعنى آخر أن الأشياء التي توصف بالقيم هي الأشياء التي تقبل الاستحواذ عليها، وبمفهوم المخالفة وباعتبار أن المعلومات لها طبيعة معنوية، فلا يمكن والحال كذلك اعتبارها من قبيل القيم القابلة للاستحواذ عليها إلا في ضوء حقوق الملكية الفكرية.

وأيا ما كان الأمر، فإن الأمر مستقر بصدد وجود خطأ عند الاستيلاء على المعلومات أو معلومات الغير، ولذلك فقد حاول هذا الاتجاه أن يحمي هذه المعلومات بدعوى المنافسة غير المشروعة، وذلك استنادا إلى حكم محكمة النقض الفرنسية: "إن الغاية من دعوى المنافسة غير المشروعة هي تأمين حماية الشخص الذي لا يمكنه أن ينتفع بأي حق استثنائي".[1]

ب- المعلومات مجموعة مستحدثة من القيم.

يرى هذا الاتجاه الحديث، أن المعلومات ما هي إلا مجموعة مستحدثة من القيم، ويرجع الفضل في ذلك إلى الأستاذين *Catala*و*Vivaut* [2] إلى قابلية المعلومات للاستحواذ كقيمة واستقلالا عن دعايتها المادية.

---

[1]- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1994 ، ص 180.

[2] - Catala, la propriété de l'information et masse , la délinquance informatique aspects de droit pénal international,p97.

أن المعلومات تقوم وفقا لسعر السوق متى كانت غير محظورة تجاريا، وأنها تنتج بصرف النظر عن دعامتها المادية عن عمل من قدمها وأنها ترتبط بمؤلفها عن طريق علاقة قانونية، تتمثل في علاقة المالك بالشيء الذي يملكه وهي تخص مؤلفها بسبب علاقة التبني التي تجمع بينهما.

إن هذا الرأي يؤسس على حجتين لإعطاء وصف القيمة على المعلومات:

الأولى: قيمة المعلومات الاقتصادية، والثانية وجود علاقة تبني تجمع بين مؤلفها، أما الأستاذ *Vivaut* فيؤسس ذلك على حجتين أيضا، الأولى مستوحاة من بلا فيول روريبير وهي أن فكرة الشيء أو القيمة لها صورة معنوية، وأن نوع محل الحق يمكن أن ينتمي إلى قيمة معنوية ذات الطابع الإقتصادي، وأن تكون جديرة بحماية القانون،

وأما الحجة الثانية: فيقدم لنا الأستاذ فيفانتي نفسه حيث يرى إن كل الأشياء المملوكة ملكية معنوية، والتي يعترف بها القانون وترتكز على الاعتراف بأن للمعلومات قيمة، عندما تكون من قبيل البراءات أو الرسومات أو النماذج أو التحصيلات الضرورية أو حق المؤلف، والإنسان الذي يقدم ويكشف ويطلع الجماعة على شيء ما بصرف النظر عن الشكل أو الفكرة، فهو يقدم لهم معلومات بمعنى الواسع ولكنها خاصة به، ويجب - - أن تعامل هذه الأخيرة بوصفها قيمة تصبح محلا لحق، فلا توجد ملكية معنوية بدون الإقرار بالقيمة المعلوماتية، ولذلك فهو يرى أن القيمة المعلوماتية ليست بالشيء المستحدث إذ أنها موجودة من قبل في مجموعة ما.

بصفة عامة تعد المعلومات محلا للجريمة المعلوماتية فهي الموضوع الذي يرد عليه النشاط الإجرامي في جرائم المعلوماتية، لذلك هذه المعلومات لقيت دراسة وبحثا مستفيضا من قبل المتخصصين في مجال علوم الحاسبات الآلية والإجرام المعلوماتي، وهو ما أدى إلى وجوبية فهمها فهما كاملا لكي يتسنى حمايتها على نحو صحيح[1].

البند الثاني : خصوصية مجالات الجريمة المعلوماتية:

رغم أن البحث يدور حول نطاق تطبيق نصوص القانون الجنائي، إلا أنه وكما يبدو أننا بصدد ظاهرة إجرامية ذات طبيعة متميزة، تتعلق غالبا بما يسمى بالقانون الجنائي المعلوماتي.

[1] -Abdelkrim Daho Idrissi, La sécurité de la société de l'information entre les institutions sécurutaires civiles et para sécuritaire, Tome I: L'expérience Français 1ere édition 2003, casablanca P 78.

ففي معظم حالات ارتكاب الجريمة المعلوماتية، نجد أن الجاني يتعمد التدخل في مجالات النظام المعلوماتي المختلفة ومنها:

أ – مجال المعالجة الإلكترونية للبيانات:

يتدخل الجاني من خلال ارتكاب الجريمة المعلوماتية في مجال المعالجة الإليكترونية الآلية للبيانات، سواء من حيث تجميعها أو تجهيزها حتى يمكن إدخالها إلى جهاز الحاسوب وذلك بغرض الحصول على معلومات.[1]

ب – مجال المعالجة الإلكترونية للنصوص والكلمات الإلكترونية.

يتدخل الجاني في مجال المعالجة الإلكترونية للنصوص والكلمات، وهي طريقة أتوماتيكية تمكن مستخدم الحاسوب من كتابة الوثائق المطلوبة، بدقة متناهية بفضل الوسائل التقنية الموجودة تحت يده، وبفضل إمكانيات الحاسوب، من تصحيح وتعديل ومحو وتخزين وطباعة واسترجاع ،وهي إمكانيات لها علاقة وثيقة بارتكاب الجريمة.[2]

---

[1]– محمد علي العريان ، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر،طبعة 2004،ص48.

En France, l'article 323-1 du nouveau code pénal, sanctionne l'intrusion dans un système automatisé. L'alinéa 2 de cet article aggrave même la sanction lorsque l'intrusion a eu pour effet de falsifier ou de supprimer des données.
Andrieu Eric, « Internet et la protection des données personnelles », *LEGICOM* 1/2000 (N° 21-22) , p. 155-166 URL : www.cairn.info/revue-legicom-2000-1-p-155 .

[2] – يحمي المشرع الفرنسي سرية البيانات الإلكتروني من خلال المواد 226–16 إلى 226-24من قانون العقوبات التي تجرم المساس بسرية المعلومات المخزنة، وقد كان المشرع الفرنسي ينص بموجب القانون رقم 87–17 الصادر في 6 يناير سنة 1978الخاص بالمعلوماتية والباقات والحرية ، على تجريم إستخدام المعلومات المسجلة في غير الأغراض التي وضعت من أجلها في الحاسب الألي، كما كان يجرم أيضا جريمة إفشاء هذه المعلومات،كما كان ينص بموجب قانون 19 لسنة 1988 على تجريم محو البيانات الإلكترونية كلها أو بعضها أو تعديلها ، يرجع تجريم التزوير في المستندات الإلكترونية إلى ما تقدم به أحد نواب البرلمان الفرنسي ، في 5 أغسطس سنة 1986 من اقتراح يرمي إلى إدخال بعض التعديلات على جريمة التزوير في المحررات المنصوص عليها في قانون العقوبات لتشمل أيضا تغيير الحقيقة في البيانات الإلكترونية ، غير أن هذا الإقتراح لم يؤخذ به، ورأي مجلس الشيوخ إعتبار تزوير المستندات الإلكترونية جريمة مستقلة عن جريمة التزوير في المحررات. وقد صدر القانون رقم 88–19 في 5 يناير سنة 1988 الذي انطوى على تجريم صورتين: الأولى هي تزوير المستندات المعالجة آليا أيا كان شكلها إذا كان من شأنها الإضرار بالغير (المادة 462–5)، والصورة الثانية فهي الخاصة باستعمال المستندات المزورة سالفة الذكر ،المادة 462. 6 – وبمناسبة إستبدال قانون العقوبات الفرنسي سنة 1994 بالقانون القديم ألغى الشارع الفرنسي نص المادتين سالفتي الذكر، وأخذ بإقتراح تعديل نص جريمة التزوير الأصلية ليستوعب أيضا المستندات الإلكترونية، وذلك بتعديل نص المادة 441–1 من قانون العقوبات.

- La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, plus connue sous le nom de loi informatique et libertés
- La loi Godfrain du 5 janvier 1988, ou Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, est la première loi française réprimant les actes de criminalité informatique et de piratage, Nommée d'après le député RPR Jacques Godfrain.

كما أن للجرائم المعلوماتية التي تنصب على المعلومات وتقنيتها خصائص وسمات تميزها عن غيرها من الجرائم التقليدية الأخرى، فالجريمة المعلوماتية باعتبارها جريمة مستحدثة كانت و لا زالت تثير ضجة في الاوساط الفقهية بخصوص تحديد ماهيتها والافعال الاجرامية التي تدخل في نطاقها أي أنواعها.

الفرع الثالث : أنواع جرائم الانترنت

تنشأ الجريمة في الفضاء الافتراضي عبر اعتماد مبدأ الاختراق المعلوماتي لحدود نظام من النظم السائدة في هذا الفضاء، وذلك لمباشرة زمرة من الأنشطة غير المشروعة، والتي تشمل:

1. سرقة أو استغلال البرمجيات، دون وجود إِذْنٍ مسبق بذلك.
2. الدخول إلى ساحة النظم الحاسوبية، وشبكات الهواتف بأنواعها، لاستغلال الموارد المتاحة فيها.
3. التلاعب بالبيانات، وتغيير محتوى ملفات الغير، أو إتلافها، أو نقلها، ونشرها.
4. كسر الشفرات البرمجية للبرمجيات التطبيقية المحميَّة، أو الملفات المشفرة لأغراض الحفاظ على سريَّة محتوياتها لأي سبب كان.
5. مباشرة أعمال قرصنة على الخدمات العامة والخاصة المتاحة على الشبكات الحاسوبية.
6. زج الفيروسات الحاسوبية، أو برمجيات مشابهة؛ لإحداث خلل في أداء المنظومة، أو إتلاف مواردها المعلوماتية[1].
7. تهريب موارد معلوماتية من نظام إلى آخر.
8. ممارسة أنشطة إرهابية بمختلف مستوياتها إزاء البنى التحتية للدول، أو المؤسسات أو الأفراد.

[1]- حسن مظفر الرزو، القانون العراقي والمفاهيم المعلوماتية لجرائم الفضاء الافتراضي بالحاسوب، مؤتمر القانون العراقي وتطور المجتمع، كلية الحدباء الجامعة، 24-2001/3/25، الموصل، جمهورية العراق، ص 11.

تنشأ هذه الجرائم داخل الفضاء الافتراضي الحاسوبي، وبعد تحقيق اختراق معلوماتي لبنية أحد النظم، فتباشر الخطوات التي تهدف إلى تحقيق أهدافها غير المشروعة، وقد صنفها معهد العدالة القومي بالولايات المتحدة الأمريكية عام 1985 بحسب علاقتها بالجرائم التقليدية، فاعتبر أن الصنف الأول يتمثل في الجرائم المنصوص عليها في قانون العقوبات متى ارتكبت باستعمال الشبكة، والصنف الثاني تضمن دعم الأنشطة الإجرامية ويتعلق الأمر بما تلعبه الشبكة من دورفي دعم جرائم غسيل الأموال، المخدرات ،الاتجار بالأسلحة ،واستعمال الشبكة كسوق للترويج غير المشروع في هذه المجالات ،بينما يتعلق الصنف الثالث بجرائم الدخول في نظام المعالجة الآلية للمعطيات[1]، وتقع على البيانات والمعلومات المكونة للحاسوب وتغييرها أو تعديلها أو حذفها مما يغير مجرى عمل الحاسوب ، بينما الصنف الرابع فتضمن جرائم الاتصال وتشمل كل ما يرتبط بشبكات الهاتف، وما يمكن أن يقع عليها من انتهاكات باستغلال ثغرات شبكة الأنترنت، وأخيرا صنف الجرائم المتعلقة بالاعتداء على حقوق الملكية الفكرية ويتمثل في عمليات نسخ البرامج دون وجه حق، وسرقة حقوق الملكية الفكرية المعروضة على الشبكة دون إذن من صاحبها بطبعها وتسويقها واستغلالها باي صورة طبقا لقانون حماية الملكية الفكرية .

في حين عددت وزارة العدل الأمريكية عام 2000 في معرض تحديدها للمكاتب المحلية لإنفاذ القـــــــانون الفيدرالي المتعلق بجرائم الكمبيوتر دون أن تقوم بتصنيفها وهي:

---

[1] – وما يلاحظ على التشريعات السابقة أنها لم تورد تعريف لنظام المعالجة الآلية للمعطيات، مكتفية بوضعه محلا للحماية، رغم انه الشرط الأولي اللازم تحققه للبحث عن توفر أركان الجريمة من عدمه، وقد عرفت الاتفاقية الدولية للإجرام المعلوماتي النظام المعلوماتي في المادة الثامنة منها على انه:

Système informatique désingne tout dispositif isole ou ensemble de dispositifs, interconnectes ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme un traitement automatisé de donnée .

بينما عرفه الفقه الفرنسي أنه : "كل مركب يتكون من وحدة او وحدات معالجة تتكون كل منها من الذاكرة و البرامج و المعطيات و أجهزة الإدخال و الإخراج و أجهزة الربط و التي يربط بينها مجموعة العلاقات التي عن طريقها تتحقق نتيجة معينة و هي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية" ،فهو يتكون من عنصرين:

1– مركب : يتكون من عناصر مادية و معنوية مختلفة تربط بينها نتيجة علاقات توحدها نحو تحقيق هدف محدد.

2– ضرورة خضوع النظام لحماية فنية : حفاظا على خصوصية البيانات المتناقلة عبر الشبكات ، يوجد ثلاث أنواع من الأنظمة : أنظمة مفتوحة للجمهور، أنظمة قاصرة على أصحاب الحق و بدون حماية فنية أنظمة قاصرة على أصحاب الحق و تتمتع بالحماية الفنية، و النوع الثالث فقط هو المتمتع بالحماية الجنائية، و لكن التشريعات لم تشرط وجوده،تماشيا مع الرأي الراجح من الفقه ذلك أن الحماية الجنائية تمتد لتغطي أنظمة المعالجة الآلية للمعطيات سواء كانت محمية و غير محمية.

السطو على بيانات الكمبيوتر، الاتجار بكلمات السر، حقوق الطبع، سرقة الأسرار التجارية، تزوير الماركات، تزوير العملة، الصور الفاضحة الجنسية، واستغلال الأطفال، الاحتيال، الإزعاج عن طريق شبكة الانترنت، التهديد، الاتجـــار بالمتفجرات أو الأسلـــحة النـــارية أو المخدرات وغسيل الأموال عبر الشبكة .

بينما يذهب الاتجاه العالمي الجديد خاصة ما ورد بالاتفاقية الأوربية لعام2001 لجرائم الكمبيوتر والانـــــترنت فقد قسمت هذه الجرائم إلى:

البند الأول: الجرائم الماسة بنظام المعالجة الآلية للمعطيات

إن الصورة الغالبة لتحقيق غاية المجرم المعلوماتي[1] في نطاق الشبكة تتمثل في فعل الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه بدون إذن، ومن ثم قيام الجاني بارتكاب فعله الذي قد يكون مجرم فيشكل احد أنواع جرائم الانترنت، أولا يكون كذلك ،وتنصب هذه الجرائم على المعلومة، باعتبارها العنصر الأساسي المكون للبرامج والبيانات والمعلومات الموجودة بالحاسب الآلي، ويشترط أن تكون المعلومة خاصة قاصرة على فرد أو افراد دون غيرهم، تبلغ حد من الأهمية به يستأثرون بها و تشكل لديهم عامل مهم، في أدائهم يميزهم عن غيرهم ،وتحمل ابتكارا أو إضافة يكونوا هم مصدرها[2].

---

[1] – إن المجرم المعلوماتي ،هو شخص يختلف عن المجرم العادي فلا يمكن أن يكون هذا الشخص جاهلا للتقنيات الحديثة المعلوماتية ،فهناك ثلاثة أنواع بارزة لهؤلاء المجرمين أو بالأحرى ثلاث تصنيفات.

أولا : ألهاكرز و هو فضولي في بعض الأحيان يكون عادة من المراهقين المولعين بالشبكة العنكبوتية حيث يدفعهم الفضول إلى معرفة كلمة سر بعض الأشخاص و الدخول على نظامهم المعلوماتي، كما يقولون بعض الكتاب أنهم لا يشكلون خطر.

ثانيا : الكراكرز : هم أشخاص متسللون يتابعون عن كثب آخر الأخبار و برامج الحماية المنية للأجهزة و المعلومات،إلى حد أنهم ينشئون النوادي لتبادل المعلومات

وهؤلاء المجرمون يستطيعون الاحتياز الأمني، لمختلف المواقع بقصد التخريب و الاختلاس و التزوير ، و من أهم هذه الجماعات هي جماعة القراصنة الروس الذين يعتبرون لأفضل على الإطلاق ، ففي استطلاع للرأي أكد أنهم متمكنون من الخرق الآلي للأنظمة بنسبة 82 بالمائة حتى أن الولايات المتحدة الأمريكية وجهت الاتهام لروسيا بمحاولة سرقة برامج نظام تمركز الصواريخ العالي ، لأن بعض الهاكرز الروس قاموا بمهاجمة موقع الأطلسي، وللعلم فإن هناك بعض المجلات التي تصدر مهمتها الدفاع عن هذه الفئة التي لا تعتبرها مجرمة بل تقول أنهم يبلون حسنا، و أنهم يكتشفون الثغرات الأمنية في الأنظمة المعلوماتية.

ثالثا : مصمموا مواقع إرهابية و إباحية و حتى الوهمية لجلب الأفراد المهتمين بالتسوق مثلا من اجل معرفة شفرة بطاقة الائتمان، و استعمالها لحاجات شخصية و لكن الملاحظ ـــأن هذه الفئة اقل خبرة من الفئة السابقة الذكر.

D.M. Trent , "Hackers , Crackers , and Trackers , American Legion Magazine ,February , 1997 , p34 .

[2] – عبد القادر الفتوح، الانترنت للمستخدم العربي ، مكتبة العربي، الرياض، 2001، ص 11 .

ولقد تضمن قانون الاحتيال وإساءة استخدام الكمبيوتر"*CFAA*"[1] لعام 1996 الصادر عن المشرع الأمريكي، تجريم الدخول غير المشروع الى أنظمة المعلوماتية، معددا صور هذه الجريمة من خلال المادة 1030 من هذا القانون وهي:

أ- الدخول العمدي الى جهاز الحاسوب بدون تصريح أو تجاوزا للتصريح الممنوح له، ويحصل بأية وسيلة على معلومات تقررت من قبل حكومة الولايات المتحدة بناء على أمر تنفيذي وتصريح برلماني يتطلب الحماية، ضد الإفشاء غير المخول به لأسباب تتعلق بالدفاع الوطني أو العلاقات الأجنبية.

ب- الوصول عمدا الى الحاسوب بدون ترخيص، أو تجاوز الترخيص الممنوح بقصد الحصول على معلومات واردة في سجل مالي بمؤسسة مالية، أوان تشمل هذه المعلومات المتضمنة في ملف وكالة أو معلومات من أي حاسب محمي إذا تعلق بمحتوى اتصالات خارجية او بين الولايات.

---

[1] -CFAA : The *Computer Fraud and Abuse Act* was enacted by Congress in 1986 as an amendment to existing computer fraud law (18 U.S.C. 1030), which had been included in the Comprehensive Crime Control Act of 1984. It was written to clarify and increase the scope of the previous version of 18 U.S.C. 1030 while, in theory, limiting federal jurisdiction to cases "with a compelling federal interest-i.e., where computers of the federal government or certain financial institutions are involved or where the crime itself is interstate in nature." (see "Protected Computer", below). In addition to clarifying a number of the provisions in the original section 1030, the CFAA also criminalized additional computer-related acts. Provisions addressed the distribution of malicious code and denial of service attacks. Congress also included in the CFAA a provision criminalizing trafficking in passwords and similar items.
https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

The Act has been amended a number of times—in 1989, 1994, 1996, in 2001 by the USA PATRIOT Act, 2002, in 2008 by the Identity Theft Enforcement and Restitution Act, and in 2013 by the Aaron's Law Act. In January 2015 Barack Obama proposed expanding the CFAA Obama, Goodlatte Seek Balance on CFAA Cybersecurity

The president wants tougher penalties for hackers while easing punishment for 'insignificant conduct.' By Tom Risen :

http://www.usnews.com/news/articles/2015/01/27/obama-goodlatte-seek-balance-on-cfaa-cybersecrity.

ج- الوصول العمدي بدون ترخيص لأي حاسوب غير عام، يخص إحدى إدارات أو وكالات الولايات المتحدة، مخصص لاستعمال حكومة الولايات المتحدة، أو لم يكن مخصص لها ولكن استعمل من قبل أو لأجل حكومة الولايات المتحدة الأمريكية و كان ذلك التصرف مؤثرا على ذلك الاستعمال من قبل أو لأجل حكومة الولايات المتحدة .

د-الوصول لمعرفة وبقصد الغش الى الحاسوب محمي، بدون ترخيص أو بتجاوز الترخيص الممنوح له، وبأيه وسيلة تسهل نية الغش ويتحصل على أي شيء ذي قيمة، مالم يكن موضوع الغش والشيء المتحصل عليه يتوقف فقط على استخدام الحاسوب وان قيمة هذا الاستخدام لا تزيد عن 5000 دولار خلال فترة سنة.

وانتقد هذا القانون[1]، لانطوائه على الكثير من الغموض والقصور، يمكن للمجرمين تفادي تطبيق القانون عليهم، بإستخدام حاسبات وشبكات من خارج الولايات المتحدة والدخول الى أنظمة الحاسبات داخل الولايات المتحدة الأمريكية والاعتداء عليها او استخدام هذه الأنظمة ذاتها عن بعد للاعتداء على حاسبات تقع في دول أخرى.

في حين نجد ان المشرع الفرنسي، قد تناول جريمة الدخول غير المشروع او البقاء بدون صلاحية داخل نظام معلوماتي، من خلال المواد 1/323 إلى 3/323 مجرما فعل الدخول أو البقاء بطريق الغش في نظام المعالجة الآلية للمعطيات أو جزء منه، و فرق بين مجرد الدخول او البقاء ،و بين ما يترتب عن هذا الدخول أو البقاء من محو او تعديل في المعطيات المخزنة او إتلاف تشغيل هذا النظام.

و بالرجوع للمشرع الجزائري نجد انه، عاقب على جرائم أدرجها في القسم السابع مكرر من قانون العقوبات المعدل بالقانون 23/06 المؤرخ في 06/12/20 المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات بالمواد 394مكررالى 394 مكرر 7 مجرما من خلالها:

[1]- القانون الأمريكي المتعلق بالاحتيال وإساءة استخدام الكمبيوترCFAA لعام 1996،المادة 1030.

1. فعل الدخول أو البقاء عن طريق الغش في كل او جزء من منظومة المعالجة الآلية للمعلومات أو محاولة ذلك , او متى ترتب عنه تغيير معطيات المنظومة او حذف نظام التشغيل أو تخريبه.

2. الإدخال أو الإزالة بطريقة الغش لمعطيات في نظام المعالجة الآلية للمعلومات.

3. ـــالقيام عمدا وعن طريق الغش بتصميم او بحث او بتوفير، نشر، أو الاتجار بمعطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

4. حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان، المعطيات المتحصل عليها من إحدى الجرائم الخاصة بأنظمة المعالجة الآلية للمعطيات.

5. المشاركة في مجموعة او اتفاق بغرض الإعداد لجريمة من الجرائم المنصوص عليها الخاصة بأنظمة المعالجة الآلية للمعطيات.[1]

---

[1] – أما بالنسبة للتشريع الجزائري فقد احدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات و الجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات القانون رقم04-05 المؤرخ في 10 نوفمبر 2004.

* المادة 394 مكرر " يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من خمسين ألف إلى مائة ألف دينار كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظمة. و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة تكون العقوبة الحبس من 06 أشهر إلى سنتين و غرامة من خمسين ألف إلى مائة و خمسون ألف دينار"

المادة 394 مكرر1 " يعاقب بالحبس من 06 أشهر إلى 03 سنوات و بغرامة من 500.000 دج إلى 2000.000 كل من ادخل بطريقة الغش معطيات في نظام أو أزال او عدل بطريقة الغش المعطيات التي يتضمنها"

- المادة 394مكرر 2 " يعاقب بالحبس من شهرين إلى 03 سنوات و بغرامة من 1000.000 دج إلى 5000.000 دج كل من يقوم عمدا و عن طريق الغش بما يلي :

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

- المادة 394مكرر 3 " تضاعف العقوبة المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات اشد".
- المادة 394 مكرر 4 " يعاقب الشخص المعنوي الذي يرتكب احدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى المقرر للشخص الطبيعي"

البند الثاني : الجرائم المرتبطة بالمحتوى بالكمبيوتر "التزوير والاحتيال "

تعتبر من اكثر جرائم نظم المعلومات انتشارا [1]،فلا تكاد تخلو جريمة من جرائم نظم المعلومات، من شكل من اشكال تزوير البيانات، وتتم عملية التزوير بالدخول إلى قاعدة البيانات وتعديل البيانات الموجودة بها أو إضافة معلومات مغلوطة بهدف الاستفادة غير المشروعة من ذلك.

ومما لاشك فيه ان البدء التدريجي في التحول إلى الحكومات الإلكترونية، سيزيد من فرص ارتكاب مثل هذه الجرائم حيث سترتبط الكثير من الشركات والبنوك بالإنترنت مما يسهل الدخول على تلك الأنظمة من قبل محترفي اختراق الأنظمة وتزوير البيانات لخدمة اهدافهم الإجرامية، وجرائم التزوير ليست بالجرائم الحديثة، ولذا فانه لا تخلوا الأنظمة من قوانين واضحة لمكافحتها والتعامل معها جنائيا وقضائيا و" تكفي التشريعات الحالية لتجريمها وتحديد العقوبة عليها[2]"

- المادة 394 مكرر 5 " كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم و كان هذا التحضير مجسد أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها".
- المادة 394 مكرر6 " مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم على اغلاق المحل أو مكان استغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".
- المادة 394 مكرر 7 "يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذا القسم بالعقوبات المقررة على الجنحة ذاتها".

[1]- أضاف المشرع الجزائري في تعديله الأخير لقانون العقوبات ،قانون 04/15في القسم السابع من الكتاب الثالث من الباب الثاني من الفصل الثالث و الذي يشمل المواد 394 مكرر إلى المادة 394 مكرر 7 ، حيث ادمج المشرع الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و هذا ما نستخلص منه انه قد اعتبر المعلومات مالا من نوع خاص.

و لكن رغم ذلك فان المشرع قد اغفل في نصوصه بعض النقاط و هي:

- لم يتعرض للاعتداء على سير نظام المعالجة الآلية للمعطيات.
- لم يتعرض للتزوير المعلوماتي.

[2]- داود حسن طاهر، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض،2001، ص 67.

التّدليس والتزوير المعلوماتي

يعرف بالتّدليس المعلوماتي صنع أو تعديل المعطيات الإلكترونيّة أو فسخها أو إدخالها أو إعدامها، [1]إذا كان ذلك عن عمد، ومن شأنها أن تغيّر من حقيقة البيانات، وبهدف استخدامها في الإجراءات القانونيّة على أنّها صحيحة، سواء كان ذلك على سند ورقي أو سند غير مادي وذلك بنية الإضرار بالغير.

ويقصد بالتّزوير المعلوماتي الأفعال العمديّة وغير الشّرعيّة التّي من شأنها إلحاق الضّرر المادي بالغير، سواء بإتلاف المعطيات الإلكترونيّة أو فسخها أو تعديلها أو إعدامها أو إدخالها أو صنعها، وبجميع أشكال الاعتداء على عمل النّظام المعلوماتي، وذلك بهدف التّزوير والإضرار والحصول على مردود اقتصادي لفائدة الفاعل أو لفائدة الغير، وذلك هو التمييز النظري لدى رجال القانون بين أفعال التّدليس وأفعال التّزوير.

1. الاحتيال الالكتروني :

تم تعريف الاحتيال الرقمي في المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010جريمة الاحتيال، التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير،[2]عن طريق:

1. إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات.
2. التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.
3. تعطيل الأجهزة والبرامج والمواقع الالكترونية .

[1]– ورد تعريف لهذا الاعتداء في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 المادة 10: جريمة التزوير: استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقية في البيانات تغييرا من شأنه إحداث ضرر،وبنية استعمالها كبيانات صحيحة .

[2] – كالتلاعب بعنوان الكتروني يكون مشابه الى حد كبير لعنوان الكتروني معروف وموثوق فيه وكمثال على ذلك العناوين الموضحة بالأسفل والتي توحي انها لمايكروسوفت ولكنها في الحقيقة لا تمت لها بصلة

- Micosoft.com
- Microsoft.info.com
- Microsoft-info.com
- Microsoft.com@no.how.com

ويهدف احتيال الإنترنت في العادة إلى سلب أموال المستخدمين –إما بسرقة أرقام بطاقات ائتمانهم أو بجعلهم يرسلون حوالات مالية أو شيكات أو دفعهم إلى الكشف عن معلومات شخصية بغية التجسس أو انتحال الشخصية أو الحصول على معلومات حسابهم المالي ويتضمن الاحتيال أشكالاً مختلفة منها :

2. سرقة المال/الاحتيال: يعني الاحتيال عبر الانترنت عملية التقاط التفاصيل المصرفية، ولا سيما أرقام التعريف الشخصية، وأرقام توثيق المعاملات، بقصد سرقة الحسابات المصرفية للآخرين.

3. الإحتيال التجاري: يحصل الغش التجاري عندما يدّعي البائعون بيع سلع أو خدمات، لا تتطابق مع المواصفات المذكورة أو لا يتم تسليمها على الأطلاق بعد أن سبق ودفع ثمنها، ويمكن أن ينتج ذلك عن عملية انتحال هوية او احتيال، يمكن أن يكون بيع خدمات رقمية (مثلاً، رنة الهاتف) مصدراً آخراً للاحتيال التجاري، إذ يطلب المتصل سعراً خيالياً أو غير عادلٍ، وغالباً ملزماً باشتراك دائم لخدمات لا يرغب بها المشتري، في معظم الأحيان، لا يدرك المستخدمون (وبخاصة الأولاد والشباب) عواقب هذه العقود التجارية التي تبرم على شبكة الانترنت.[1]

البند الثالث : الجرائم المرتبطة بالمحتوى المعلوماتي

تعدّ الشّبكات المفتوحة وسيلة سهلة في اتّجاه الاعتداء على الحريّات الخاصّة، وعلى كلّ ما يتّصل بالشّخص، وإذا كانت الجريمة تتطلّب في عالمها المادي شيئا من "الحذق والتّعب"، فإنّها السّهولة الكاملة في فضائها اللامادي، بفضل أدوات المعلوماتيّة وتقنيّاتها،[2] وهي تتحقّق في أوقات

[1] - Youth protection rountable tool kit-stiftung digitale chancen 2009 , http://unesco.mil-for-teachers.unaoc.org.

[2] -Eric A. Caprioli, Les moyens juridiques de lutte contre la cybercriminalité, www.caprioli-avocats.com
Première publication : Revue Risques n°51, Les cahiers de l'assurance, Ed. LGDJ/SEDDITA, juillet-sept 2002, p. 50-55.

قياسيّة لم يشهد لها التّاريخ مثلا. ويمكن أن يشمل الاعتداء شرف الإنسان وعرضه وأخلاقه وأمنه.

ونمّت المعلوماتيّة فعلا أشكال السب والشّتم والميز العنصري والإرهاب والتّحريض على الجريمة والتّجسّس والمتاجرة بجسد الطّفل وبجميع الأشكال الجنسيّة[1].

وتعدّ الشّبكات المفتوحة فضاءً سهلا للقول بخيار العنصر أو القوم سواء لأسباب دينيّة أو عرقيّة أو لونيّة، وهي فضاء ليّن لإشهار الخطب والمقالات العنصريّة والتّباغض بين الأجناس.

1. جرائم الاعتداء على الحياة الخاصة للأفراد

تتمثل هذه الجرائم في فضح الأسرار والتشهير والقذف، [2] حيث أن الإنترنت وسيلة نشر جماهيرية عالمية مما يمكن من أن تستغل هذه الصفة ويشهر بشركات أو أشخاص بقصد الإضرار بالسمعة الشخصية أو المالية إما بسبب المنافسة، أو بداعي الانتقام، ونحو ذلك .وتوجد على شبكة الإنترنت اليوم مئات المواقع، والمنتديات، التي تخصصت في كشف الخصوصيات، وفضح الأسرار الشخصية للشخصيات العامة، بل وتعدى الأمر على قيام كثيرين باستغلال الإنترنت، وتخصيص مواقع لأسماء، وشخصيات عامة للتشهير بهم ونشر أسرارهم.

---

[1]- محمد أمين الرومي، جرائم الكمبيوتر و الانترنيت، دار المطبوعات الجامعية، 2003 ، ص 182.

[2]- عاقب المؤسس الدستوري على هاتة انتهاكات بنص المادة المادة 39 من الدستور الجزائري رقم 16-01 المؤرخ في 06 مارس *2016* الجريدة الرسمية رقم 14 المؤرخة في 7 مارس *2016* ، تنص على ما يلي : لا يجوز انتهاك حُرمة حياة المواطن الخاصة وحرمة شرفـــه ويحميهما القانون.

- سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.
- لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية. ويعاقب القانون على انتهاك هذا الحكم.
- حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه، كما تم النص على هذا النوع من الاعتداءات في المادة من 14 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010: جريمة الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات.

2. انتهاك الخصوصية

تتفق التشريعات الدولية[1]على ضرورة احترام خصوصية الفرد، ويعتبر مجرد التطفل على تلك المعلومات، سواء كانت مخزنة في الحاسب الآلي أو في بريده الالكتروني أو في أي مكان اخر

---

[1]- تشريعات الخصوصية لمختلف دول العالم :

- السويد: قانون حماية المعطيات رقم 289 تاريخ 1973/5/11 المعدل في الأعوام 1979 و 1982 و 1986 و1990 و 1992 . قانون البيانات الشخصية لعام 1998 حل محل القانون المشار اليه .

- الولايات المتحدة الأمريكيةU S Aعلى المستوى الفيدرالي- قانون الخصوصية لعام 1974

- قانون خصوصية الاتصالات الالكترونية لسنة 1986 و قانون حماية خصوصية المستهلك لعام 1997 .
- *The consumer Internet privacy act of 1997*- قانون حماية خصوصية الضمان الاجتماعي على الخط لعام 1997.
- *Social security online privacy protection act of* 1997
- قانون خصوصية الاتصالات لعام 1997
- قانون خصوصية المعطيات لعام 1997 .
- *The data privacy act* of 1997 1977 قانون حماية المعطيات تاريخ 1977/1/27 عدل جذريا بتاريخ 1990/12/20 كما جرى تعديله العام 1994 *The Data Protection Act*
- مشروع قانون حماية البيانات عام 2000 المتوافق مع القانون الأوروبي لعام 1995
- 1978 النمسا 1Austria
- القانون الفدرالي لحماية المعطيات 1978/10/18 المعدل بالقوانين رقم 314 لسنة 81 228 لسنة 1982 و 370 لسنة 1986 و و605 لسنة 1987 و 233 لسنة 1988 و 609 لسنة 1989 و 91 لسنة 1993 و 79 لسنة 1994 و 632 لسنة 1994
- قانون حماية البيانات لعام 2000 . 2000 *Data protection bill (Datenschutzgesetz*

- الدانمارك
  - ✓ قانون التسجيل الخاص رقم 293 تاريخ 1978/6/8 المعدل في 1988/4/1
  - ✓ قانون تسجيل السلطات العامة 1978/6/8 المعدل ايضا بتاريخ 1988/4/1 .
  - ✓ قانون معالجة البيانات الشخصية لعام 2000
- فرنسا: قانون المعالجة الآلية للمعطيات ، ملفات المعطيات والحريات الفردية رقم 17-78 تاريخ 1978/1/6 المعدل في الاعوام 1988, 1992, 1994, 1999, 2000
- النرويج: قانون تسجيل المعطيات الشخصية رقم 48 تاريخ1978/6/9 المعدل بالقانون رقم 55 تاريخ 1987/6/12، والقانون 66 تاريخ 1991/7/20 .
- لوكسمبورغ: سنة 1979
  - ✓ القانون المنظم للارقام الوطنية (الهوية) للاشخاص الطبيعية والقانونية تاريخ 1979/3/31 .
  - ✓ القانون المنظم لاستخدام المعطيات الاسمية في المعالجة الآلية للمعطيات تاريخ 1979/3/31 .
  - ✓ قانون حماية الخصوصية بتاريخ1982/8/11
- استراليا
  - ✓ قانون حرية المعلومات لعام 1979 وتعديله الجذري بتاريخ 1982/3/9 وتعديلاته اللاحقة .
  - ✓ قانون الخصوصية 1988 وتعديلاته لعامي 1989 و1990 و1997.
  - ✓ قانون 2000 المعدل لقانون الخصوصية المتعلق بحماية البيانات في القطاع الخاص
- روسيا: قانون حماية المعلومات لعام 1995 .

انتهاكاً لخصوصيته الفردية[1]، وأدى انتشار الإنترنت إلى تعرض الكثير من مستخدمي الإنترنت لانتهاك خصوصياتهم الفردية، سواء عمدا أو مصادفة، فبكل بساطة ما أن يزور مستخدم الإنترنت أي موقع على شبكة الإنترنت، حتى يقوم ذلك الموقع بإصدار نسختين من الكعكة الخاصة بأجهزتهم (*Cookies*)وهي نصوص صغيرة يرسلها العديد من مواقع الويب، لتخزينها في جهاز من يزور تلك المواقع لعدة أسباب لعل منها التعرف على من يكرر الزيارة للموقع أو لأسباب أخرى، وتبقى واحدة من الكعكات في الخادم (السيرفر) الخاص بهم، والأخرى يتم تخزينها على القرص الصلب لجهاز الزائر للموقع في أحد الملفات التي قامت الموقع الأخرى بتخزينها من قبل دون أن يشعر صاحب الجهاز بذلك، أو حتى الاستئذان منه! وفورا يتم إصدار رقم خاص ليميز ذلك الزائر عن غيره من الزوار، وتبدأ الكعكة بأداء مهمتها بجمع المعلومات وإرسالها إلى مصدرها أو إحدى شركات الجمع والتحليل للمعلومات، وهي عادة ما تكون شركات دعاية وإعلان.

وكلما قام ذلك الشخص بزيارة الموقع، يتم إرسال المعلومات وتجديد النسخة الموجودة لديهم، ويقوم المتصفح لديه بعمل المهمة المطلوبة منه، مالم يقم صاحب الجهاز بتعديل وضعها، وقد تستغل بعض المواقع المشبوهة هذه الكعكات بنسخ تلك الملفات والاستفادة منها بطريقة

المادة 23 من الدستور الروسي .Article 23 of the Constitution of the Russian Federation

- تركيا : مشروع قانون حماية البيانات الشخصية لعام 2000.

[1]- قدم الاتحاد الأمريكي للحريات المدنية، في فبراير 2013، دعوى قضائية، باسم مؤسسات أمريكية، ضد وكالة الأمن القومي (أن أس إيه)، تتهمها فيها بـــ"خرق قوانين الخصوصية، والتجسس على محتويات الرسائل الإلكتروني، والتصفح على الإنترنت، والاتصالات التي تتم عبر الشبكة الدولية."وتُمثل الدعوى المقدمة من المنظمة المستقلة، المعنية بحقوق الإنسان والحريات المدنية، كلا من مؤسسة "ويكميديا"، ومعهد "رذرفورد" المحافظ، ومجلة "ذي نيشن"، ومنظمة العفو الدولية فرع الولايات المتحدة، ومنظمة "بن المركز الأمريكي" (منظمة تعنى بالأدب وحرية التعبير)، و"هيومن رايتس ووتش"، والرابطة الوطنية لمحامي الدفاع الجنائي، والصندوق العالمي للمرأة، ومكتب واشنطن في أمريكا اللاتينية.وقال بيان صادر عن الاتحاد الأمريكي للحريات المدنية، إن "وكالة الأمن القومي وخلال عملية مراقبتها (للإنترنت) استنسخت ومشطت عددا ضخما من مواد الإنترنت التي تحدث داخل الولايات المتحدة، بمساعدة شبكات اتصال عملاقة." وأشار البيان إلى أن وكالة الأمن القومي غير مخولة قضائيا بمراقبة الرسائل الإلكترونية والنشاطات على شبكة الإنترنت، لافتة إلى أن تلك العمليات، شملت مراقبة ملايين الأمريكيين العاديين.

وقال باتريك تورومي، محامي الاتحاد، إن "المراقبة المستمرة تعدّ خرقا للخصوصية، وتقوّض حريات التعبير والتحقيق على حد سواء." وتقول الدعوى التي تم التقدم بها لمحكمة اتحادية في ولاية ميريلاند، القريبة من العاصمة واشنطن، حيث يقع المقر الرئيسي لوكالة الأمن القومي، إن "عملية المراقبة التي تمارسها الوكالة الأمنية الحكومية تتجاوز الصلاحيات التي خولها الكونغرس لها."

الأربعاء، 11 مارس، 2015، منظمات أمريكية تقاضي "وكالة الأمن القومي" بتهمة التجسس لمزيد من التفاصيل انظر الرابط التالي : http://felesteen.ps

أو بأخرى[1]، كما قد يحصل أصحاب المواقع على معلومات شخصية لصاحب الجهاز طوعا، حيث يكون الشخص عادة اقل ترددا عندما يفشى معلوماته الشخصية من خلال تعامله مع جهاز الحاسب الآلي، بعكس لو كان الذي يتعامل معه إنسان آخر[2] و هناك وسائل لحماية الخصوصية أثناء تصفح الإنترنت ، ولكن " من الصعب جدا السيطرة على ما يحدث للمعلومة بمجرد خروجها من جهاز الحاسب (الآلي)[3]، وعلى ذلك فان حماية الخصوصية، يجب أن تبدأ من البداية بتحديد نوعية البيانات ،التي لا ينبغي أن تصبح عامة ومشاعة ثم بتقييد الوصول إلى تلك المعلومات"[4].

البند الرابع :الجرائم المرتبطة بحقوق المؤلف والحقوق المجـــاورة [5]

تضمنت قوانين حماية الملكية الفكرية،[6] في العالم بصفة عامة حماية الكتب والكتيبات وغيرها من المواد المطبوعة، والمصنفات التي تلقى شفاهية كالمحاضرات والخطب وغيرها، كذلك

---

[1] -Volio Fernando, Legal personality, privacy and the family,in Henkin (ed), The International Bill of Rights, Columbia University Press 1981.

[2]- داود حسن طاهر ،المرجع السابق،ص ص 50- 52.

[3] -The E-Privacy Imperative, Protect Your Customers, Internet Privacy and Ensure Your Company's Survival in the Electronic Age, by Mark S. Merkow, James Breithaupt, 2001.

[4]- داود حسن طاهر ،المرجع السابق ،ص 53 .

[5]- محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص ، دار النهضة العربية ،القاهرة، بند 1078 ، ص 803.

[6]- المعاهدات الدولية لحقوق الملكية الفكرية :

1. ميثاق باريس لحماية الملكية الصناعية 1883 و تعديلاته 1967.
2. ميثاق بيرن لحماية الحقوق الأدبية و الفنية 1886 ثم وثيقة باريس 1971.
3. اتفاقية مدريد للتسجيل الدولي للعلامات التجارية 1891 و تعديلاتها و البروتوكول المتعلق بها 1989.
4. اتفاقية مدريد للحد من الاستخدام غير المشروع للمؤشرات الجغرافية 1891.
5. اتفاقية لاهاي بشان الإيداع الدولي للتصاميم الصناعية 1925 و تعديلاتها 1934 و القرار المكمل لها 1960.
6. الاتفاقية العالمية لحقوق المؤلف اليونسكو- 1952.
7. اتفاقية نيس للتصنيف العالمي للسلع و الخدمات لغرض تسجيل العلامات 1957.
8. اتفاقية لشبونة لحماية الأصول و التسجيل الدولي 1958 و تعديلاتها 1967 و1979.
9. ميثاق روما لحماية المؤدين و منتجي التسجيلات الصوتية و الهيئات الإذاعية 1961.
10. المعاهدة الدولية للتعاون بشان براءات الاختراع – وايبو- 1970.
11. ميثاق جنيف لحماية منتجي الفونوغراف ضد النسخ غير الشرعي 1971.

المصنفات المسرحية والموسيقى، والتمثيل ... الخ، وبرامج الحاسوب (في أعقاب انضمام الدول العربية إلى اتفاقية برس)؛ حيث امتدت إلى البرمجيات سواء كانت بلغة المصدر أو الألة، إضافة إلى حماية قواعد المعلومات المجمعة وتحديداً حماية طريقة التجميع سواء كانت بطرق تقليدية أو آلية، ولكي تتوافق مع المادة رقم (10) من اتفاقية برس، وتشمل الحماية الحقوق المعنوية للمؤلف والحقوق المالية لاستغلال المصنف وهى حماية للمؤلف وحده يمنع بموجبها أى استغلال أو استعمال يضر بمصلحة المؤلف، ويكون للمؤلف وحده الحق في استنساخ المصنف وإجازة استعماله[1]، وفقاً لشروط تقررها القوانين العربية في هذا الحقل، ومن أكثر التحديات هي مفهوم الاستعمال الشخصي للمصنف ومداه ونطاقة إضافة إلى الإشكالات المتعلقة بمدى ونطاق استخدام تلك المصنفات لغايات علمية أو بحثية أو في المعارض.

من خلال الرجوع للدراسات القانونية نجد أن مفهوم البرنامج ونطاقة خلق إشكاليات عديدة، منها ما إذا كان إعادة إنتاج البرنامج أو اقتباس أجزاء منه، أو اتباع وسائل برمجية غير المتبعة في إنتاجه أصلاً يعد من طرق النسخ الغير مشروعة أو التقليد؛ حيث اتفق القضاء على أن

---

12. اتفاقية فيينا لوضع تصنيف دولي لمكونات العلامات 1973.
13. معاهدة واشنطن حول حقوق الملكية للدوائر المتكاملة 1989.
14. معاهدة قانون العلامات التجارية وايبو- 1994.
15. اتفاقية التدابير المتعلقة بأثر التجارة على حقوق الملكية الفكرية – تربس- 1994.
16. معاهدة حماية حقوق المؤلف- وايبو -1996.
17. -معاهدة حماية الأداء و التسجيل الصوتي - وايبو – 1996.
18. معاهدة بودابيست الدولية لمكافحة جرائم المعلوماتية و الاتصالات 2001 .ذكرهم : مصطفى عبد الغني : الجات و التبعية الثقافية، مركز الحضارة العربية، 1998، ص 17.

[1] -Cour de cassation, première Chambre civile, 28 février 2006 (Mulholland Drive), Bull. civ. 1,126 : « l'exception de copie privée prévue aux articles L. 122-5 et L. 211-3 du Code de la propriété intellectuelle, tels qu'ils doivent être interprétés à la lumière de la directive européenne susvisée, ne peut faire obstacle à l'insertion dans les supports sur lesquels est reproduite une oeuvre protégée, de mesures techniques de protection destinées à en empêcher la copie, lorsque celle-ci aurait pour effet de porter atteinte à l'exploitation normale de l'oeuvre, laquelle doit s'apprécier en tenant compte de l'incidence économique qu'une telle copie peut avoir dans le contexte de l'environnement numérique ». Cédras Jean, « Un aspect de la cybercriminalite en droit français : le téléchargement illicite d'œuvres protégées par le droit d'auteur », *Revue internationale de droit pénal* 3/2006 (Vol. 77) , p. 589-610
URL : www.cairn.info/revue-internationale-de-droit-penal-2006,p,589. .

التقليد أو النسخ الكامل للمنتج بغرض الاستغلال المالي، لا يثير إشكالاً في التطبيق، ولكن الذي يثير الإشكال هو اقتباس الخوارزميات المحتواه ضمن البرنامج، فالقضاء الأجنبي يرى من وجهة نظره أن حقوق المؤلف الخاصة بالبرمجيات تتفق مع أحكام الاتفاقيات الدولية بشأن عدم شمول الخوارزميات والحقائق للحماية، وهذا يعنى أن الاقتباس الذي لا يتجاوز النسخ الجزئي وطريقة الهندسة العكسية المتبعة في إعادة بناء البرنامج، تخضع لمعايير معينة قبل القول بحصول النسخ أو الاعتداء على حقوق المؤلف[1].

إن الإجرام الرقمي في النطاق القانوني، لا يتعلق بالمعلومات القانونية الشخصية فقط، بل اتسع استخدامها حتى في المسائل المالية، كالغش المعلوماتي أو غش الحاسوب، والاحتيال المعلوماتي أو احتيال الحاسوب، ونصب الحاسوب وغيرها مما يوضح أن الظاهرة الاجرامية المستحدثة تتمحور رغم اختلاف أنماط السلوك الإجرامي وذلك حول فعل الغش أو النصب أو الاحتيال،ومن بين الاصطلاحات التي شاعت في العديد من الدراسات وتعود الآن إلى واجهة التقارير الإعلامية،اصطلاح الجرائم الاقتصادية المرتبطة بالكمبيوتر ***Computer-Related Economic Crime***، وهو تعبير يتعلق بالجرائم التي تستهدف معلومات قطاعات الأعمال أو جرائم الاعتداء على الأموال، وبالتالي يخرج من نطاقها الجرائم التي تستهدف البيانات الشخصية أو الحقوق المعنوية على المصنفات الرقمية، وكذلك جرائم المحتوى الضار أو غير المشروع و فيما يلي بعض صوره.

1. جريمة التحويل الإلكتروني للأموال

يتم التحويل غير المشروع للأموال، بعدة وسائل يصعب حصرها لسرعة وتيرة التطور في هذا المجال، لكن يمكن الإشارة إلى أكثرها انتشاراً.[2] استخدام برامج معده خصيصا لتنفيذ الاختلاس :

– أشهر هذه الوسائل هو تصميم برامج معينة، تهدف إلى إجراء عمليات التحويل الآلي من حساب إلى آخر، سواء كان ذلك من المصرف نفسة أو من حساب أخر في مصرف آخر، على أن يتم ذلك في وقت معين يحدده مصمم هذا البرنامج، وأشهر هذه الوقائع قيام احد العاملين بمركز الحاسبات المتعاقد مع مصرف الكويت التجاري، لتطوير أنظمة المعلومات بالاستيلاء على

[1]– يونس عرب، التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية، المرجع السابق، ص ص 20-21.

[2]– محمد أمين الشوابكة، جرائم الحاسوب والانترنت–الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع،الاردن،2011، ص178 .

مبالغ طائلة من المصرف، بعد أن تمكن من اختيار خمسة حسابات راكدة في خمس فروع محليه للمصرف، واعد لها برنامجا تمثلت مهمته في تحويل مبالغ معينة من هذه الحسابات الى حسابات أخرى فتحت باسمه في الفروع نفسها، على أن تتم عملية التحويل أثناء وجوده بالطائرة في طريقة إلى المملكة المتحدة عائدا إلى بلاده بعد انتهاء عقد عمله، ثم فتح حسابات أخرى فور وصوله وطلب من المصرف تحويل هذه المبالغ إلى حساباته الجديدة في بريطانيا[1].

– كما توجد برامج أخرى تقوم بخصم مبالغ ضئيلة من حسابات الفوائد على الودائع المصرفية، بإغفال الكسور العشرية بحيث يتحول الفارق مباشرة إلى حساب الجاني، لأنها برامج تعتمد على التكرار الآلي لمعالجة معينة، ومما يؤدي إلى صعوبة اكتشاف هذه الطريقة رغم ضخامة المبلغ، هو ان هذه الاستقطاعات تتم على مستوى ألاف الأرصدة في وقت واحد مع ضآلة المبلغ المخصوم من كل حساب على حده بحيث يصعب أن ينتبه إليه العميل [2].

– التحويل المباشر للأرصدة: يتم ذلك عن طريق اختراق أنظمة الحاسب وشفرات المرور ،أشهرها قيام احد خبراء الحاسب الآلي في الولايات المتحدة باختراق النظام المعلوماتي لأحد المصارف، وقيامه بتحويل 12 مليون دولار إلى حسابه الخاص في ثلاث دقائق فقط، وعادة ما يتم ذلك أيضا عن طريق إدخال معلومات مزيفة وخلق حسابات و مرتبات وهمية، وتحويلها إلى حساب الجاني ،ويمكن أن يتم التحويل المباشر أيضا عن طريق التقاط الإشعاعات الصادرة عن الجهاز إذا كان النظام المعلوماتي متصلا بشبكة تعمل عن طريق الأقمار الصناعية فهناك بعض الأنظمة إلى تستخدم طابعات سريعة تصدر أثناء تشغيلها إشعاعات إليكترومغناطيسية، ثبت أنه من الممكن اعتراضها والتقاطها أثناء نقل الموجات وحل شفراتها بواسطة جهاز خاص لفك الرموز وإعادة بثها مرة أخرى بعد تحويرها[3].وهوما نصت عليه اتفاقية بودابست في المادة05[4].

---

[1] – هشام فريد رستم، قانون العقوبات، مخاطر المعلومات مكنة الآلات الحديثة، مصر، 1992،ص 81 .

[2]. David Bainbridge, Introduction to computer law, third edition, Pit Man publishing,1996, p237 .

[3] محمد سامي الشو، ثورة المعلومات وانعكاسها على قانون العقوبات، دار النهضة العربية: القاهرة، ، 1994ص 70-72 وما بعدها .

[4] –Article 5 - Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération et la suppression de données informatiques, Convention sur la cybercriminalité ,Budapest, 23.XI.2001.

– التلاعب بالبطاقات المالية،: لقد ظهرت أولى هذا النوع من الاحتيال بالتقاط الأرقام السرية لبطاقات الدفع المختلفة، [1]من أجهزة الصرف الآلي للنقود إلى أن ظهرت الصرافة الآلية *Electronic Banking* والنقود المالية *digital Cash* .

أما جرائم الاعتداء على هذه البطاقات، فتتمثل في استخدامها من قبل غير صاحب الحق بعد سرقتها أو بعد سرقة الأرقام السرية الخاصة بها، وهو ما يتم عن طريق اختراق بعض المواقع التجارية، التي يمكن ان تسجل عليها أرقام هذه البطاقات.

و في هذا النوع من الاعتداءات لا نجد صعوبة في تطبيق نصوص جرائم السرقة والنصب عليها سواء تم ذلك عن طريق سرقة البطاقة نفسها، أو عن طريق سرقة الرقم السري واستخدامه استخدام غير مشروع للتحايل على المؤسسات المالية، وصرف هذه المبالغ، خاصة أن النموذج التجريمي لجريمة النصب لم يشترط في الوسائل الاحتيالية أن تكون مرتكبة ضد الإنسان فيكفي أن ترتكب هذه الوسائل الاحتيالية ضد الآلة ما دامت تؤدي إلى الحصول على نفع غير مشروع أضرارا بالآخر[2] .

2. جرائم الاعتداء على أجهزة الصرف الآلي للنقود:

تثور هذه المشكلة في حالة استخدام الجهاز لصرف ما يتجاوز الرصيد الفعلي اذا تم ذلك بواسطة العميل صاحب البطاقة فالمسألة هنا لا تعدو أن تكون مسألة مديونية بين المؤسسة المالية والعميل ولا يمكن تكييفها بأنها سرقة ،لان الاستيلاء على المبلغ لم يتم دون رضاء المؤسسة المالية طالما ان هذه الاخيرة تعلم بأن الجهاز غير مرتبط بسقف حساب العميل حتى لا يتجاوزه[3].

---

[1]– ومن الأمثلة الواقعية لاحتيال " بطاقات الائتمان واقعة المتطفل hacher كيفيين ميتنك الذي أسندت إليه تهمة استخدام دخول احتيالي للكمبيوتر للحصول على 20.000 بطاقة ائتمانية من شركة (netcom) للاتصالات في سان جوس بكاليفورنيا.

[2]– قضى القضاء الفرنسي بأنه من الجائز استخدام نظم المعلومات في تحقيق جريمة النصب و لذلك قضى بأن استخدام الكمبيوتر في اصطناع ايصالات و طبعها نظرا لما له من امكانيات في اجراء حسابات تمثل الايهام بوجود دين حقيقي تقع به جريمة النصب، و يعقب الفقه على الحكم قائلا أن الجاني لا ينصب على الالة و لكن ينصب على الانسان الذي يجلس خلف هذه الالة ،مشار الية بالتفصيل عند مدحت رمضان، الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية، مصر،2000،ص152.

[3]- محمد إبراهيم محمد الشافعي، النقود الإلكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س 12، ع1، يناير، 2004، ص142–148.

3. جرائم الاستيلاء على النقود الالكترونية :

يمكن تعريف النقود الالكترونية *Electronic Cash*[1] بأنها "قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدماً، وغير مرتبطة بحساب مصرفي، تحظى بقبول غير من قام بإصدارها، وتستعمل كأداة دفع". وتتمثل أهم عناصرها في أن قيمتها النقدية تشحن على بطاقة بلاستيكية، أو على القرص الصلب للحاسب الشخصي للمستهلك، فهي تختلف عن البطاقات الإئتمانية، لأن النقود الإلكترونية يتم دفعها مسبقاً، بالإضافة إلى أنها ليست مرتبطة بحساب العميل، فهي أقرب إلى الصكوك السياحية منها إلى بطاقة الائتمان، أي أنها استحقاق عائم على مؤسسة مالية، يتم بين طرفين هما: العميل والتاجر، دون الحاجة إلى تدخل طرف ثالث، كمصدر هذه النقود مثلاً[2]فهي مجموعة من البروتوكولات والتوقيعات الرقمية التي تتيح للرسالة الالكترونية أن تحل فعليا محل تبادل العملات النقدية[3]، ومن هذه البطاقات ما يعمل عن طريق إدخالها إلى المركز الخاص بالمعاملة المصرفية لدى البائع أو الدائن حيث تم انتقال البيانات الاسمية من البطاقة إلى الجهاز الطرفي للبائع تحول عليه نتائج عمليات البيع والشراء إلى البنك الخاص بالبائع[4].

---

[1]– لم يتفق الرأي حول تعريف النقود الالكترونية او الإحاطة بمضمونه وذاتياته، وذلك بسبب الغموض الذي يحيط بالمصطلحات والمفاهيم الجديدة المرتبطة به .ولقد أقرت لجنة (Basel) للتسويات الدولية هذه الصعوبة. فالتعريف يمزج بين المفاهيم التقنية الحديثة والخصائص الاقتصادية والقانونية في ذات الوقت .كما ان تنظيم وترتيب مخططات النقود الالكترونية يختلف بحسب المؤسسة التي تتولى إصدارها. لذا نرى اختلاف المصطلح المستخدم في هذا المجال، ففي بعض الدراسات يطلق على النقود الالكترونية مصطلح (virtual cash) أي النقد الافتراضي، وبعضها يسميها (electronic cash) وبعضها (electronic money) وبعضها (digital cash) وبعضها(electronic cash)

- Basel committee Risk management for electronic Banking and electronic money activities. March 1998. In

  : http://www.bis.org/publ/bcbs35.htm

- Mechelle Baddeley Gonville – using E–cash in the new money: An economic analysis of micropayment systems. Journal of Electronic commerce Research. Vol. 5, No.4, 2004: In : www.csulb.edujournalsjecrissues 2004 paper3.pdf.p. 240 .

[2] محمد إبراهيم محمد الشافعي، النقود الإلكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، ع1، 2004، ص ص142–148.

[3] منير الجنبيهي و ممدوح الجنبيهي، البنوك الالكترونية، دار الفكر الجامعي، الإسكندرية، ط 2 ، 2006، ص47 .

[4] عبد الفتاح بيومي حجازي، صراع الكمبيوتر والانترنت، في القانون العربي النموذجي، دار الكتب القانونية ، دار للنشر والبرمجيات، القاهرة 2007، ص 609 .

و قد قام المركز القومي لمعلومات جرائم السرقات بالولايات المتحدة الاميريكية *(The National Fraud Information Center (NFIC)*و الذي تم إنشاءه عام 1992للتعرف على أوجه الحماية من الجرائم الالكترونية وآثارها السلبية، حيث يقوم معتادي الشراء من خلال الانترنت، بالاتصال بالرقم الساخن لهذا المركز أو عن طريق البريد الالكتروني، المخصص له على شبكة الانترنت والإبلاغ عن أية مخالفات أو سرقات تمت لهم من خلال بطاقات الائتمان[1].

الأمر يعتمد على وعى حاملي هذه البطاقات للمخاطر المتوقعة، و فيما يلى بعض الملاحظات الواجب أخذها في الاعتبار للتقليل من أثار تلك الممارسات:

في حالة عدم وجود نية لاستخدام بطاقات الائتمان للشراء من خلال الانترنت يجب التوجه لمسئول الائتمان بالبنك وإغلاق إمكانية الاستخدام من خلال الانترنت.

بالنسبة للمشتريين أيضا يمكن لهم استصدار بطاقات للشراء من خلال الانترنت فقط، وعدم تحميل تلك البطاقات بمبلغ كبير من المال، فيكفى أن تحمل بقيمة المشتريات الحقيقية خلال فترة محددة.

يجب الشراء من خلال المواقع التي لا تتم عملية الشراء إلا بعد الاتصال تليفونيا، أو إرسال بريد الكتروني، للتأكد من صدق عملية الشراء و ذلك من جانب العارضين للسلع و الخدمات.

يجب على العارضين للمنتجات و السلع عبر الانترنت ،أيضا أن ينتابهم الشك فى حالة الشراء بأسعار عالية، وعليهم عدم إتمام العملية إلا بعد الاتصال بالمشترى، والتأكد منه سواء بالاتصال التليفوني أو بإرسال خطاب بريدي له.

[1]– قد برزت حوادث السرقة بشكل متطور في عصر الانترنت، بحيث أمكن على سبيل المثال سرقة الأموال الكترونيا، والتعدي على الحقوق الفكرية للآخرين، وتزوير، وسرقة بطاقات الائتمان، للحصول على الخدمات المدفوعة .في الولايات المتحدة نشرت جريدة واشنطن بوست February 19.2003 قصة حادثة مهمة، حقق فيها مكتب التحقيقات الفيدرالي الأمريكي، حول اختراق أجهزة كمبيوتر، وقيل بأن من المحتمل أن يكون تم خلال هذا الحادث سرقة أرقام ثمانية ملايين بطاقة ائتمانية، من شركة Data Processors Intel التي تجري عمليات تحويل مالية لشركات الائتمان الدولي، فيزا وماستركارد أمريكان اكسبريس وديسكفري

WWW.cnn.com/2003/02/18/techn...

يجب على العارضين أيضا التحقق من عمليات الشراء التي تتم من خارج البلاد، وان تكون لديهم قائمة بالبلاد الأكثر خطورة في سرقة بطاقات الائتمان و منع الشراء منهم كلما أمكن ذلك.

4. القمار عبر الانترنت

في الماضي كان لعب القمار يستلزم وجود اللاعبين على طاولة واحدة ليتمكنوا من اللعب, أما الآن ومع انتشار شبكة الإنترنت على مستوى العالم فقد أصبح لعب القمار أسهل، وأصبح بالإمكان التفاف اللاعبين على صفحة واحدة من صفحات الانترنت على مستوى العالم ومن أماكن متنوعة.[1]

5. الإرهاب الرقمي[2]:

في عصر الازدهار الالكتروني وفي زمن قيام حكومات الكترونية كما في الجزائر، تبدل نمط الحياة وتغيرت معه أشكال الأشياء وأنماطها ومنها ولا شك أنماط الجريمة والتي قد يحتفظ بعضها بمسماها التقليدي مع تغيير جوهري أو بسيط في طرق ارتكابها، ومن هذه الجرائم الحديثة في طرقها القديمة في اسمها جريمة الإرهاب والتي أخذت منحنى حديث يتماشى مع التطور التقني.[3]

---

[1] - S - Mcquade,Understandingand Managing Cyber Crime ,Boston, Allyn & Bacon, 2006,p 45.

[2] -C. Wilson, Holding management accountable, a new policy for protect against computer crime,Proceedings of the National Aerospace and Electronics Conference, USA 2000, 272-281.

-جلال الزعبي، جرائم تقنية نظم المعلومات، دراسة مقارنة، من دار الثقافة للنشر و التوزيع ، الأردن، 2014،ص 317و ما بعدها .

[3]- حسين شفيق، الإرهاب الرقمي، دار الفكر للطباعة و النشر و التوزيع، 2015، ص ص 175-192.

كما نجد الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010قد جرمت هذا النوع من الجرائم في المادة 15 تحت عنوان : الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات

1. نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.
2. تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.
3. نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.

نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

6. التجارة الالكترونية للمخدرات:

تطرح شبكة الانترنت معضلات لم تكن لتخطر على نفسية الإنسان إذ تحولت إلى سوق للمخدرات والمؤثرات العقلية، و اخترعت مصطلحات مستوحاة من العالم الافتراضي تجسدت في عبارة *Cyber Drugs*[1] .

و تبين لجنة الدول الأمريكية لمكافحة تعاطي المخدرات،[2] أن الجماعات الإجرامية المنظمة تستعمل الوسائل الالكترونية للترويج للمخدرات و المواد غير المشروعة، كما يشير التقرير الصادر عن منظمة الشرطة الدولية(أنتربول) أن 890 مليون شخص في آسيا وأروبا وأمريكا الشمالية ممن يتعاطون المخدرات يحصلون عليها عن طريق الشبكة[3]. هذا وقد كانت منظمة الأمم المتحدة منذ بداية الألفية مافتئت تلفت انتباه المجتمع العالمي، على ضرورة التعاون الدولي[4] للتصدي لسوء استخدام الشبكة المعلوماتية في مجال التجارة بالمخدرات، حيث جاء في قرار الجمعية العامة للأمم المتحدة رقم 132/404 لشهر فيفري 2000 ما يلي :

---

[1]– عمر محمد بن يونس، المخدرات والمؤثرات العقلية عبر الإنترنت ، دار الفكر الجامعي،مصر، 2004، ص 18

- . le Petit Larousse, "l'ensemble des actes de violence commis par une organisation pour créer un climat d'insécurité ou renverser le gouvernement établi", c'est ne prendre en compte qu'une partie du problème".
- Le terrorisme est l'emploi systématique de la violence, (attentats, assassinats, enlèvements, ...) à des fins politiques, de telle sorte que leur retentissement psychologique – terreur et peur – dépasse largement le cercle des victimes directes pour frapper l'opinion publique concernée : http://fr.wikipedia.org/wiki/Terrorisme .
- تثبت الدراسات الفرنسية أن عبارة إرهاب و إرهابي ظهرت في القرن 18 في أعقاب الثورة الفرنسية ، إذ كانت الدولة تقوم بإرهاب السكان مستعملة القوة لاسترجاع الأمن و منه استخدم مفهوم "terreur institutionnalisée". ثم تحولت كلمة « terreur »في القرن 19 إلى عبارة « terrorisme »لتفيد " العنف الموجه ضد الدولة أو أعضاء الحكومة بغية ضرب استقرار هياكل الدولة و إضعاف البلاد. أنظر/http://www.dictionnaires-francais.fr

[2]– أنظر تقرير اللجنة التابعة لمنظمة الدول الأمريكية عن نصف الكرة الأرضية لعامي 2000/1999

[3]– المخدرات الاصطناعية ، نشرة إعلامية منشورة على موقع الإنتربول في شبكة الإنترنت.

[4]–واهتمت دول العالم قاطبة بمكافحة جرائم المخدرات وعقدت المؤتمرات والاتفاقيات الدولية المختلفة ومنها الاتفاقية الوحيدة لمكافحة المخدرات عام (1961م)، اتفاقية المؤثرات العقلية عام (1971م)، واتفاقية الامم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية عام (1988م). وعلى المستوى العربي تم عام (1996م) اقرار الاتفاقية العربية لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية، كما تم عام (1986م) إقرار القانون العربي النموذجي الموحد للمخدرات، عيد محمد فتحي، الإجرام المعاصر، أكاديمية نايف العربية للعلوم الأمنية ،1999،الرياض،ص ص 94-110.

" وإذ تسلم الجمعية بأن استخدام شبكة الإنترنت يتيح فرصا جديدة وتفرض تحديات جديدة، بالنسبة للتعاون الدولي في مكافحة إساءة استعمال المخدرات وإنتاجها والاتجار بها على نحو غير مشروع، وإذ تسلم بالحاجة إلى زيادة التعاون بين الدول وتبادل المعلومات، بما في ذلك ما يتصل بالخبرات الوطنية بشأن التعدي للتشجيع على إساءة استعمال المخدرات والاتجار غير المشروع بها، بواسطة هذه الوسيلة وبشأن استخدام شبكة الإنترنت لعرض المعلومات المتصلة بخفض الطلب على المخدرات " نحاول في عجالة التعرض لتأثير الشبكة العالمية في الإشهار بالمخدرات، ثم طرق المتاجرة الالكترونية بها. يبدو أن تغلغل مسألة المخدرات في الفضاء الافتراضي بدأت بنوايا حسنة، إذ شرع بعض المستخدمين في نشر الوعي بمخاطر التعاطي الظاهرة، و آثارها على الإنسان و المجتمع كآفة ذات عواقب خطيرة، في المقابل وجدت النفوس الضعيفة في هذه النافذة فرصة و سبيلا هينا للإتجار بالمواد السامة و توزيعها، و فوق ذلك المطالبة بتعديل المنظومة القانونية لإباحة بيع المخدرات[1]،فضلا عن ذلك تقوم بعض المواقع الخاصة بيع بذور القنب الهندي مرشدة مستخدمي الانترنت بطرق زراعتها[2].

دور الشبكة العالمية في الترويج للمخدرات: قد نتساءل هل يمكن للفضاء الرقمي أن يتحول إلى صفحة إشهارية للترويج بالمواد، التي تكون سببا في فتور وخدر العقل الإنساني، والتي تحظرها كل الأديان السماوية و القوانين الوضعية و القيم الأخلاقية.

معروف أن الترويج للسلع عامة، هي وسيلة يستخدمها التجار للتأثير على سلوك المشتري لدفعه على الاستهلاك، وقد تكون وطأة الانترنت أكثر فعالية، بسبب الصور و التقديم المغري.

و نفس الأمر يحدث بالنسبة للمخدرات إذ تقوم بعض المواقع[3] بإيهام الأشخاص بمشروعية تعاطي هذه المنتجات، فتأهلهم على كيفية اقتنائها، فزراعتها والاعتناء بها، و تسويقها، في وقت

---

[1]- محمد فتحي عيد، الإنترنت ودوره في انتشار المخدرات، مركز البحوث والدراسات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص 6/5، " كانت أول إساءة لاستخدام شبكة الانترنت في مجال الاتصال المادي والقانوني بالمخدرات والمؤثرات العقلية، خاصة بالدعوة إلى تعاطي المخدرات والحض عليها وكان لجماعة أمريكية تسمي Drug Reform Coordination Networkويتزعمها ديفيد بوردين قصب السبق في هذا الخصوص فهي تعمل عبر شبكة الإنترنت منذ عام 1993" .

[2] -Internet le nouveau supermarché de la drogue, http://www.melty.fr/internet-le-nouveau-supermarche-de-la-dr-actu11193.html.

[3]- أحصت السلطات البريطانية في سنة 2000 حوالي 1000 موقع في العالم يروج و يبيع المواد المخدرة، أنظر المقال الخاص: Grand banditisme et criminalite sur internet, http://strategique.free.fr.

تسعى المجموعة الدولية على محاربة هذه الآفة. بطبيعة الحال هذه الطريقة في الشراء عملية بالنسبة للمستهلكين إذ تقيهم من أعين قوات الأمن التي تراقب حركة تجار المخدرات في الشوارع، إذ تصل السلعة عبر البريد في تستر كبير، و حتى إذا كانت مغشوشة لا يمكن للشخص تقديم شكوى لأنه اشترى مخدرا لا يليق به. تنامي تجارة المخدرات تعود إلى الفراغ القانوني الموجود على مستوى الكثير من الدول إذ تسمح هذه الأخيرة من بيع أنواع من بذور القنب الهندي الموجهة للفلاحة دون منع البذور المخدرة الأخرى، هذا واقع فرنسا مثلا، و الأمر الذي يزيد في خطورة الظاهرة هو زيارة الأطفال و الأحداث لهذه المواقع، فالأنترنت أصبح حقا ميدانا لتجار المخدرات لتسويق سمومهم، إذ لا تفوتنا الفرصة للإشارة إلى وجود جماعات من أنصار تعاطي المخدرات أو ما يعرف المطالبين بإباحة المخدرات، دورهم نشر ثقافة المخدرات. بطبيعة الحال الصفقات التجارية الخاصة بالمخدرات تتم عبر الشبكة و الدفع المستحقات المالية تجري بالوسائل الالكترونية.

7. جرائم معلوماتية ضد الحكومة *Crimes Against the Government*

يقصد بالجرائم ضد الحكومة أو بالأحرى ضد المصلحة العامة – بوجه عام – هي تلك الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات الطابع العام ؛ [1]

أي تلك الحقوق التي ليست لفرد أو أفراد معينين بذواتهم ؛ فالحق المعتدى عليه هو للمجتمع في مجموع أفراده ؛ أو هو الدولة باعتبارها الشخص القانوني الذي يمثل المجتمع في حقوقه ومصالحه كافة[2].

ومن أمثلة هذه الجرائم : جرائم الاعتداء على الأمن الخارجي أو الداخلي للدولة أو الرشوة، أو الاختلاس وتزييف العملة وتزوير المستندات الرسمية، ولقد أسفرت الحياة العملية وقوع جرائم معلوماتية، تتدخل ضمن زمرة هذه الجرائم ؛ ولعل من أبرزها:

- العبث بالأدلة القضائية و التأثير فيها.
- تهديد السلامة العامة.

[1]– غانم مرضي الشمري، الجرائم المعلوماتية ماهيتها–خصائصها–كيفية التصدي لها، دار الثقافة للنشر والتوزيع، الأردن، 2016، ص 157.

[2]– محمود نجيب حسني، شرح قانون العقوبات ،القسم الخاص، دار النهضة العربية بالقاهرة، 1988، ص 11.

- بث البيانات من مصادر مجهولة.
- جرائم تعطيل الأعمال الحكومية
- الحصول على معلومات سرية.
- الإرهاب الإلكتروني[1].

8 .**جرائم مزادات الانترنت** : جرائم الاحتيال عبر مزادات الأنترنت متعددة الصور ؛ ومن أبرزها :

- **الاحتيال و عدم التسليم أو التوصيل:**

وطبقا لهذه الطريقة يقوم البائع بعرض صنف معين للبيع من خلال المزاد؛ وفي حقيقة الأمر هذا الصنف وهمي وغير موجود أصلا، وفي المحصلة النهائية لا يتسلم المشتري شيئا على الإطلاق بعد انتهاء المزايدة على الصنف، وفي حالة حصول الدفع بواسطة بطاقة ائتمانية فإن البائع المحتال يحصل على رقم البطاقة واسم المشتري؛ ويسئ استخدام هذه البطاقة .

- **الإحتيال وخداع المشتري حول القيمة الحقيقية للصنف المعروض للبيع:**

ومن صور الاحتيال عبر الإنترنت : قيام البائع بمحاولة خداع المشتري حول القيمة الحقيقية للصنف المعروض للبيع، ويمكن ذلك من خلال إدراج معلومات كاذبة ومضللة حول هذا الصنف، وذلك عن طريق استخدام صور معينة بخلاف الصورة الحقيقية للصنف المعروض؛ أو تصوير ذلك الصنف، ومن ثم تعديل هذه الصور ليبدو الصنف بحالة أفضل مما هو عليه حقيقة.[2]

- **الاحتيال بطريقة المثلث:**

وهذه الطريقة تخلص في أن علاقة البيع والشراء تكون ثلاثية الأطراف، المحتال والمشتري وشركة تبيع على الإنترنت ،وطبقاً لهذه الطريقة : يقوم المحتال بشراء البضائع من الشركة البائعة باستخدام بطاقات ائتمانية مسروقة أو مزورة، ثم يقوم ببيع هذه البضائع من خلال مزادات

[1]–حسين شفيق، الإعلام الجديد و الجرائم الالكترونية ،الإرهاب الالكتروني، دار الفكر للطباعة و النشر و التوزيع،2015، ص 175-192 .

[2]–يوسف حسن يوسف، الجرائم الدولية للأنترنت، المركز القومي للإصدارات القانونية،ط1، 2011،ص 293 .

الانترنت لأحد المشترين، والذي يقوم بتحويل أثمان البضائع إلى البائع المحتال؛ والذي بدوره يرسل البضائع إلى المشتري.

وفي حالة اكتشاف تزوير أو سرقة البطاقة الائتمانية تقوم الشرطة باستجواب المشتري البريء، وتصادر البضائع كدليل للتحقيق، وينتهي الأمر بأن يصبح كل من المشتري والشركة ضحايا للمحتال؛ الذي خرج من مثلث هذه الطريقة الإحتيالية؛ لتدخل بدلاً منه الدولة أو جهات التحقيق والمحاكمة .

- تجارة بضائع السوق السوداء :

ومن صور جرائم المزادات عبر الإنترنت : تجارة بضائع السوق السوداء ، وذلك بعرض هذه البضائع عبر مزادات الإنترنت، ومن هذه البضائع، أنظمة حاسب منسوخة أو اسطوانات موسيقية وفيديو منسوخة، ويتم تسليم البضائع دون تغليف أو كفالة أو حتى تعليمات الاستخدام، وأحياناً تشمل هذه التجارة، بيع القطع الأثرية على شبكة الانترنت والتي تكون محرمة في بعض الدول.

- المزادات الصورية [1]:

ونقصد بالمزادات الصورية : قيام مواقع المزادات بعمليات مزايدة متعددة، وذلك بهدف شراء صنف معين بسعر منخفض، أو بيع صنف بسعر مرتفع.

والصورة الأولى – شراء صنف معين بسعر منخفض – يقوم بها المشتري المحتال ويحدث هذا عند قيام أحد المشترين بعرض أثمان مختلفة سواء مرتفعة أم منخفضة للصنف ذاته، وذلك عن طريق استخدام ألقاب وأسماء متعددة على الشبكة، حيث تدفع عروض الشراء بالأثمان المرتفعة بالسعر لأن يصعد سريعا ويبلغ مستويات عالية ؛ الأمر الذي يخيف المشترين الآخرين عند ارتفاع السعر ويثنيهم عن استكمال المزايدة، وعليه وفي الدقائق الأخيرة من المزاد يقوم المشتري نفسه بسحب عروض الشراء العالية التي قدمها، ومن ثم شراء الصنف بأقل الأسعار.

[1]– يوسف حسن يوسف، المرجع السابق، ص 294 .

والصورة الثانية – أي بيع صنف معين بسعر مرتفع – يقوم بها البائع المحتال:

وذلك عن طريق التضخيم الزائد للسعر من قبل البائع بهدف رفع السعر إلى أعلى مستوى ممكن، إذ يقوم البائع وشركاء له بالتصرف كمشترين مختلفين باستخدام أسماء مختلفة ؛ وذل بهدف رفع السعر إلى أعلى مستوى ممكن.

- جرائم مزودي الخدمات :

وهذه الجرائم تضم كافة الأفعال التي يقوم بها المورد أو المتعهد المستضيف، أو متعهد الإيواء لخدمات الانترنت؛ وذلك مثل : مواقع الاستضافة وشركات توفير الخدمة، وغيرها من الجهات التي يفترض أن تقوم بتوفير وتأمين الخدمة وبتنظيم وتخزين المضمون الذي يسمح للموردين المستخدمين بالوصول إلى الجمهور؛ وذلك من خلال توريد الخدمات إلى مواقع خارجية، وهذه الخدمات من الممكن أن تكون خدمات إجبارية أو علمية .

كما أن هذه الأفعال يمكن أن تنطوي على : تقديم مواد غير مصرح بها للجمهور أو إفشاء أسرار أو مساساً بحق الإنسان في احترام حياته الخاصة [1].

وخلاصه لما سبق يمكن القول ان جرائم الانترنت هي" أفعال تتم عبر شبكة الانترنت، مخالفة للقانون والتنظيمات المعمول بها، وتلحق أضرار بنظام المعلومات أو بالأموال أو الأشخاص أو النظام العام " وبذلك يمكن إخضاعها للنصوص التقليدية، أمام قصر القوانين التي تحمي المعلوماتية وتجرم كل ما يمكن أن يعد فعل غير مشروع يرتكب من خلال شبكة الانترنت، ويلحق أضرار للغير سواء في شخصه أو ماله، تتناسب مع طبيعة وخصوصية هذه الجرائم .

وبتعبير آخر؛ نجد أن الجرائم المعلوماتية في حركة – مد – عنيفة، بينما التشريعات التقليدية وغير التقليدية في حركة – جزر– مخيفة [2].

---

[1]– يوسف حسن يوسف، المرجع نفسه، ص 295 .

[2] - Mahmoud saleh addle, Electronic Crime ,The ITU / BDT Arab Regional Workshop on, " Developing the Legislative Aspects for Combating Electronic Crime, " Muscat 2nd- 4th April 2006.

الفرع الرابع: أركان الجريمة الإلكترونية.

يتزايد الاهتمام العالمي بالجرائم المعلوماتية لحماية المصلحة العامة، التي تقتضي تأمين استخدام أجهزة الكمبيوتر وشبكة المعلومات الدولية (الانترنت)، من عبث العابثين الذي يتمثل في ارتكاب جرائم الأموال وجرائم الآداب وجرائم الإرهاب وجرائم السب والقذف، وجرائم غسل الأموال.

الأمر الذي أثر على حقوق الأفراد وحرياتهم، حيت وفرت الأنظمة المعلوماتية وسائل جديدة، في ايدي مجرمي المعلوماتية لتسهيل ارتكاب العديد من الجرائم، ومن هنا كان من الضروري أن تواكب التشريعات المختلفة هذا التطور الملحوظ في جرائم المعلوماتية.

و المواجهة التشريعية للجرائم الالكترونية، ضرورية للتعامل من خلال قواعد قانونية غير تقليدية لهذا الإجرام غير التقليدي، مواجهة تتعامل بشكل عصري متقدم مع جرائم المعلوماتية المختلفة، التي يأتي في مقدمتها الدخول غير المشروع علي شبكات الحاسبات، والتحايل علي نظم المعالجة الآلية للبيانات وإتلاف البرامج وتزوير المستندات المعالجة الكترونيا.

البند الأول : جريمة الدخول في نظام الكمبيوتر

تعاقب غالبية التشريعات المقارنة [1]الحديثة على الدخول في نظام الكمبيوتر،[2] غير أن موقف التشريعات الحديثة، تتباين في تجريم الدخول غير المصرح به، من هذه التشريعات ما يقيد تجريم الدخول بقيد يتعلق بالركن المعنوي، فيستلزم توافر قصد خاص لدى المتهم كما فعل المشرع

[1]– جرمت المادة 6 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010: جريمة الدخول غير المشروع:

1. الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.
2. تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:

- محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين.
- الحصول على معلومات حكومية سرية .

[2] -Alain BENSOUSSAN, Internet, aspects juridiques, éd. Hermes, 1998, p. 198 ,Martin WASIK, Computer Crimes and Other Crimes against Information Technology in the United Kingdom, Rev. int. dr. pén. 1993, p. 632.

الجزائري،[1] وهو قصد التأثير في البيانات أو التأثير في نظام الكمبيوتر نفسه أو قصد الحصول على بيانات تمس الأمن القومي أو الاقتصاد الوطني، للعقاب على هذا الدخول أو قصد التهديد أو الابتزاز.

1. الركن المادي في جريمة الدخول غير المشروع[2].

ويقصد بالدخول الاتصال بجهاز حاسب آلي خاص بشخص الغير بدون موافقته، ويتخذ الدخول صورا مختلفة؛ فمنها أن يقوم الفاعل بتشغيل جهاز مغلق وبالتالي الاطلاع على ما به من بيانات، ومنها ما يقوم به الفاعل من استخدام برامج للدخول في النظام بدون إذن صاحبه، فيطلع على ما يقوم به صاحب الجهاز أو ينتقل بين أجزاء الجهاز، ليطلع على ما يحتويه أقسام هذا الجهاز من معلومات.

وقد إستعمل نظام مكافحة جرائم المعلوماتية تعبير "الدخول غير المشروع" ويقصد به الدخول بدون وجه حق، وبالتالي فإنه لا يعد دخولا غير مشروع إذا توافر رضاء صاحب النظام، كأن يكون هناك اتفاق بينهما أو كان الجهازان ينتميان إلى شبكة واحدة، وبالتالي فالجهازان متصلان بالشبكة ذاتها مما يفيد توافر الرضاء الضمني بدخول العاملين على الجهاز الخادم للشبكة إلى الأجهزة المنتمية إلى ذات الشبكة.

كما لا يعد من قبيل الدخول غير المشروع، أن يتم ذلك من جهة عامة لها الحق في مراقبة أجهزة الحاسب الآلي المتواجدة لدى الأفراد، مادام أن النظام يسمح لتلك الجهات بممارسة الحق في المراقبة، وقد يكون ذلك من ضمن الحالات التي يسمح بها النظام لمكافحة جرائم الإرهاب أو الجرائم المخلة بالآداب أو جرائم الماسة بأمن الدولة.

---

[1]- في قانون العقوبات الذي تمم العنصر الثالث من الباب الثاني من الكتاب الثالث من الأمر 156/66 بقسم سابع مكـــــرر عنوانه " المساس بأنظمة المعالجة الآلية للمعطيات " و يشمل المواد من 394 مكرر إلى 394 مكرر 7 ".

[2]- المشرع الجنائي الجزائري نص على هذه الحالة في المادة 394 مكرر قانون العقوبات: "يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 إلى 150000 دج".

2. الركن المعنوي في جريمة الدخول غير المشروع:

تنتمي هذه الجريمة إلى الجرائم العمدية، وبالتالي فإنه يلزم توافر القصد الجنائي من علم وإرادة، وبالتالي لو حدث الدخول بطريق الخطأ فإن الجريمة لا تقو.

ومؤدى ما سبق أن الدخول بدون وجه حق في حد ذاته لا المشرع الجزائري جريمة معاقبا عليها، ومع ذلك فإن المؤسس الدستوري و المشرع الجزائري يعاقب على التجسس على النظام أو التنصت، فمن يتداخل في جهاز غيره ويطلع فقط على ما يقوم به، دون أن يكون لديه قصد خاص معين من القصود سابقة الذكر (قصد التهديد أو الابتزاز، قصد العبث بالنظام أو البيانات الموجودة فيه أو قصد الإتلاف، قصد الحصول على بيانات تمس أمن الدولة أو الاقتصاد الوطني) لا يرتكب جريمة الدخول غير المشروع ولكنه يرتكب جريمة التنصت أو التجسس المحضور دستوريا[1] و تشريعيا[2] .

---

[1]- المادة 39من الدستور الجزائري رقم 16-01 ، تنص على ما يلي : لا يجوز انتهاك حُرمة حياة المواطن الخاصة وحرمة شرفه ويحميهما القانون.

- سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.
- لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية. ويعاقب القانون على انتهاك هذا الحكم.
- حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه.

انطلاقا من نص هذه المادة فان الدستور الجزائري يضمن سرية المكالمات الهاتفية وكل الاتصالات بأشكالها المختلفة من التنصت والمراقبة أو الاستماع أو النشر أو الإطلاع سواء كانت خطابات أو برقيات أو مستندات الخ ...

[2]- في المادة 303 ق ع ج وماء جاء به قانون 23/06 المؤرخ في 2006/12/20 تنص على ما يلي: "كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير و ذلك بسوء نية وفي غير الحالات المنصوص عليها قانونا في المادة 137 ، يعاقب بالحبس من شهر واحد(01) إلى سنة واحدة (01) وبغرامة من 25000 د ج إلى 100000 دج أو بإحدى هاتين العقوبتين .

- أما المادة 303 مكرر فتنص على أنه :" يعاقب بالحبس من ستة(06) أشهر إلى ثلاث (03) سنوات و بغرامة من 50000 د ج إلى 300000 د ج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك :

1- بالتقاط ، أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية في غير إذن صاحبها أو رضاه.

2 – في التقاط ، أو تسجيل أو، نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه.

يعاقب على الشروع في ارتكاب الجنحة المشار إليها في هذه المادة بالعقوبة ذاتها المقررة بالجريمة التامة .

إن صفح الضحية يضع حدا للمتابعة الجزائية .

البند الثاني : أركان جريمة العبث بالنظام أو بالبيانات

تقع تلك الجريمة بتوافر ركنين: الركن المادي والركن المعنوي. ويتكون الركن المادي من نشاط ونتيجة وعلاقة سببية، فهي إذن جريمة مادية أي جريمة ضرر وليست مجرد جريمة خطر كجريمة الدخول.

والعبرة ليس بطريقة معينة اتبعها الجاني، بل بقيامه بسلوك إيجابي يتمثل في استخدام أية وسيلة يحقق بها غاية معينة، وقد حددها النظام ضمن عدد معين من الأضرار منها أن يتوصل الجاني إلى إيقاف الشبكة المعلوماتية عن العمل.

كما يمكن أن يقع النشاط المعاقب عليه بأن يستعمل الجاني فيروسات، وهي برامج الغرض منها تدمير أو مسح المعلومات، بيد أن الجريمة لا تقع بمجرد زرع الفيروس ولكن بتحقيق نتيجة مادية معينة، وهي التدمير أو المسح للمعلومات أو اضطراب في سير النظام بحيث لا يعمل على الوجه المعتاد الصحيح.[1]

ومن صور النشاط المعاقب عليه، أن يقوم الفاعل بإعاقة النظام، من التطبيقات على ذلك أن أحد المتهمين كان يعمل مستخدما في إحدى الشركات، وقد استغنت عنه تلك الشركة، فغير كلمة المرور كونه كان عالما بها فترة عمله فعجز بقة العاملين استخدام الشبكة ،وتكبدت الشبكة خسائر فادحة من جراء ذلك ومن جراء تغيير الشبكة بعد ذلك.[2]

وتختلف جريمة العبث بالنظام أو بالبيانات عن جريمة الدخول بقصد العبث بالنظام أو بالبيانات، في الركن المادي في كلتا الجريمتين؛ ففي الجريمة الأولى لا تقع الجريمة إلاّ بتحقق نتيجة معينة، وهو الضرر المتمثل في العبث بالنظام أو بالبيانات، بينما تقع الجريمة الثانية بمجرد التداخل إذا كان قصد المتداخل هو العبث بالنظام أو بالبيانات ولو لم يتمكن من تحقيق غايته في إلحاق الضرر بهذا النظام أو بتلك البيانات[3].

---

[1] -Alain Bensoussan, Internet, aspects juridiques, éd. Hermes , 1998, p. 200

[2] -Nevada Cybercrime Task Force Nets Hacker, U.S. Department of Justice, Press Release: *http://www.cybercrime.gov/sanduskyPlea.htm. 2004.*

[3] - VIVANT Michel et autres , Droit de l´informatique et des réseaux , Lamy 2001, p.1810.

الفرع الخامس: دوافع ارتكاب الجرائم المتعلقة بشبكة الإنترنت. [1]

الدافع أو الباعث هو العامل المحرك للإرادة الذي يوجه السلوك الإجرامي، كالمحبة والانتقام، فهو عبارة عن قوة نفسية تدفع الإرادة إلي الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة، وهو يختلف من جريمة إلى أخرى تبعا لاختلاف الناس من حيث السن والجنس ودرجة التعليم وغير ذلك من المؤثرات، كما أنه يختلف بالنسبة للجريمة الواحدة من شخص لأخر[2].

وفي هذه الفئة المستحدثة من الجرائم، ثمة دوافع عديدة ومتنوعة تحرك الجناة لارتكابها قد تكون من أجل المعلومات التي تكون إما محفوظة على أجهزة الحاسبات الآلية أو منقولة عبر شبكة الإنترنت، وقد تكون من أجل الإضرار بأشخاص أو جهات معينة، وقد تكون سعيا وراء الربح المادي أو إبراز الذات وغيرها[3]:

يمكن القول إن ضريبة التقدم لم تكن يوماً منخفضة، ولكن ضريبة التخلف عن مواكبته والارتقاء إلى مستوى تحمل المسؤولية التي تترتب عليها كانت على الدوام أشد وطأة وأغلى كلفة بكثير، فهذا التطوّر الكبير لشبكة الإنترنت لم يكن مصحوبًا بقواعد قانونية واضحة، إذ أنها لا تغطي مجموعة واسعة من الجرائم عبر الإنترنت ولا تقيم حدودًا واضحة لما هو مقبول أو مرفوض، فالتطبيق الضعيف لقوانين مكافحة هذا النوع من الجرائم وخطورة هذه المسألة يتطلب المزيد من التشريعات والتعاون الدولي.

أمام هذا الواقع القانوني الذي يتخطى الحدود الوطنية، حاولت مؤخرًا عدة دول، من خلال عدد من المعاهدات، معالجة هذه التحديات لأنه لا يوجد حتى هذه اللحظة نظام عالمي لمكافحة مساوئ الإنترنت.

---

[1]- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي، دار الفكر الجامعي، الإسكندرية،2004م، ص ص 13-15 .

[2]- فوزية عبد الستار، شرح قانون العقوبات، القسم العام، دار النهضة العربية : القاهرة، 1992م، ص 479.أيضا منصور محمد عقيل وعلى قاسم ، الإنترنت والأبعاد الأمنية ، مركز البحوث والدراسات الشرطية ، دبي، 1996،ص 12.

[3]- منير محمد الجنبيهي وممدوح محمد الجنبيهي، المرجع السابق، ص ص 16-17 .

see :Bruce sterling ,The hacker Crackdown law and Disorder on the Electronic frontier,1994, p.159.

كذلك آمنة على يوسف، قراصنة الكمبيوتر، المؤتمر القومي الثالث عشر لأمن الكمبيوتر بواشنطن بالولايات المتحدة الأمريكية،1998 ،ص 8.

وفي الواقع، لا يمكن معالجة التحديات القانونية والفنية والتنظيمية المتعلّقة بالأمن السيبراني بشكلٍ صحيح إلا من خلال اعتماد استراتيجية على المستوى الدولي يشارك فيها جميع ذوي العلاقة لمعالجة الأمر، و هذا ما سنتناوله في الباب الثاني من الرسالة الموسوم بـــ التعاون الحمائي في مواجهة مخاطر الأمن المعلوماتي، من خلال فصلين ندرس الأول سبل مواجهة مهددات الأمن ألمعلوماتي و نختم أوراق الرسالة بالفصل الثاني المعنون بـــ الجهود الدولية في مجال الأمن ألمعلوماتي

الباب الثاني

التعاون الجنائي في مواجهة مخاطر الأمن المعلوماتي

الباب الثاني:

التعاون الحمائي في مواجهة مخاطر الأمن المعلوماتي.

العصر الرقمي قاب قوسين أو أدنى من مميزات و محاسن، تجعل الحياة سهلة بتلبية الخدمات للمستفيدين في وقت قياسي، نظرا لتدفق اللامتناهي للمعلومات في كافة قطاعات المعرفة البشرية في أي وقت من الاوقات، ومفاسد وإفرازات سلبية تشكل معاناة يتم العمل على التصدي لها بجهود دولية ووطنية، ومن أكبر السلبيات ما اصطلح على تسميته بأمن المعلومات، واستدعى الأمر بناء جوانب قانونية وفنية لحماية المعلومات، أو بعبارة أخرى تحقيق ''أمن المعلومات"،وبيان المخاطر التي تهدد المعلومات ومصادرها وآليات ووسائل وأدوات الحماية التقنية والإدارية للمعلومات، واستراتيجيات الحماية القانونية للمعاملات الرقمية والبنوك الإلكترونية ومعرفة موقف التشريعات الوطنية، الإقليمية و الدولية منها، وحجية الإثبات في المعاملات الرقمية والتجارة الإلكترونية، وأمن وسلامة نظم المعاملات الإلكترونية في البنوك والمؤسسات المالية والمصرفية، والتكييف القانوني لأشكال الاعتداءات أو الدخول غير المشروع على الشبكة، وتدمير الشبكات أو تعطيلها أو الاستيلاء عليها وانعكاس ذلك على البنى المؤسسية في المجتمعات، وأنماط الإنتاج والروابط الدولية، فهو أمر ذي أبعاد تراكمية طويلة الأمد[1].

ومن هنا أصبح حل مسألة البحث عن إطار استراتيجي عالمي، لأصحاب المصلحة–مؤسسات وأفراد– من أجل التعاون الدولي والحوار والتنسيق في مواجهة مخاطر الأمن المعلوماتي، و هذا هو محك القضية وذاك هو الجذع الذي تترامى عليه باقي أوراق الرسالة في دراسة الفصلين التاليين :

- الفصل الأول : سبل مواجهة مهددات الأمن ألمعلومات.
- الفصل الثاني : الجهود الدولية في مجال الأمن ألمعلوماتي.

[1]– أنطون زحلان، الطبيعة الشاملة للتحدي التقني، مجلة المستقبل العربي،العدد263، بيروت،2001، ص52.

الفصل الأول :

سبل مواجهة مهددات الأمن المعلوماتي.

تعتبر مسألة المخاطر والتهديدات السيبرانية، من المسائل الحساسة في المؤسسات العامة والخاصة التي تقوم بأثمنة معلوماتها، فهذه المخاطر والتهديدات السيبرانية تتعدد وتتنوع في عالمنا اليوم مع زيادة المعاملات الرقمية، وعدم الوعي بكيفية الحماية منها-المبحث الأول - فسواء كانت هذه التهديدات عبر اختراق البريد الإلكتروني أو اختراق الحساب الخاص على الشبكات الاجتماعية، أو غيرها من أشكال المخاطر التي قد تهدد الأفراد والمؤسسات، فيجب علينا جميعًا أن نبذل جهدًا إضافيًا للتصدي لهذه النشاطات غير المشروعة والمخاطر، واتخاذ التدابير الوقائية والاستجابة السريعة ضدها من أجل خلق "توازن ردع نسبي و إضفاء الحماية والبقاء آمنين على شبكة الإنترنت -المبحث الثاني- .

وفيما يلي نتعرض لأسئلة هذا الفصل محاولين الاجابة حول ما الذي يجب حمايته؟ وممن نحميه؟ ولماذا نحميه؟ وخطوات الحماية الحالية، وتجربة لأهم الدول في هذا المجال؟ ثم ما هو المطلوب للوصول إلى منظومة حماية متكاملة للبيانات المتداولة عبر الشبكات؟

المبحث الأول : أمن المعاملات والمعلومات الإلكترونية.

تعدد المخاطر الناتجة عن استخدام الانترنت، منها ما يتخذ شكل انتحال الغير شخصية شخص آخر عن طريق سرقة الكلمات السر الخاصة به، أو تسجيل بعض الوسائل و إعادة إرسالها، بالإضافة إلى إمكانية اختراق الموقع و العبث بمحتوياته و الاستخدام غير المرخص به و العديد من المخاطر الأخرى [1]

و للحماية من تلك الأخطار يتعين استخدام مجموعة من التقنيات، اثبت الواقع العلمي ضرورة الاعتماد عليها للحفاظ على استقرار المعاملات عن طريق الانترنت، وسنقوم من خلال هذا المطلب بدراسة أهم التقنيات المستخدمة للتحقق من هوية العميل في(المطلب الأول)، واهم الوسائل المستخدمة في حماية أمن المراسلات و المواقع الإلكترونية في (المطلب الثاني).

المطلب الأول: أمن المعاملات من طرف سلطات الموثوقية في الجزائر.

التصديق الإلكتروني من المبادرات الرئيسية لتحقيق أهداف الإدارة الإلكترونيّة؛ إذ يضع البنية الأساسيّة اللازمة للجهات الحكومية لتوفير الخدمات الإلكترونية، بما من شأنه رفع فاعلية الحكومة وتسهيل المعاملات على المواطنين والمقيمين، كما يسهم في رفع مستوى الأمن والمصداقيّة في التعاملات الإلكترونية؛ إذا يعتبر التصديق الإلكتروني الحل التقني و القانوني الذي يساعد مستخدمي الإنترنت، على تبادل المعلومات بأمان وسرية عن طريق استخدام الهوية الإلكترونية، والهواتف النقالة[2].

ويهدف السلطة الوطنية للتصديق الإلكتروني في الجزائر إلى توفير تقنيات آمنة، لتوثيق المعلومات وتصديقها إلكترونيًّا، وتحديد هوية المستخدمين والمصادقة عليها، والتوقيع على جميع المعاملات إلكترونيًّا من خلال استخدام الهوية الإلكترونية.

---

[1] –حسن طاهر داوود ، امن الشبكات المعلومات، معهد الإدارة العامة، السعودية، 2004 ، ص 101و ما بعدها .

[2]- مثال عن المواقع الخاصة بخدمة التوثيق الالكتروني:

- ✓ CertCo , http://www.certco.com
- ✓ VeriSign, http://digitalid.verisign.com/
- ✓ Infrastructure à clés publiques du gouvernement du Canada,
- ✓ http://www.cse.dnd.ca/cse/francais/gov.html

BelSign (Belgique & Luxembourg), www.kpmg.com.au/certauth.html

و بما أن التبادلات على شبكة الإنترنت، تتم من خلال شبكة مفتوحة لا تحتوي على أي وجود مادي، لذا فلا يمكن التعرف على هوية الأشخاص الذين نتواصل معهم، فالعالم الافتراضي يعرضنا لعدد من المخاطر مثل سرقة الهوية، واعتراض الآخرين على رسائل الغير و استنكار عملية بيع أو دفع أو تبادل، وعليه فإن وضع أجهزة أمنية مثل التصديق الإلكتروني بات من إحدى الضروريات.

تعدّ سلطة التصديق مسؤولة قانونا، عن ضمان وجود صلة رسمية بين الشخص والمفتاح العمومي، كجزء من بنية ذات مفتاح عمومي، ويتمثل دورها في التحقق من دقة المعلومات الواردة في الشهادة الالكترونية التي تصدرها، والتأكد من صحة الوثيقة مقابل شخص آخر...[1] هو:

- الموثق الإلكتروني هذا الأخير هو طرف ثالث محايد يتمثل في أفراد أو شركات أو جهات مستقلة محايدة تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الإلكترونية.

والوظيفة الأساسية للموثق الإلكتروني أو لجهة التوثيق الإلكترونية، هي تحديد هوية المتعاملين في التعاملات الإلكترونية، وتحديد أهليتهم القانونية في التعامل والتحقق من مضمون هذا التعامل، وسلامته وكذلك جديته وبعده عن الغش والاحتيال[2].

---

[1]- الفقرة 1 من المادة 53 من القانون 15-04 صحة جميع المعلومات الواردة في شهادة التصديق الإلكتروني، الموصوفة في التاريخ الذي منحت فيه ووجود جميع البيانات الواجب توفرها في شهادة التصديق الإلكتروني، الموصوفة ضمن هذه الشهادة .

- الفقرة 2 من المادة 53 التأكد عند منح شهادة التصديق الإلكتروني، أن الموقع الذي تم تحديد هويته في شهادة التصديق الإلكتروني الموصوفة، يحوز كل بيانات إنشاء التوقيع الموافقة لبيانات التحقق من التوقيع المقدمة و / أو المحدّدة في شهادة التصديق الإلكتروني .

[2]- أعلن القانون الجزائري المتعلق بالتوقيع والتصديق الالكتروني15-04 عن إنشاء ثلاث سلطات للتصديق الالكتروني إحداها وطنية لدى الوزير الأول وهي سلطة مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، تكلف بترقية استعمال التوقيع والتصديق الالكترونيين وتطويرهما وضمان موثوقية استعمالهما، حيث تتولى مهمة إعداد سياسة التصديق الالكتروني والسهر على تطبيقها مع الموافقة على تلك السياسات الصادرة عن السلطتين الحكومية والاقتصادية للتصديق، أما السلطة الحكومية للتصديق الالكتروني فتنشأ لدى الوزير المكلف بالبريد وتهتم بتوفير الخدمات لكافة المتدخلين، أما السلطة الاقتصادية فتكمن مهمتها في إعداد دفتر شروط يحدد كيفيات تأدية خدمات التصديق الالكتروني مع مراقبة ومتابعة المتعاملين الموفرين لهذه الخدمة بالنسبة للمواطنين، من خلال اتخاذ التدابير اللازمة لضمان استمرارية الخدمات في حال العجز والتحقق من مطابقة طالبي التراخيص مع سياسة التصديق الالكتروني بنفسها، والتحكيم في النزاعات القائمة بين المتعاملين في المجال.. سعيد باتول، كل التفاصيل حول التوقيع والتصديق الالكترونيين، مقال منشور بتاريخ2015/03/10 ، متوفر على الرابط التالي : http://www.echoroukonline.com/ara/articles/236134.html

ويأخذ التوجيه الأوروبي رقم 93 سنة 1999 المتعلق بالإطار المشترك للتوقيع الالكتروني، و الذي وضع نظاما لتلك الخدمة، والذي ادخل في القانون الداخلي الفرنسي بداية من 13 مارس 2000 [1] بفكرة الموثق الإلكتروني، وأطلق عليه تسمية مقدم خدمات التصديق،[2]

وهي نفس التسمية التي جاء بها المشرع الجزائري في المرسوم التنفيذي07-162، والقانون الجزائري المحدد القواعد العامة بالتوقيع و التوثيق الالكترونيين رقم 04 لسنة 2015، و بموجب هذا الأخير حتى يتمكن مقدمي خدمات التصديق الإلكتروني[3] ممارسة نشاط التصديق الإلكتروني، يتطلب عليه الحصول على ترخيص تمنحه سلطة البريد والمواصلات السلكية واللاسلكية[4]، وهذا الترخيص يكون مرفق بدفتر الشروط يحدد حقوق وواجبات مؤدي الخدمات والمستعمل.

---

[1]– Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques .Journal officiel n° L 013 du 19/01/2000 p12 – 20.

[2] – نسرين عبد الحميد نبيه، الجانب الإلكتروني للقانون التجاري، منشأة المعارف، الإسكندرية، 2008، ص29.
Conformément à la définition par la directive européen 1999/93/CE- Article 2 11 /"prestataire de service de certification", toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques.

[3] – الفقرة 12 من المادة الثانية من القانون 15-04 مؤدي خدمات التصديق الإلكتروني: شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني، كذلك المادة 20من القانون المغربي ظهير رقم 1.07.129 صادر في 19 من ذي القعدة 1428 ،30 نوفمبر 2007، بتنفيذ القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية" مقدمو خدمات المصادقة الإلكترونية المعتمدون دون غيرهم، الذين يمكنهم إصدار شهادات إلكترونية مؤمنة، وتسليمها وتدبير الخدمات المتعلقة بها وفق الشروط المحددة في هذا القانون والنصوص المتخذة لتطبيقه ".

[4] – المادة 29 من القانون 15-04 تعين السلطة المكلّفة بضبط البريد و المواصلات السلكية واللاسلكية في مفهوم هذا القانون سلطة اقتصادية للتصديق الإلكتروني، و المادة 33: من القانون 15-04 يخضع نشاط تأدية خدمات التصديق الإلكتروني إلى ترخيص تمنحه السلطة الاقتصادية للتصديق الإلكتروني

أما عن الأشخاص الذين يجوز لهم قانونا ممارسة هذا النشاط، يجب أن تتوفر فيهم نفس الشروط لممارس نشاط تقديم الانترنت في الجزائر[1].

ويتعين على كل متعامل يرغب في تأدية نشاط خدمات التصديق الحصول على ترخيص تمنحه السلطة الاقتصادية للتصديق الالكتروني أن يستوفي شرط الجنسية الجزائرية سواء كان شخصا طبيعيا أو معنويا ويتمتع بقدرة مالية كافية مع التمتع بمؤهلات وخبرة كافية في مجال تكنولوجيات الإعلام والاتصال، إضافة إلى خلوه من أي متابعة قضائية حكمت عليه فيها في جناية أو جنحة تتنافى مع النشاط .

وعن مدة صلاحية شهادة التأهيل قبل الحصول على الترخيص اللتان تمنحان بصفة شخصية فقد حدد بسنة واحدة قابلة للتجديد مرة واحدة، مع تبليغ الشهادة في اجل أقصاه 60يوما ابتداء من تاريخ استلام الطلب المثبت بإشعار الاستعلام، إلا انه لا يسمح له بتأدية الخدمة إلا بعد الحصول على الترخيص الذي حددت مدة صلاحيته بخمس سنوات قابلة للتجديد، الذي يتعين أن يكون مرفقا بدفتر شروط يحدد كيفيات وشروط تأدية خدمات التصديق الالكتروني.

وفي حال الإخلال بأحكام دفتر الشروط من طرف مؤدي خدمات التصديق الالكتروني، فإنه يتعرض لعقوبة مالية تتراوح ما بين 20مليونا و 500مليون سنتيم، أما في حال انتهاكه للمقتضيات التي يتطلبها الأمن القومي والدفاع الوطني فتقوم السلطة الاقتصادية بالسحب الفوري للترخيص مع حجز كافة التجهيزات والمعدات بشكل تحفظي، بينما يعاقب كل من أدلى بإقرارات كاذبة وأخل عمدا بتحديد هوية طالب شهادة التصديق ما بين 3أشهر و 3سنوات سجنا.

أما عن شهادة التصديق الالكترونية، فهناك من قام بتعريف شهادة التصديق الالكترونية[2] بأنها : شهادة تصدرها جهة وسيطة أو جهة ثالثة ما بين طرفين متعاملين بالطريق الالكتروني، و يكون مضمون هذه الشهادة صحة البيانات المتبادلة بين الطرفين، و يقرر بأن شهادة التصديق الالكترونية هي صك أمان يفيد صحة وضمان المعاملة الالكترونية من حيث صحة البيانات و مضمون المعاملة و كذلك أطرافها[3] .

[1] – المادة 3 من المرسوم التنفيذي 07-162 المؤرخ في 30 ماي 2007 الصادر في الجريدة الرسمية عدد 37 لسنة2007 والذي نظم نشاط التصديق الالكتروني من خلال إخضاعه إلى نظام الترخيص الوارد في المادة 39 من القانون 2000-03 المؤرخ في 5 أوت 2000 المحدد للقواعد العامة المتعلقة بالبريد و الاتصالات السلكية و اللاسلكية.

[2] –المادة 2 من القانون 15-04 المؤرخ في 1 فبراير 2015المحدد للقواعد العامة للتوقيع و التصديق الالكترونيين قد عرفت شهادة التصديق الإلكتروني : وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني و الموّقع . كما عرفها المشرع المغربي في المادة 10من القانون رقم 53.05

[3] – عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، دار الفكر الجامعي بالإسكندرية، 2004, ص 161، مشار اليه عند درار نسيمة ، المرجع السابق، ص ص 49-50.

وبذلك تكون جهة التوثيق الالكتروني، مسئولة عن توثيق المعاملات الرقمية، الأمر الذي يجعل الوضع تطبيقا لمهمة الموثق العادي.

الفرع الأول: واجبات مقدمي خدمات المصادقة [1]:

إن تدخل شخص ثالث من الغير (مقدم خدمة المصادقة)، مستقل عن الأطراف وحده يتيح تقوية فاعلية نظام التوقيع الإلكتروني[2]، لهذا فرض المشرع الجزائري على عاتق مقدمي خدمات المصادقة أو الشخص الثالث التزامات، يتعين عليهم مراعاتها عند إصدار الشهادات الإلكترونية، وبما أن مقدمي خدمات المصادق يقومون بالتحري عن سلامة المعلومات التي تجمعها من حيث مضمونها ومحتواها وصحة صدورها ممن تنسب إليه، وتصدر بذلك شهادة تصديق إلكترونية تشهد فيها بذلك، ويتم الاعتماد عليها في إتمام المعاملات الإلكترونية، إلا أنه قد يحدث أن يفشلوا أو يقصروا أحيانا في التحري عن صحة المعلومات التي اعتمدوا عليها، ويعملوا على إصدار شهادات إلكترونية غير مطابقة للواقع، وقد لا يتم اكتشاف ذلك إلا بعد إتمام المعاملة الإلكترونية، اعتمادًا على هذه الشهادات غير الصحيحة، فتخل هذه الشهادات بالثقة المشروعة التي أولاها المتعاملون في عمل مقدمي خدمات المصادقة والشهادات التي أصدروها، وعندها تثار مسؤوليتهم تجاه من أصابه ضرر إثر تعامله اعتمادًا على هذه الشهادات غير الصحيحة .

---

[1] – طارق كميل، مقدمو خدمات المصادقة الإلكترونية، التنظيم القانوني واجباتهم ومسؤولياتهم، مجلة جامعة الشارقة للعلوم الشرعية و القانونية، المجلد 5،العدد3،أكتوبر2008،ص253.

2 – Pour la législation française :la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié. Les certificats délivrés par des prestataires de services de certification électronique qualifiés sont présumés qualifiés. L'arrêté du 26 juillet 2004 encadre et définit la reconnaissance de la qualification des prestataires de services de certification électronique.

1. la loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique ;
2. le décret n°2001-272 du 30 mars 2001, pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, modifié par le décret n°2002-535 du 18 avril 2002 .
3. le décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;
4. la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés .

- حتى يقوم مقدمو خدمات المصادقة بدورهم على أكمل وجه، يتوجب عليهم أن يتقيدوا بالالتزامات التي تهدف إلى حماية المعلومات الشخصية، وتلك التي تتعلق بصحة المعلومات موضوع شهادة المصادقة[1].

الفرع الثاني : الالتزامات التي تهدف إلى حماية المعلومات الشخصية.

يقع على عاتق مقدم خدمة المصادقة الالكترونية، العمل على حماية المعلومات الشخصية والتي تدور حول الالتزام بالسلامة والالتزام بالإعلام والنصح والالتزام بالحفاظ على المعلومات ذات الطابع الشخصي،[2] وعليه سنعمل على تناول هذه الالتزامات حسب الآتي:

البند الأول: التزام السلامة

يقع على عاتق مقدم خدمة المصادقة، أن يقدم ضمانات كافية حتى يتمكن من ممارسة نشاطه، وبالتالي استعمال نظامٍ معلوماتي موثوقٍ به، وأن يقوم بحماية مفتاحه الخاص الذي يستعمله لتوقيع شهادات المصادقة الصادرة عنه وذلك بشكل ملائم.[3]

وفي جميع الأحوال يلتزم مقدمو خدمات المصادقة، باعتماد آلية لإنشاء التوقيع الإلكتروني من الجهة الإدارية المختصة بالدولة، ولا يجوز لهم تعديلها إلا بعد الحصول على الموافقة الكتابية من الجهة الإدارية، وكذلك يلتزم مزود الخدمة أو مقدم خدمة المصادقة، باعتماد قائمة الأجهزة والإدارات الخاصة، بإنشاء وتثبيت التوقيع الإلكتروني من الجهة الإدارية، كما تلتزم بتوفير نظام صيانة للأجهزة يعمل طوال 24 ساعة في اليوم، ويجب تأمين كل هذا بوسائل التأمين المتعددة ضد المخاطر المتوقع حدوثها، وأخيرًا يجب على هذه المنظومة أن تكون قادرة على إلغاء الشهادة أو التوقيع الإلكتروني، أو إيقافها بناء على طلب صاحبها، أو في الحالات التي يحددها القانون والنظام.

---

[1] – المادة 53 مت القانون 15-04 يكون مؤدي خدمات التصديق الإلكتروني، الذي سلم شهادة تصديق إلكتروني موصوفة، مسؤولا عن الضرر الذي يلحق بأي هيئة أو شخص طبيعي أو معنوي، اعتمد على شهادة التصديق الإلكتروني هذه ...

[2] –هذه الالتزامات ورد النص عليها في مختلف التشريعات المقارنة، ومنها نص المادة 9 من قانون الأونسترال النموذجي المتعلق بالتوقيعات الإلكترونية لسنة 2001 ونص المادة 24 من قانون إمارة دبي الخاص بالمعاملات والتجارة الإلكترونية لسنة2002 ، ونص الفصل 15 من قانون المبادلات والتجارة الإلكترونية التونسي.

[3] – وسيم شفيق الحجار، الإثبات الإلكتروني، مكتبة صادر ناشرون، بيروت لبنان،2002 ، ص 326 وضياء أمين مشيمش "التوقيع الالكتروني، دراسة مقارنة، منشورات صادر الحقوقية، بيروت، لبنان، سنة النشر غير مذكورة، ص 16.

ويجب على عاتق مقدم خدمة المصادقة أن تكون لديه القدرة على إنشاء منظومة تكوين البيانات الإلكترونية، التي يباشر من خلالها إنشاء التوقيع الإلكتروني، وفي العادة فإن هذه المنظومة تكون مؤمنة عند استيفائها للشروط التالية:

1. الطابع المنفرد لبيانات إنشاء التوقيع الإلكتروني.
2. سرية بيانات إنشاء التوقيع الإلكتروني.
3. عدم قابلية الاستنتاج أو الاستنباط لتلك البيانات.
4. حماية التوقيع الإلكتروني من التزوير أو التقليد أو التحريف أو الاصطناع أو غير ذلك من صور التلاعب.
5. عدم إحداث أي إتلاف بمحتوى المحرر الإلكتروني أو توقيعه.
6. أن لا تحول هذه المنظومة دون علم الموقع علمًا تامًا بمضمون المحرر الإلكتروني قبل توقيعه له.

البند الثاني : الالتزام بالإعلام والنصح.

إن التوقيع الإلكتروني والإجراءات التقنية المعدة لتطبيقه، تعد إجراءات معقدة وغامضة، ومن أجل تعزيز ثقة المتعاملين بالتوقيع الإلكتروني، يقع على عاتق مقدم خدمة المصادقة، أو مزودي خدمات المصادقة الإلكترونية، الالتزام بإعلام المتعاملين معه بشكل واضح بطريقة استعمال خدماته وبكيفية إنشاء التوقيع وكيفية التحقق منه.

البند الثالث: الالتزام بالحفاظ على المعلومات ذات الطابع الشخصي. [1]

من أجل قيام مقدم خدمة المصادقة بوظيفته، بالتعرف على صاحب شهادة المصادقة يعمل على جمع المعلومات عن الشخص المذكور، ويقع على عاتقه الالتزام بالأحكام المتعلقة بحماية

[1] –لقد نص الفصل15 من قانون المبادلات والتجارة الالكترونية التونسي على أنه) يتعين على مزود خدمات المصادقة الإلكترونية، وأعوانهم المحافظة على سرية المعلومات، التي عهدت إليهم في إطار تعاطي أنشطتهم باستثناء تلك التي رخص صاحب الشهادة كتابيًا أو الكترونيًا في نشرها أو الإعلام بها، أو في الحالات المنصوص عليها في التشريع الجاري به العمل"، وبناءً على ذلك فإن المشرع عمل على حماية المعلومات والبيانات التي يتداولها مزود خدمة المصادقة الإلكترونية والتي تخص العملاء، وحظر عليه المشرع أو من يعمل معه إفشاء سرية هذه البيانات، وعدم الإفصاح عنها إلا إذا رخص له بذلك قانونًا.

الأشخاص الطبيعيين عند معالجة المعلومات ذات الطابع الشخصي، [1]في حال التداول الحر لهذه المعلومات، ويتعين عليه الاكتفاء بالمعلومات الضرورية[2] لإنشاء الشهادة دون أي معلومات أخرى، كما لا يمكنه استعمال هذه المعلومات إلا في إطار وظيفته كمقدم لخدمة المصادقة، ولا يمكنه بأي شكل من الأشكال إدارة المعلومات المجمعة واستثمارها في أغراض أخرى إلا بعد الحصول على موافقة المتعامل أو تبعا للحالات التي يجيزها المشرع .

المطلب الثاني : الإستراتيجية الوطنية للجزائر الالكترونية[3].

تعتبر الجهود التي تبذلها الجزائر لترقية قطاع تكنولوجيات الإعلام والاتصال الحديثة، و تجسير الفجوة الرقمية، من أهم معالم التنمية الاقتصادية البارزة ،خاصة وأن الجزائر تنفتح على اقتصاد السوق والاقتصاد العصري،[4] وتمتلك موارد هامة تشجع على تطوير هذه التكنولوجيات في السوق الجزائرية، [5]حيث تبرز المجهودات التي تبذلها الدولة في مشاريع

---

[1] –لقد أقر الاتحاد الأوروبي وكذلك البرلمان الأوروبي، مبدأ الحفاظ على المعلومات الشخصية، من خلال التوجيه الصادر في24 اكتوبر 1995 والمتعلق بكيفية معالجة هذه المعلومات، وقد أوصى الدول الأعضاء الأخذ بهذا التوجيه وإدماجها في تشريعاتها الداخلية في تاريخ أقصاه 24 أكتوبر، 1998 ، وطبقًا للمادة الثانية من هذا التوجيه فإن المعلومات ذات الطابع الشخصي تعرف بأنها "كل معلومة تتصل بشخص محدد الهوية أو قابل للتحديد"، سعيد السيد قنديل، التوقيع الالكتروني، ماهيته وصوره وحجيته في الإثبات"، دار الجامعة الجديدة للنشر، الإسكندرية،2004 ، ص 77.

[2] –إن إبرام الصفقات بالوسائل الالكترونية، تحتاج إلى إدخال معلومات رقمية مع مراعاة الضوابط والاحتياطات الفنية اللازمة ،والتي ترتب آثارًا قانونية وفنية بالنسبة لهذا النوع من الصفقات، وفي هذا المجال نجد التوجيهات الأوروبية قد تركت لمقدمي خدمات التصديق، حرية وضع اسم للموقع سواء كان إسمه الحقيقي أو إسمه المستعار،

ما دام أي منها يمكن أن يؤدي إلى التحقق من هوية هذا الموقع، وكل ذلك مع عدم الإخلال بإمكانية الدخول لمعرفة شخصية الموقع الحقيقية، ولذلك يفضل أن يحتفظ مقدم الخدمة ببعض المعلومات التي تمكنه من معرفة شخصية الموقع، سعيد السيد قنديل، مرجع سابق، ص80.

[3] -Jan Kosko, Computer Security: Protection Is The Name of The Game, NIST Research Report, June 1989, pp. 5-8.

[4] – الجزائر و فرنسا وقعتا في 19 ديسمبر 2012 وثيقة إطار للتعاون تم بموجبها تحديد العديد من الأعمال خاصة تبادل المعلومات و التجارب و إنشاء مؤسسات و تطويرها في مجال تكنولوجيات الإعلام و الإتصال و تسيير الأقطاب التكنولوجية بين البلدين.

[5] – سعت الجزائر إلى الاستفادة من خدمات شبكة الإنترنت والتقنيات المرتبطة بها ، من خلال ارتباطها بشبكة الإنترنت في شهر مارس من عام 1994، عن طريق مركز البحث والإعلام العلمي والتقني (CERIST) ،الذي أنشأ في شهر مارس سنة 1986 من قبل وزارة التعليم العالي والبحث العلمي، لمزيد من التفاصيل أنظر محمود ابقران، الانترنيت ، دراسة اتصالية ومصطلحية، مجلة المعلومات العلمية والتقنية ،العدد 01، ج9 ،الج ا زئر ، 1999، ص 21

وتنظيمات، تهدف من خلالها إلى تضيق الفجوة بينها و بين الدول المتقدمة و كذا الدول المجاورة لها[1] ،من أبرز هذه المشاريع:

الفرع الأول: مشروع الحكومة الالكترونية:

يعتبر مشروع – الجزائر الإلكترونية– [2] من المشاريع الكبرى ،التي أعدتها وزارة البريد وتكنولوجيات الإعلام والاتصال ،بداية من العام 2009 في إطار تشاورات شملت مؤسسات وإدارات عمومية إضافة إلى متعاملين اقتصاديين عموميين وخواص، كما شملت الجامعات ومراكز البحث والجمعيات المهنية، التي تنشط في مجال علوم وتكنولوجيات الإعلام والاتصال، يهدف المشروع أساسا إلى عصرنة الإدارة العمومية وتقريبها من المواطن، والعمل على إدخال التكنولوجيات الحديثة في كل مؤسسات الدولة.

تتركز إستراتيجية الحكومة الالكترونية في الجزائر، على ضمان الفعالية في تقديم الخدمات الحكومية للمواطنين، و أن تكون متاحة للجميع، و من هذا المنطلق أخذت وزارة الداخلية و الجماعات المحلية، على عاتقها عملية تقنين الخدمات الإلكترونية بإطلاق ورشة كبرى لعصرنة الإدارة المركزية و الجماعات المحلية ،و ذلك بالوضع التدريجي لنظام وطني للتعريف المؤمن.

الفرع الثاني : التعليم الالكتروني.

شهدت الجزائر عملية تغير المناهج الدراسية و شملت عملية إدخال استعمال الحاسوب في مختلف المراحل، ولكن استخدام تكنولوجيا المعلومات و الاتصال لم يكن واضح المسار، فعملية الإصلاح ركزت على تدريب المعلمين باعتباره أمرا لازما لتحقيق الغرض من الإصلاح، وبعد إصلاحات أوت 2000 التي قامت بها الحكومة لقطاع الاتصالات لم تعرف الساحة الجزائرية، أي مبادرة للتعليم في ميدان تكنولوجيا المعلومات و الاتصال إلا مع نهاية عام

[1] - Nesrin saadoun. The Conference of Digital Information Technology .Modren Trends in The Information Technology . Amman - Jordan 9 - 11 October 2012 .

[2]– الجمهورية الجزائرية الديمقراطية الشعبية، اللجنة الإلكتروني، الجزائر الإلكترونية، ديسمبر 2008، ص 23 .

2005أين أطلق مشروع كمبيوتر لكل أسرة *OUSRATIC* مع إمكانية الربط بشبكة الانترنت، و الذي تهدف من خلاله الحكومة إلى تعميم استخدام التكنولوجيا الحديثة،

و التحضير لدخول مجتمع المعلومات بالإضافة إلى المبادرة التي أطلقتها وزارة التكوين المهني و التمهين ،بالاشتراك مع أحد موزعي خدمة الانترنت في الجزائر *EEPAD* في مارس 2006التي تهدف للتكوين في التعليم عن بعد باستخدام شبكة الانترنت، و كذا المبادرة التي أطلقتها وزارة الإعلام و تكنولوجيا الاتصالات من خلال خدمة التعليم عبر شبكة الانترنت المسبقة الدفع .

1. مشروع" تربيتك: "

قام مجمع" إيباد " الرائد في مجال الانترنت في الجزائر، بإطلاق مشروع مجاني خاص بالتعليم عن بعد عبر الانترنيت، أو بما يعرف ب"تربيتك "عرف مشاركة 02 ألف تلميذ شهادة بكالوريا و 19 آلاف تلميذ السنة الربعة متوسط، كما قامت هذه المؤسسة بتوزيع 20 حاسوب في إطار مشروع حاسوب لكل تلميذ، الذي أطلقته برعاية وزارة التربية.

- هذه الشبكة موجهة للمقدمين والمترشحين لشهادة البكالوريا والتعليم المتوسط (*BEM*)هذه الخدمة مجانية لمدة شهرين من أجل التحضير الجيد لهؤلاء المترشحين.

2. مشروع أسرتك: *Ousratic*

هو مشروع أطلق منذ سنة 2005 في الجزائر، وهو مشروع الرئيس عبد العزيز بوتفليقة الذي أعلن عنه رسميا في قمة تونس لمجتمع المعلوماتي، يقوم على توفير حاسوب لكل عائلة ،و الهدف هو تعميم أجهزة الحواسيب المصغرة و خدمة الانترنت في المنازل الجزائرية[1].

- في مجال البحث العلمي سعت الجزائر، إلى ربط الجامعات و مراكز البحث بالأنترنت منذ 1993 و كذا تسطير مجموعة من المشاريع ،عبر مراحل لفائدة هذا القطاع الذي يعد من أهم الميادين التي تساعد على تجسير الفجوة الرقمية، من المشاريع المتعلقة بالتكنولوجيات الحديثة للإعلام و الاتصال في التعليم العالي و البحث العلمي نذكر:

أ –المشاريع المتعلّقة بالهياكل الأساسيّة للاتّصال:

1- مشروع : *ARN* هو أكبر مشاريع قطاع التعليم العالي و البحث العلمي، فيما يخص الاتصال، الهدف منه توفير الهياكل القاعدية والأدوات التكنولوجية، اللازمة لكل العناصر الفاعلة في هذا القطاع (مسؤولين، أساتذة، باحثين، طلبة)قصد التكفل باحتياجاتهم، بالنسبة للإعلام و الاتصال و المعلومات العلمية والتقنية) .

2- مشروع التعليم عن بعد: *Télé- Enseignement* يتمثل في تزويد كل المؤسسات الجامعية بهياكل التعليم العالي مثل: توجيهات المحاضرة عن بعد.

3- مشروع المكتبة الافتراضية :الهدف منه هو إنشاء سياسة وطنية، لنشر المعلومات العلمية و التقنية في ميدان العلوم الاجتماعية و الإنسانية ،مهمتها اكتساب المعلومات و الوثائق العلمية، يدخل هذا المشروع الذي انطلق في أكتوبر 2002في إطار سياسة تدعيم برنامج تطوير البحث العلمي في العلوم الاجتماعية و الإنسانية، الذي أشرفت عليه وزارة

[1]- باشيوة سالم، الرقمنة في المكتبات الجامعية الجزائرية، دراسة حالة المكتبة الجامعية المركزية، بن يوسف بن خدة، مجلة Cybrarian Journalالالكترونية ، ع21، ديسمبر 2009، متاح على الموقع التالي :
http://www.journal.cybrarians.info ،

التعليم العالي والبحث العلمي، و جعل من المكتبة الجامعية المركزية كعينة نموذجية، لكن بدون الخوض في التفاصيل فقد توقف المشروع بمجرّد حدوث تغيرات على مستوى الإدارة.

4- مشروع" الفهرست "المكتبة الرقمية :جاء هذا المشروع في إطار التعاون الأورو متوسطي للتعليم العالي، ومن أجل تثمين مبادرات برنامج *Tempus IV* الذي يعمل على تدعيم التعليم والبحث العلمي في الجزائر، حيث أن هذا المشروع ضمّ جامعتين أجنبيتين *Université Libre de Bruxelles, Aix Marseille* وسبعة جامعات وطنية، والهدف منه هو العمل على إنشاء شبكة جهوية لهذه المكتبات، تعمل على توفير محتوياتها وإتاحتها للاستغلال الأمثل والمشترك، وبدأت هذه المكتبات كخطوة أولى بتأليف الفهارس وتنقيتها أو إعدادها بحسب المعايير الدولية والموحدة، حتى يتم التعامل مع التسجيلات البيبليويوغرافية بكل مرونة وسهولة .نفس المصير لقاه هذا المشروع حيث لم يعمر طويلاً لمعطيات سياسية .[1]

5- الجامعة الإفتراضية الأورومتوسّطية " ابن سينا: " هي مشروع أورومتوسّطي لمنظّمة اليونسكو بالتّعاون مع الاتّحاد الأوربيّ، يرمي إلى تطوير و توسيع التّعليم عن باعد في الحوض المتوسّطيّ، باستخدام شبكة الإنترنت و قد انضمّت إليه الجزائر ممثّلة في جامعة التّكوين المتواصل .[2]

ب –المشاريع المتعلقة بالهياكل القاعدية لتنظيم التسيير و الحصول على المعلومات:

1- الحصول على المعلومات العلمية:أكثر من 30 مركزا لمعطيات مرجعية و نصية متوفرة في مركز البحث العلمي و التقني" *CERIST* " تسمح بشكل يومي لهذا المركز الاستجابة للطلبات و احتياجات تخص البحوث البيبليويوغرافيا.

[1]– آمنة عبد ربه، الجزائر في مجتمع المعلومات، واقع و آفاق ،رسالة ماجستير في علوم الإعلام و الاتصال ،جامعة الجزائر ، 2006/2005 ،ص106 . .

[2]– عاقلي فضيلة، الإطار القانوني للتجارة الالكترونية وواقع استخدامها في الدول العربية، حالة الجزائر، ورقة عمل الملتقى العلمي الدولي الرابع حول:عصرنة نظام الدفع في البنوك الجزائرية و إشكالية اعتماد التجارة الالكترونية في الجزائر - عرض تجارب دولية – يومي28-29 أفريل 2011- .

2- أرشيف الوثائق الوطني:أدت جهود *CERIST* إلى هيكلة المعلومات المتخصصة في التعليم العالي و البحث العلمي، فتم تجميعها و دخلت في التراث الوطني المعلوماتي، و الذي يساهم ارث المخزون العالمي للأنترنت.

الفرع الثالث : التجارة الالكترونية:

سمحت التجارة الالكترونية للمؤسسات أن تمارس أعمالها بطريقة لم تكن متاحة من قبل، فقد بدأت شركات كبرى و صغرى في جميع أنحاء العالم، التأسيس لتجارة الأعمال الافتراضية، والتي تسمح بتطوير أسواق جديدة و خلق فرص إضافية في الأسواق الحالية .- و المؤسسات الجزائرية كغيرها من مؤسسات هذا العالم لم تستطع أن تتجاهل هذه المعطيات، المتولدة عن تطور تكنولوجيا المعلومات، و على رأسها شبكة الانترنت و كذا ما تفرضه ظاهرة العولمة، من انفتاح المؤسسات على العالم، فسعت منذ أن فتح لها المجال في 1995 بالاشتراك في شبكة الانترنت ،إلى استغلال إمكانيات الدعاية و الاتصال التي تمنحها شبكة الانترنت.

بالنسبة للجزائر بدأت تظهر ملامح التجارة الإلكترونية، رغم أنه لحد الآن لم تتبلور قواعد تشريعية و قانونية حول التجارة الالكترونية، أول ظهور للتجارة الالكترونية بمفهومها الحديث، مرتبط بشكل أساسي بالأنترنت كوسيلة اتصال و هذا بظهور شركات تزويد الانترنت سنة 1997 ،حيث كانت شركة" جيكوس "أول شركة جزائرية، تتعامل بالتجارة الالكترونية لأنها كانت تقوم بربط المؤسسات و الأفراد بالأنترنت، يكون الدفع نقدا أو بالحوالة..

إضافة إلى ذلك و في المجال التشريعي، هناك عدة قوانين صودق عليها متعلقة بجانب من جوانب التجارة الالكترونية، كحماية الملكية الصناعية و الفكرية و قسم خاص من قانون العقوبات يتعلق بجرائم الانترنت، كما اعترف المشرع الجزائري في القانون المدني بكتابة العقد

الالكتروني، ضف إلى ذلك قانون خاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها .[1]

لقد ضبطت الجزائر إستراتيجية شاملة للنهوض بالتجارة الالكترونية، مرتكزة على عوامل كثيرة من بينها: بنية تحتية متطورة يمكنها استيعاب كل المعاملات الالكترونية على غرار السحب بالبطاقات و الدفع الإلكتروني، وضرورة تعميم الثقافة الرقمية حتى ينخرط كل المتداخلون في المعاملات التجارية في هذه المنظومة الجديدة.

لكن المعطيات المتوفرة تؤكد أن الجزائر لازالت في طور التجربة والدراسة في هذا المجال، فبالرغم من وجود بعض المؤسسات التي تتعامل بالتجارة الالكترونية إلا انها تهدف في الغالب إلى الدعاية و الإعلان عن البضائع، بالإضافة إلى أن النظام المصرفي الجزائري لا يتلاءم مع المعطيات الجديدة .[2]

بشكل عام رغم أن مجمل المؤسسات التجارية الجزائرية، تملك وسائل إتصال حديثة بريد إلكتروني ،فاكس ...)و كذا حظيرة معلوماتية معتبرة، إلا أن استغلالها من طرف المؤسسة يبقى محدود كالبريد الالكتروني، كما أن توفر جل المؤسسات على شبكة الانترنت، و امتلاك صفحات دعاية على شبكة الانترنت، لا يكفي لتحقيق استغلال أمثل للفرص التي تمنحها التجارة الالكترونية على شبكة الانترنت، بل يجب توفر إستراتيجية حقيقة، و أهداف مسطرة و دراسات جدوى ... و كذا تكوين و توظيف العنصر البشري المؤهل÷، للاستغلال تكنولوجيا الانترنت لصالح المؤسسة و توظيفها في تحسين و زيادة قدرتها التنافسية ،و اقتحام أسواق عالمية و كذا استغلال وفرة المعلومات و تنوعها عن أسعار و سلع و خدمات وطلبات السوق ،و التعرف على ما يقدمه المنافسون مما يكسبها ميزة تنافسية في حالة استعمالها لهذه المعلومات في تطوير أدائها .

---

[1]– زيد مراد ،عصرنة نظام الدفع في البنوك و إشكالية اعتماد التجارة الالكترونية في الجزائر، الملتقى العلمي الدولي الرابع حول، عصرنة نظام الدفع في البنوك الجزائرية و إشكالية اعتماد التجارة الالكترونية في الجزائر - عرض تجارب دولية – يومي28-29 أفريل -2011 .

[2]– جمال مزغيش، التجارة الالكترونية على شبكة الانترنت، حالة توجه المؤسسات الجزائرية نحو التجارة الالكترونية، رسالة ماجستير ،جامعة الجزائر ،جوان 2001 ،ص 186 .

الفرع الرابع : الصحة الالكترونية [1].

تعتبر الجزائر من أكبر الدول اعتمادا على الأدوية المستوردة في العالم، ومع ذلك تعيش البلاد تأخرا رهيبا، في مجال رقمنة القطاع وهي العملية التي تسمح ليس فقط بضمان الشفافية في القطاع ومحاربة التبذير والفساد، بل تمكن من معرفة حجم الاحتياجات الحقيقية للبلاد وتوجيه الاستثمار الحقيقي والمنتج للقاء على الاختلالات الحقيقية الموجودة.

ردم الهوة الرقمية، تتطلب أيضا تشجيع وترقية التشريعات ووضع القوانين، التي تسمح بوثبة رقمية في القطاع كما أن تشجيع الاستثمار الرقمي في القطاع الصحي، يمر حتما عبر إلزام جميع المتعاملين ببذل جهد في الاتجاه سواء من أطباء ممارسين أو مصحات أو شبكة المستشفيات الوطنية، وإلزام الجميع بالرقمنة والارتباط بالشبكة الوطنية، وجعل ذلك ملزما حتى قبل فتح أي عيادة طبية جديدة، ونجد أحد تطبيقات الصحة الالكترونية .

1. مشروع البطاقة الالكترونية للضمان الاجتماعي" الشفاء[2]:"

يعد هذا المشروع الحلقة الأهم في برنامج عصرنة المنظومة الوطنية للضمان الإجتماعي، إذ تمنح بطاقة الشفاء التي تعتبر بطاقة الكترونية للمؤمن اجتماعيا:

أ. تشخيصه و تحديد هوية ذوي الحقوق.

ب.الحصول على حقوقه ضمن الخدمات التي يقدمها الضمان الاجتماعي.

ج. الحصول بسرعة على تعويضات عن تلك الخدمات ، بدون أن يكون مضطرا لتقديم طلب مكتوب أو ملئ استمارة و تقديم ورقة العلاج.

د. الاستمرار في الاستفادة من نظام الدفع دون الحاجة إلى تقديم دفتره .[3]

---

[1]- دليلة العوفي، مجتمع المعلومات في الجزائر واقع الفجوة الرقمية، مذكرة ماجستير في علوم الإعلام و الاتصال ،جامعة الجزائر،الجزائر، 2007/2006،ص 146 .

[2]- مرسوم تنفيذي رقم 10- 116مؤرخ في 3 جمادى الأولى عام 1431 الموافق ل 18 أبريل سنة 2010، يحدد مضمون البطاقة الالكترونية للمؤمن له اجتماعيا و المفاتيح الالكترونية لهياكل العلاج و لمهني الصحة و شروط تسليمها و استعمالها و تجديدها .

[3]- بطاقة الشفاء، متوفر على موقع بوابة المواطن http://www.elmouwatin.dz :،اطلع عليه يوم2015/02/01

الفرع الخامس : البطاقة التعريف الوطنية الإلكترونية و جواز السفر البيومتري

في إطار الإصلاحات الهيكلية الكبرى، التي تمس هياكل و مهام الدولة واقتصاد البلد و التي أطلقها رئيس الجمهورية السيد عبد العزيز بوتفليقة، قامت وزارة الداخلية و الجماعات المحلية بإطلاق ورشة كبرى لعصرنة الإدارة المركزية و الجماعات المحلية، و ذلك بالوضع التدريجي لنظام وطني للتعريف المؤمن.[1]

- هذا النظام الذي شكل العمود الفقري لمسار عصرنة مجتمعنا ارتكز على محورين أساسيين و هما:

1. إطلاق بطاقة التعريف الوطنية البيومترية و الإلكترونية.
2. إطلاق جواز السفر الإلكتروني و البيومتري.

إن هذه الاختيارات الأساسية المتخذة من طرف السلطات العمومية، لها غايات رئيسية تتمثل من جهة، في تحسين فعالية تدخل الدولة سواء فيما يتعلق بالتكفل بانشغالات المواطنين، أو وضع قيد العمل السياسة الوطنية للتنمية الاجتماعية و الاقتصادية أو أخيرا، من أجل مواجهة وضعيات أزمات.

ومن جهة أخرى، هدفت هذه العملية الخاصة بعصرنة وثائق الهوية و السفر، إلى تنمية و بصفة متواصلة لسياسات تبسيط و تخفيف الإجراءات الإدارية و كذا مكافحة البيروقراطية التي تشكل كبحا لتنمية البلاد.

كما هدفت هذه الاختيارات ثالثا، إلى تحسين نوعية الخدمات المقدمة للمواطنين في مختلف مجالات حياة مجتمعنا و المساهمة كذلك في تجسيد، على أرض الواقع، لمبادئ العدالة الاجتماعية و المساواة و كذا تحقيق السياسة الوطنية الجوارية عن طريق تقريب الإدارة من المواطن.

1- قانون رقم 03 - 14 مؤرخ في 24 ربيع الثاني عام 1435 الموافق لـــ 24 فبراير سنة 2014، يتعلق بسندات ووثائق السفر الذي الغى الأمر رقم77-1 المؤرخ في 3 صفر عام 1397 الموافق 23 يناير سنة 1977 والمتعلق بوثائق سفر المواطنين الجزائريين www.premier-ministre.gov.dz.

أخيرا، و لمواجهة تحديات العولمة المتسارعة، حددت وزارة الداخلية و الجماعات المحلية، كذلك كهدف من خلال هذه العملية، حماية مجتمعنا و بلادنا ضد آفة الجريمة المنظمة، و بالأخص الجريمة المنظمة العابرة للحدود، و كذا ظاهرة الإرهاب و التي تستعمل غالبا تزوير و تقليد وثائق الهوية و السفر كوسيلة لانتشارها[1].

[1] - http://www.interieur.gov.dz

المبحث الثاني : خريطة تأمين المعلومات في المجتمع الرقمي النامي و المتقدم.

أدت الثورة المعلوماتية إلى فتح الباب لحدوث تغييرات اكبر للحضارة الإنسانية، حيث امتدت هذه التغيرات لتشمل جميع جوانب الحياة الاقتصادية و الاجتماعيـــة و السياسية والثقافية[1].

كما أن تمييع الحدود المكانية و سيادة الفضاء المفتوح، مع غيال المركزية، و عدم وجود مركزية تمسك بزمام أركان السلطة داخل كيان الفضاء المعلوماتي، جعل المجتمع أكثر عرضة للتهديدات الرقمية التي قد تعصف بمركزاته الحيوية.

يضاف الى ذلك وجود ثغرات أمن معلوماتي نتيجة لتنامي الخبرات لدى المستخدمين وتقادم التكنولوجيا الرقمية، بسرعة كبيرة تساهم بتعميق المخاطر المحتملة للتهديدات، أو الهجمات المعلوماتية.

لذا أضحت عملية الدخول الى المنظمات الرقمية[2]، أو مجاميع العمل بحاجة الى تحويل رقمي، وإستخدام كلمات عبور، و انشاء جدران نارية محكمة للحفاظ على مقومات أمن سليم[3].

المطلب الأول: حماية البيانات المتداولة عبر الشبكات

تحاول كل من المؤسسات الحكومية و الشركات و المؤسسات الخاصة، قدر الإمكان عمل شيئا ما، يحد أو يقلل إلى حد بعيد من اختراق مواقعها و الشبكات المرتبطة بالأنترنت عن طريق كمبيوتراتها .[4]

---

[1] – محمد أديب رياض الغنيمي، شبكات المعلومات، الحاضر و المستقل، المكتبة الأكاديمية، القاهرة، 1999 ، ص 12.

[2]– مجتمع المعلومات أو المجتمع الرقمي: هو ذلك المجتمع الذي يتعامل أفراده و مؤسساته مع المعلومات بشكل عام، و التكنولوجيا الرقمية و تكنولوجيا الاتصال بشكل خاص، في تسيير أمور حياتهم في مختلف قطاعاتها الاقتصادية، الاجتماعية، الثقافية، التربوية ، السياسية، الصحية، وذلك من اجل التنمية المستدامة للمجتمع، حسن مظفر الرزو، الفضاء المعلوماتي، مركز دراسات الوحدة العربية،لبنان،2007،ص 245. كذلك:

Isabelle Mouton , La Société numérique en question(S),Sciences Humaines, Seuil, Éditions, 2011, P7.

[3]– حسن مظفر الرزو، المرجع السابق، ص 250.

[4] - Forouzan, Behrouz,Introduction to cryptography and network security,2008, p 3.

و تأتي تلك المحاولة من باب تامين الشبكات العائدة لتلك المؤسسات، بمثابة وسيلة تحد- ان لم تمنع مطلقا- من عملية الاختراق لهذه الشبكات -

تنامي دور تكنولوجيا المعلومات والاتصالات، ودخولها كعنصر فاعل ورئيسي في كافة مناحي الحياة الشخصية والمؤسسية في المجالات المختلفة بصورة غير مسبوقة، وما ترتب عليه من تراكم معرفي إلكتروني يعرف بالمحتوى المعلوماتي الرقمي.

فنجد هذا المحتوى يشمل العديد من المجالات والأفرع الرئيسية في المجالات الاقتصادية والتجارية والبنكية، وخدمات الحكومة الالكترونية، وأيضا خدمات نشر وإتاحة المعلومات والبيانات والأخبار مثل بوابات المعلومات، وقواعد البيانات المرتبطة بها، والمواقع، والخدمات الإخبارية من وكالات الأنباء والصحف والمجلات والدوريات العلمية والثقافية، وأيضا خدمات الاتصال بين الجهات الخدمية الحكومية والخاصة، والتي تعتمد اعتمادا كبيرا على شبكات المعلومات للربط فيما بينها، للتسهيل والإسراع في الإجراءات من أجل تقديم المزيد من الخدمات الدقيقة والمميزة للمستفيدين والمرتبطين بهذه الجهات من أفراد ومؤسسات وجهات أخرى محلية وإقليمية ودولية[1].

وفيما يلي محاولة لتقسيم هذا المحتوى طبقا لطبيعته ونوع استخدامه:

الفرع الأول : المحتويات الأساسية محل الحماية و التأمين [2]

عندما نتحدث عن المحتوى، فإننا نُشير إلى محتوى المعلومات، وسواء كانت المعلومات على شكل وثائق ورقية مثل الملفات والتقارير أو ملفات إلكترونية، أو قواعد بيانات في الخوادم وأجهزة الحاسوب أو الأشرطة أو الأقراص الإلكترونية، فإن جميع هذه الأشكال سوف تندرج تحت تعريف المحتوى، وسيكون نطاق المحتوى هو الجانب الآخر له. فالمعلومات المكتوبة في ملفات وملفات نصيَّة، مُخزَّنة في أجهزة الحاسوب والمواقع الإلكترونية، وجداول البيانات التي تحتوي

[1]- ماجد عثمان، رئيس مركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء ،ورقة بحثية عن حماية البيانات المتداولة عبر الشبكات، للمؤتمر الدولي الأول حول حماية أمن المعلومات في قانون الإنترنت،جوان، 2008.

[2] -John Wiley, Handbook of information security,volume.2, 2006,p60.

على بيانات رقمية، وملفات الصوت والصورة متعدِّدة الوسائط والصور الفوتوغرافية وما إلى ذلك، فإن جميع هذه الأشكال من البيانات، بالمعنى الدقيق للكلمة، تدخل في تعريف المحتوى.

البند الأول : المحتوى الاقتصادي والمالي[1]:

في عصر ثورة المعلومات، يعتمد الاقتصاد الرقمي أساساً، على إنتاج التكنولوجيا الحديثة وتوزيعها واستخدامها، في مجال المعلومات والاتصالات، ويركز في الاستغلال الأمثل لموارد المجتمع المحدودة، في جميع مراحل الإنتاج والتوزيع؛ مع الاعتماد شبه الكلي على المكون التكنولوجي في الإنتاج، مقابل الوفير الشديد في عناصر الإنتاج الأخرى، من مواد خام، وعمل، ورأسمال؛ وكذلك الاستثمار المتزايد في هذا المكون، خاصة في البحوث والتطوير، وفي تنمية القدرات والمهارات البشرية؛ بهدف توسيع دائرة الاستغلال الأمثل لها في القطاعات كافة. ومن المعروف أن معظم مكونات ثورة الاتصالات، والاقتصاد الرقمي، تُنتج في دول آسيا، حالياً، مثل: الهند، والصين، وإندونيسيا، وماليزيا؛ بل إن معظم برامج الحاسب، تُعَدّ، حالياً، في العديد من دول العالم النامي.

وفي مجال المال والبنوك، تحسنت الخدمة وضبطت القوائم المالية بصورة دقيقة. وقد ربطت ثورة الاتصالات العالم، من خلال شبكات عملاقة، تسمح لرؤوس الأموال، أن تنتقل بيسر عبر الحدود الدولية، في عملية ضخمة لنقل الثروات.

وأهم تأثيرات ثورة الاتصالات، في المجال الاقتصادي، كانت في قطاع النقل والمواصلات؛ فلا يستطيع أحد أن ينكر الدور الرئيسي للاتصالات الرقمية في إشارات المرور وحركتها، وخدمة مراكز الاتصال والمقاسم الهاتفية، وأسلوب الحجز في السكك الحديدية والطائرات والسفن[2].

و المحتوى الاقتصادي والمالي : يضم كافة المعلومات والبيانات الخاصة باقتصاديات المؤسسات والدول، ويتضمن المعلومات المتعلقة بالقطاعات الاقتصادية والمعاملات المالية الخاصة بالخدمات البنكية مثل خدمات الإيداع والسحب والاستعلام[3].

---

[1] - Henri Kloetzer, Introduction à l'économie numérique, Lavoisier, management et information, collection dirigée par nicolas manson, 2012 ,p127.

[2] -http://www.qalqilia.edu.ps/itec.htm.

[3] -http://www.banquemisr.com.eg.

البند الثاني : المحتوى العسكري

الخطط والتدابير العسكرية و أسرار الدولة الحربية و المشروعات النووية و صناعة الأسلحة، كل هذه المعلومات التي تتعلق بالجانب الأمني و الاستراتيجي للبلاد، التي تعتبر أكثر المعلومات حساسية و سرية في أي دولة التي كانت توضع سابقا في عشرات المجلدات، يمكن في الوقت الحاضر في ضل الثورة المعلوماتية تخزينها في ذاكرة الحاسوب، و معالجتها آليا أو وضعها على قرص مغناطيسي، سهل الحمل او تحميلها على مواقع خاصة على شبكة الانترنت.[1]

ويمكن في ظل هذا الوضع للمخترقين، أن يقوموا باستخدام الوسائل التقنية خلال فترة زمنية قصيرة، من اي مكان في العالم بالوصول إلى هذه المعلومات، بل قد يصل الأمر إلى حد تدمير هذه المعلومات العسكرية و محوها، الأمر الذي يشكل خطرا على الأمن القومي لأي دولة[2].

وتبدو خطورة و حساسية المعلومات العسكرية و الأمنية للدولة، إذا علمنا أن البنتاغون يقوم بتغيير أنظمة الترميز السرية لبياناته و لمعلوماته الحسابية يوميا، كما انه ينفق على احد برامجه (200) مليون دولار كل سنة، و يقوم هذا البرنامج بإلغاء و كتم الإشارات الصادرة من الآلات المستخدمة بواسطة العسكريين ووكالات الأمن و متعهدي الدفاع [3].

البند الثالث: المحتوى الاجتماعي:

يتم جمع البيانات المتعلقة بالإحصاءات السكانية، و كذلك المعلومات المتعلقة بالوضع الاجتماعي للسكان، من حيث ديانتهم و أصولهم و مستوى المعيشة الخاص بهم، و كذلك نسبة الذكور إلى الإناث في الدولة، و التوزيع الجغرافي للسكان، و غير ذلك من المعلومات، و التي تبنى عليها الدولة خططها التنموية و الاقتصادية .

---

[1]- نهلا عبد القادر المومني ،الجرائم المعلوماتية ،دار الثقافة للنشر و التوزيع ، ط1 ، 2008 ،ص 211 .

[2]- و كان كتاب قد صدر في باريس تحت عنوان (عين واشنطن) كشف عن قيام جهازي المخابرات الأمريكية، و الإسرائيلية باختراق جميع أجهزة الحاسوب في العالم، بهدف الحصول على جميع المعلومات المتعلقة بالدول الأخرى في المجالات كلها ،و أشار الكتاب إلى أن الولايات المتحدة الأمريكية، تقوم بعمل كمائن للنظم المعلوماتية لدى أعدائها و حلفائها على حد سواء ، بحيث تصبح لديها جميع المعلومات في مختلف المجالات . و قد أكد الكتاب كذلك وجود ما يسمى بمركز المعلومات الكوني الذي تودع فيه المعلومات التي يتم تجميعها عبر نظم معلوماتية خاصة تم ترويجها و بيعها في العالم و في النهاية هي تعمل في خدمة وكالة المخابرات الأمريكية (CIA) و الموساد الإسرائيلي.

[3]- نهلا عبد القادر المومني، نفس المرجع ،ص 212 .

وبعد انتهاء عملية جمع هذه المعلومات، يتم عادة في معظم الدول تخزينها في ذاكرة الحاسوب على مواقع خاصة تابعة للدولة التي تتعلق هذه البيانات بسكانها، و من ثم تتم معالجة هذه المعلومات أليا بغية الاستفادة منها في تحقيق الأهداف المنشودة في الدولة.

إلا أن هذه البيانات و المعلومات قد يتم إساءة استعمالها، و التجسس عليها من قبل جهات قد تكون داخلية [1]، أي من داخل الدولة و لأغراض خاصة أو من قبل جهات خارجية، أي من قبل دولة معادية تهدف لمعرفة الجوانب المختلفة لدولة ما، لتحقيق أهداف خاصة بها، ومن الأمثلة على التجسس على هذا النوع من البيانات [2].

قيام موظفين من العاملين بمركز حاسوب في السويد بنسخ برامج مسجل عليها إحصاءات و بيانات سكانية، حيث قاما ببيعهما بعد ذلك إلى احد لمكاتب الخاصة بالإحصاءات و البيانات لأغراض استهلاكية مقابل ثمن رخيص[3].

الفرع الثاني : الأساليب التقنية لحماية المعطيات والمواقع الإلكترونية

في إطار تنمية تكنولوجيا المعلومات والاتصالات، ومواكبة التطور الهائل في استخدامها في كافة المجالات والأنشطة، تم التفكير في تطبيق التوقيع الإلكتروني، والذي تكمن أهميته في زيادة مستوى الأمن والخصوصية في التعاملات، نظرا لقدرة هذه التقنية على حفظ سرية المعلومات والرسائل المرسلة وعدم قدرة أي شخص أخر على الإطلاع أو تعديل أو تحريف الرسالة، كما يمكنها أن تحدد شخصية وهوية المرسل والمستقبل إلكترونيا للتأكد من مصداقية الشخصية، مما يسمح بكشف التحايل أو التلاعب[4].

---

[1] -Dominique W,Internet et après ?une théorie critique des nouveaux medias, France : Flammarion, 1999, p.108.

[2]- نهلا عبد القادر المومني، نفس المرجع ، ص 215

[3]- نفس المرجع ، ص216

[4]- مصطفى محمد، أساليب إجرامية بالتقنية الرقمية ، ماهيتها و مكافحتها، دار الكتب القانونية،المحلة الكبرى ، 2005، ص 26 و ما بعدها _ www.arab bank. Com

البند الأول : التوقيع الالكتروني و الاعتراف القانوني

تباينت التعريفات التي أعطيت للتوقيع الإلكتروني [1] ، و ذلك بحسب الزاوية التي ينظر منها إلى هذا التعريف، فهناك من عرفه، بناء على الوسيلة التي يتم بها إجراء التوقيع الالكتروني، في حين عرفه آخر، بحسب ما يقوم به من وظائف، فتنوعت تعريفات التوقيع الالكتروني, سواء من منظور الاتفاقيات الدولية، أو التشريعات الخاصة بالتوقيع الالكتروني، فنجد :

1. القانون النموذجي حول التجارة الالكترونية، الصادر عن لجنة القانون التجاري الدولي لدى الأمم المتحدة بموجب القرار رقم 162/51 تاريخ 16/1/1996، الذي أقرَّ بالقوة الثبوتية للسند والتوقيع الالكترونيين.

2. التوجيه الصادر عن البرلمان الأوروبي، بتاريخ 1999/12/13 حول التوقيع الالكتروني وتسهيل استعماله من أجل حسن سير العمل في السوق الداخلي الأوروبي، كما أقرَّ البرلمان الأوروبي توجيهاً آخر بتاريخ 2000/6/8 حول التجارة الالكترونية والتأكيد على الاهتمام بتوقيع العقود بالطرق الالكترونية.

3. قانون الأونيسترال النموذجي بشأن التوقيعات الالكترونية[2]، الذي اعتمدته لجنة القانون التجاري الدولي لدى الأمم المتحدة في دورتها ال34 بتاريخ 5/7/2001، لتنظيم التوقيع

---

[1]- أول اعتراف بالتوقيع الإلكتروني كان عام 1989 في مجال البطاقات الائتمانية، حيث أقرت محكمة النقض الفرنسية صحة التوقيع الإلكتروني واعتبرت أنه يتألف من عنصرين :هما إبراز البطاقة الائتمانية وإدخال رقم حامل البطاقة السري، وأكدت هذه المحكمة كذلك أن هذه الوسيلة توفر الضمانات الموجودة في التوقيع اليدوي، بل تفوقها. وصدر في 13 كانون أول 1999م إرشاد عن الاتحاد الأوروبي، حول التوقيع الإلكتروني ، وورد في المادة الثانية منه أن التوقيع الإلكتروني يجب أن يستوفى الشروط التالية :

- أن يكون التوقيع مرتبطاً بشخص الموقع وحده.
- أن يسمح بتعريف هوية الموقع.
- أن يكون قد وجد بوسائل تمكن الموقع من إبقائها تحت رقابته الحصرية.
- أن يكون التوقيع مرتبطاً بالبينات التي يحال اليها بشكل يسمح بكشف كل تعديل لاحق عليها.

[2]- عرفت المادة (2/أ) من قانون الإنسترال النموذجي بشأن التوقعات الإلكترونية لسنة 2001م ،التوقيع الإلكتروني: بأنه " بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها، أو مرتبطة بها منطقياً ،ويجوز أن تستخدم لتعيين هوية الموقع، بالنسبة إلى رسالة البيانات وبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات".

الالكتروني في سياق العلاقات ذات الطابع التجاري، ويعتبر هذا القانون قانوناً إسترشادياً في مجاله، لكنه لا يتضمن كل التفاصيل المتعلقة بالتوقيع الالكتروني، بل يفسح المجال لإصدار قوانين خاصة به

4. اقرار عدة دول قوانين خاصة بتنظيم التجارة الالكترونية والسندات والتواقيع الالكترونية، أهمها بريطانيا عام 1995، وألمانيا وايطاليا عام 1997[1]، والولايات المتحدة الأمريكية وفرنسا عام 2000، وتونس عام 2000[2]، ومصر عام 2004[3].

5. فقد أصدر المشرع الفرنسي قانونا هاما برقم 230 لسنة 2000 في شأن المبادلات والتجارة الإلكترونية وقد ورد ضمن أحكام هذا القانون أن التوقيع الإلكتروني يدل على شخصية الموقع، ويضمن علاقته بالواقعة المنسوبة إليه، كما يؤكد شخصيته، وكذلك صحة الواقعة المنسوبة إليه وذلك إلى أن يثبت العكس، ويترتب على ذلك أن أي تزوير يتعرض له التوقيع يكون بمثابة تزوير تنطبق عليه نصوص القانون الجنائي.

---

[1] -Depuis 1997, le régime juridique de la signature électronique est déterminé par une loi en Allemagne et par un décret en Italie.

En effet, l'Allemagne a adopté en juin 1997 la loi sur la signature " digitale ", qui constitue en fait la troisième partie d'une loi générale sur la société de l'information et qui a été complétée par une ordonnance entrée en vigueur le 1er novembre 1997.
En Italie, un décret du Président de la République, pris en 1997 en application de la loi Bassanini sur la réforme de l'administration publique, définit le régime juridique des documents informatiques, parmi lesquels la signature électronique. Les dispositions de ce décret qui concernent cette dernière ont été précisées au début de l'année 1999 par un décret du Président du conseil.

[2]- القانون التونسي الخاص بالمبادلات و التجارية الإلكترونية، عدد 83 لسنة 2000 مؤرخ في 9 اوت 2000 يتعلق بالمبادلات والتجارة الالكترونية.

[3]- عرَّف المشرع المصري التوقيع الالكتروني بموجب القانون رقم 2004/15 بأنه "ما يوضع على محرر الكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقع ويميّزه عن غيره"، كما صدر القرار رقم 109 لسنة 2005 بإصدار اللائحة التنفيذية الخاصة بالقانون رقم 15 لسنة 2004 ، وتتكون اللائحة من 24 مادة بالإضافة الى ملحق فنى وتقني ، وتوضح اللائحة الضوابط الفنية والتقنية لمنظومة تكوين بيانات إنشاء التوقيع الإلكتروني، والتى يمكن تعديلها أو تبديلها بقرار وزارى.

سيما وأن المادة 1316 في فقرتها الأولى نصت على أن" الكتابة الإلكترونية مقبولة في الإثبات كدليل كتابي على الورق، شرط أن تكون منسوبة إلى صاحبها، ودالة على شخصيته.[1]

6. في التشريع المغربي رقم 53/05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، والذي أضاف الفصل3 ـــ 417 إلى قواعد الإثبات بالكتابة في ظهير الالتزامات والعقود، حيث أصبحت " تتمتع كل وثيقة مذيلة بتوقيع إلكتروني مؤمن والمختومة زمنيا بنفس قوة الإثبات التي تتمتع بها الوثيقة المصادق على صحة توقيعها والمذيلة بتاريخ ثابت[2].

---

[1] -La France a opéré la transposition de la directive en adoptant le 13 mars 2000 la loi numéro 2000-230 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique. La modification principale apportée par cette loi est l'insertion de l'article 1316-4 dans le Code civil. Cet article définit la signature et pose l'équivalence entre la signature électronique et la signature manuscrite sou certaines conditions. Le décret numéro 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 et relatif a la signature électronique, modifié par le décret numéro 2002-535 du 18 avril 2002, fixe et organise les moyens techniques permettant de répondre aux objectifs juridiques de l'article 1316-4 du Code civil. Tandis que l'alinéa 2 de l'article 1316-4 du Code civil définit matériellement le concept de signature électronique, l'article 1.2) du décret n° 2001-272 introduit une signature électronique particulière

Le procédé de signature électronique est présumé fiable au sens du décret si :

- La signature électronique est sécurisée
- Elle est créée par un dispositif sécurisé de création de signature
- Et si la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié http://www.legifrance.gouv.fr/

[2]– المادة 3/417: " يفترض الوثوق في الوسيلة المستعملة في التوقيع الإلكتروني، عندما يتيح استخدام توقيع إلكتروني مؤمن إلى آن يثبت ما يخالف ذلك .

– يعتبر التوقيع الإلكتروني مؤمنا إذا تم إنشاؤه وكانت هوية الموقع مؤكدة وتمامية الوثيقة القانونية مضمونة وفق النصوص التشريعية والتنظيمية المعمول بها في هذا المجال .

– تتمتع كل وثيقة مذيلة بتوقيع إلكتروني مؤمن والمختومة زمنيا بنفس قوة الإثبات التي تتمتع بها الوثيقة المصادق على صحة توقيعها والمذيلة بتاريخ ثابت "

7. و من التشريعات العربية نجد المادة 14 من قانون إمارة دبي في شأن المعاملات والتجارة الالكترونية رقم 2 لسنة 2002 تجيز التعاقد بوسائط الكترونية، حيث نصت فقرتها الأولى على أنه : " يجوز أن يتم التعاقد بين وسائط الكترونية مؤتمتة، متضمنة نظامي معلومات الكترونية أو أكثر تكون معدة ومبرمجة مسبقا للقيام بمثل هذه المهمات، ويتم التعاقد صحيحا ونافذا ومنتجا آثاره القانونية على الرغم من عدم التدخل الشخصي أو المباشر لأي شخص طبيعي في عملية إبرام العقد في هذه الأنظمة."

8. أما في الجزائر فقد أدرج التوقيع الالكتروني للمرة الأولى من قبل المشرع سنة 2005 (القانون 05-10 المؤرخ في 20 جوان 2005 المعدل والمتمم للقانون المدني) الذي تم من خلاله الاعتراف بالكتابة الالكترونية كوسيلة اثبات وذلك بإضافة المادتين 323مكرر و232مكرر1 .

9. كما قننت الجزائر التوقيع الالكتروني بالمرسوم التنفيذي 07-162 المؤرخ في 30ماي 2007 الصادر في الجريدة الرسمية عدد 37لسنة2007

10. و أخيرا أفرج عن القانون رقم 04/15 المؤرخ في 01 فيفري 2015[1] الذي

يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، قصد التكفل بالمتطلبات القانونية والتنظيمية والتقنيات، التي ستسمح بإحداث جو من الثقة المواتية لتعميم وتطوير المبادلات الإلكترونية، وترسيخ المبادئ العامة المتعلقة بنشاطي التوقيع والتصديق الإلكترونيين في الجزائر. يسمح بتعميم وتطوير التبادلات الإلكترونية بين المستعملين في مجالات القطاع العام و الخاص.

فقد عرف التوقيع الالكتروني في المادة 2 بأنه : بيانات في شكل الكتروني، مرفقة أو مرتبطة منطقيا ببيانات الكترونية أخرى ، تستعمل كوسيلة توثيق.

[1]- القانون 15-04 المؤرخ في 111 ربيع 2عام 1436الموافق ل 1 فبراير 2015المحدد للقواعد العامة للتوقيع و التصديق الالكترونيين،ج.ر06.

المادة 6 "يستعمل التوقيع الإلكتروني لتوثيق هوية الموقع و إثبات قبوله مضمون الكتابة في الشكل الالكتروني "

كان الهدف من موجة التشريعات الحديثة، هو تسهيل استعمال الوسائل الإلكتروني في المعاملات التجارية، فان أبرز صور هذا المد التشريعي جاءت بالأساس لتحيين أنظمة الإثبات في القوانين المدنية المعاصرة، كما أن أسمى أهداف مواءمة أنظمة الإثبات مع متطلبات التجارة الإلكترونية، هو الاعتراف القانوني بالوثيقة الإلكترونية وإعطاءها نفس الحجية القانونية التي تتمع بها الوثيقة الكتابية العادية.

و فيما يلي التقنية الثانية لحماية البيانات و المعطيات فيما يندرج تحت مسمى الأمن الرقمي أو المعلوماتي .

البند الثاني : التشفير الإلكتروني

تحظى تقنيات و سياسات التشفير[1] في الوقت الحاضر باهتمام استثنائي في ميدان امن المعلومات، و مرد ذلك إن حماية التشفير يمثل الوسيلة الأكثر أهمية لتحقيق وظائف الأمن الثلاثة، السرية و التكاملية و توفير المعلومات، فالتشفير تقنيات تدخل في مختلف وسائل التقنية المنصبة على تحقيق حماية هذه العناصر، فضمان سرية المعلومات أصبح يعتمد على تشفير و ترميز الملفات و المعطيات، بل تشفير وسائل التثبت و كلمات السر، كما أن وسيلة حماية سلامة المحتوى، تقوم على تشفير البيانات المتبادلة و التثبيت لدى فك التشفير،و أن الرسالة الالكترونية لم تتعرض لأي نوع من التعديل أو التغيير.[2]

[1]- تشفير البيانات: هي عملية ترميز البيانات قبل تحويلها أو إرسالها واستخدامها في إجراءات التبادل، ومن ثم فك الترميز بعد الإرسال واهم ما في التشفير: هي مفاتيح الرموز والأشخاص المخولين بمعرفتها، ولها طريقتين أساسيتين تعرف بـــ (DES) Data Encryption Standardو . (PKE) Public Key Encryption-

www.crybtographie.com

[2] -Le décryptement est l'action consistant à retrouver le texte en clair sans connaître la clef de déchiffrement .

و يعد التشفير بوجه عام و تطبيقاته العديدة و في مقدمتها التواقيع الالكترونية ،الوسيلة الوحيدة تقريبا لضمان عدم إنكار التصرفات عبر الشبكات الالكترونية، و بذلك فان التشفير يمثل الإستراتيجية الشمولية لتحقيق الأهداف الأمن من جهة، و هو مكون رئيس لتقنيات و وسائل الأمن الأخرى، خاصة في بيئة الأعمال الالكترونية و التجارة الإلكترونية و الرسائل الالكترونية و عموما البيانات المتبادلة بالوسائط الالكترونية .

و من حيث مفهومه، فان التشفير يمر بمرحلتين رئيسيتين، الأولى تشفير النص على نحو يحوله إلى رموز غير مفهومة أو مقروءة بلغة مفهومة، و الثانية، فك الترميز بإعادة النص المشفر إلى وضعه السابق كنص مفهوم و مقروء، و هذه المسالة تقوم بها برمجيات التشفير التي تختلف أنواعها و وظائفها.

أما من حيث طرق التشفير، فثمة التشفير الترميزي، و التشفير المعتمد على مفاتيح التشفير، التي قد تكون مفاتيح عامة أو خاصة او مزيجا منها .

هناك عدة جوانب في الحديث عن التشفير الأول تقني أو فني والآخر قانوني، لذلك سنفصل الكلام فيهما تباعا وكما يلي :

أولا: الجانب الفني للتشفير.

ان الطريقة الشائعة للتشفير تتمثل بوجود مفتاحان [1]، المفتاح العام ***public-key*** وهو معروف للكافة.

Confidentialité : est historiquement le premier problème posé à la cryptographie. Il se résout par la notion de chiffrement, mentionnée plus haut. Il existe deux grandes familles d'algorithmes cryptographiques à base de clefs : les algorithmes à clef .secrète ou algorithmes symétriques , et les algorithmes à clef publique ou algorithmes asymétriques. Ghislaine. Labouret . Introduction à la cryptographie. P 11.Hervé Schauer Consultants (HSC) . 1999-2001 Hervé Schauer Consultants www.hsc.fr. Voir aussi Emmanuel. Bresson .CRYPTOGRAPHIE. Laboratoire de cryptographie - SGDN/DCSSI- Emmanuel.Bresson@sgdn.gouv.fr. Renaud Dumont. Cryptographie et Sécurité informatique .Université de Liège. Faculté des Sciences Appliquées.. 2010.p91.

[1]– المادة 2 الفقرتين 8 – مفتاح التشفير الخاص : هو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقّع فقط ،وتستخدم لإنشاء التوّقيع الإلكتروني ويرتبط هذا المفتاح بمفتاح تشفير عمومي.

9 - مفتاح التشفير العمومي: هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور، بهدف تمكينهم من التحقق من الإمضاء الإلكتروني، وتدرج في شهادة التصديق الإلكتروني قانون رقم 15 - 04 مؤرخ أوّل فبراير سنة 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

ومفتاح خاص *private-key*[1] يتوفر فقط لدى الشخص الذي أنشأه، ويمكن بهذه الطريقة لاي شخص يملك المفتاح العام، ان يرسل الرسائل المشفرة، ولكن لا يستطيع ان يفك شيفرة الرسالة، الا الشخص الذي لديه المفتاح الخاص [2] .

ثانيا- الجانب القانوني للتشفير

إن كلمة تشفير يونانية الأصل، وتعني باللغة الانكليزية (متخفي أو سري)[3] ويعرف التشفير اصطلاحا بأنه عملية تمويه الرسائل أو المعلومات أو البيانات بشكل لا تقرا من احد سوى من الموجهة إليه، وعرفه محمد حسين منصور بأنه (استبدال شكل البيانات من خلال تحويلها إلى رموز أو إشارات، لمنع الغير من معرفتها أو تعديلها أو تغييرها ،فالتشفير وسيلة فنية لحماية البيانات من الآخرين [4] ،أو هو (عملية الحفاظ على سرية المعلومات الثابت منها والمتحرك، باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات، إلى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير لهم بذلك لا يستطيعون فهم أي شيء، لان ما يظهر لهم هو خليط من الرموز والأرقام والحروف غير المفهومة)[5].

وقد تطرقت القوانين العربية[6] المنظمة للتوقيع الالكتروني إلى تعريف التشفير وتبيان مدلوله، فالقانون التونسي مثلا، عرفه في الفصل الأول بالاتي (التشفير : إما استعمال رموز أو إشارات

---

[1] – لمزيد من التفصيل راجع بحث للأستاذ عبد المجيد ميلاد، تشفير البيانات والتوقيع الالكتروني على الموقع الاتي:
http://www.arabcin.net/modules.php?name=News&file=article&sid=948

[2] – بيل جيتس، المعلوماتية بعد الانترنت، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون و الآداب، الكويت، 1998 ص 47 .

[3] – باسل يوسف، الاعتراف القانوني بالسندات والتواقيع الالكترونية في التشريعات المقارنة، مجلة دراسات قانونية صادرة عن بيت الحكمة، العدد الثاني، بغداد، 2001 ص 23 .

[4] – محمد حسين منصور، المسؤولية الالكترونية، دار الجامعة للنشر والتوزيع ،مصر، ص 180 .

[5] – هدى قشقوش، الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية، القاهرة، ص 60 .

[6] – عرفه المشرع المغربي في القانون رقم05 /53 من القانون المتعلق بالتبادل الإلكتروني للمعطيات القانونية ،في نص الفقرة الثانية من المادة 12 "بأنه كل عتاد أو برمجة، أو هما معا ينشأ أو يعدل من أجل تحويل معطيات سواء كانت عبارة عن معلومات أو شعارات أو رموز، استنادا إلى اتفاقيات سرية أو من أجل إنجاز عملية عكسية، لذلك بموجب اتفاقية سرية أو بدونها."الفصل 2 من القانون التونسي الخاص بالمبادلات و التجارية الإلكترونية ، عدد 83 لسنة 2000 مؤرخ في 9 اوت 2000 يتعلق بالمبادلات والتجارة الالكترونية ،التشفير :اما استعمال رموز او اشارات غير متداولة تصبح بمقتضاها المعلومات ،المرغوب تمريرها او ارسالها غير قابلة للفهم من قبل الغير او استعمال رموز او اشارات لا يمكن الوصول الى المعلومة بدونها .

غير متداولة، تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير، أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها)[1] .

كما انه قد استحدثت برامج تشفير متقدمة لحماية البيانات المخزنة على شبكات الحاسب الآلي[2].

البند الثالث : الشهادات الرقمية.

الشهادة الرقمية[3] هي بطاقة هوية رقمية لكيان (شخص اعتباري أو طبيعي)، أو مورد معلوماتي يكون هو موضوع الشهادة، وهي تشمل إلى جانب أشياء أخرى، هوية صاحب الشأن (حامل الشهادة)، والمفتاح العمومي المخصص لصاحب الشأن وهوية الجهة المُصدِرَة[4].

فالشهادات الرقمية هي ملفات تستخدم لأغراض الأمن الالكتروني، تتضمن أسم وعنوان صاحب الشهادة وتاريخ التصريح ومفتاح التشفير المستخدم في الوثيقة، والذي من خلاله يتم التعرف على التوقيع الالكتروني [5]والتأكد من صلاحيته، بالإضافة إلى اسم الشركة التجارية، ويستخدم في العادة في نظام [6](*SSL*)

---

[1]- إسماعيل عبد النبي شاهين، امن المعلومات في الانترنت بين الشريعة و القانون، مؤتمر القانون و الكمبيوتر و الإنترنت، المجلد الثالث، ص 976.و انظر كذلك ، وليد العاكوم ، مفهوم ظاهرة الإجرام المعلوماتي ، مؤتمر القانون و الكمبيوتر والإنترنت، المجلد الأول ، ص 968.

[2]- لمنع و مكافحة الجريمة ،قامت إحدى الشركات المعلوماتية بتصميم برامج هدفه الحيلولة دون الدخول الأطفال إلى المواقع غير المناسبة لهم ،لاسيما و أن الجناة يقابلون الأطفال من خلال غرف الدردشة، و يوجد كذلك في أسواق الكمبيوتر، في الوقت الحال برامج تمكن الآباء من التحكم في استخدام أطفالهم للأنترنت. انظر ، عبد الفتاح بيومي مجازي، الأحداث و الإنترنت، دار الفكر الجامعي ،الإسكندرية ، 2002،ص 295و ما بعدها.

[3]- المادة 2/3-6-7 من القانون التونسي المتعلق بالمبادلات والتجارة الالكترونية لسنة 2000 شهادة المصادقة الإلكترونية باعتبارها " الوثيقة الإلكترونية المؤمنة بواسطة الإمضاء الإلكتروني للشخص الذي أصدرها، والذي يشهد من خلالها إثر المعاينة، على صحة البيانات التي تتضمنها ".

L'article 2 de la loi *allemande* 1er novembre 1997, définit le titulaire du certificat comme une personne physique. Il prévoit, outre le certificat de clé, le certificat d'attribution, qui est " un certificat électronique séparé contenant de plus amples informations et qui fait expressément référence à un certificat de clé spécifique ".

L'article 7 de la loi, qui indique les informations que doit contenir le certificat de clé, ne correspond pas totalement aux exigences concernant les certificats " qualifiés " et figurant à l'annexe I de la directive. La durée de validité des certificats ne peut excéder cinq ans.

[4]- حمدون إ. توريه، سامي البشير المرشد، دليل الأمن السيبراني للبلدان النامية، الاتحاد الدولي للاتصالات، ط 2007، ص 63.

[5] -Fritze Grupe – Stephen G. Kerr – William Kuechler and Nilesh Patel, Understanding Digital Signatures, The CPA Journal, June 2003.

[6]- SSL (Secure Sockets Layer).

ومن ثم يقوم المتصفح بالتحقق من هذه الشهادة من خلال ثلاثة ركائز أساسية:

1. أن تكون الشهادة آتية من طرف موثوق به .

2. التحقق من سريان مفعولها في الوقت الحالي، وذلك من خلال إلقاء نظرة على تاريخ إصدار الشهادة وتاريخ انتهائها .

3. المقارنة بين اسم الموقع في الشهادة واسم الموقع في الخادم للتأكد من أن الشهادة مرتبطة بالموقع وقادمة منه .

وبعد التحقق من الشهادة يعمل على إنشاء مفتاح عشوائي للتشفير (*Symmetric Key Encryption*) يقوم بدوره على تشفير البيانات التي تنتقل من المتصفح إلى جهاز الخادم، باستخدام بروتوكول التحكم بالإرسال، وبروتوكول الإنترنت (*TCP/IP*) مما يضمن عدم التعرّض لهذه البيانات من قبل أي جهة أخرى، فلا يمكن لأحد قراءتها سوى المرسل والمستقبل، وفي نهاية المطاف يقوم الموقع بفك شيفرة الرسالة الواردة إليه من المتصفح وذلك باستخدام مفتاح خاص بالموقع ذاته (*Private Key*) ، ثم يستخدم المفتاح العشوائي لبقية الاتصال.

الجدير بالذكر أن استخدام هذه التقنية يعمل على إحداث تغيير طفيف في عنوان الموقع الإلكتروني، كالبنك مثلاً وهذه دلالة واضحة على وجود أمن معلوماتي في الشركة أو الإدارة.[1]

وعند التطرق إلى مثال البنك فإننا نلحظ عند الدخول إلى موقع البنك بأن عنوانه يبدأ بـــ "*http*" ولكن بمجرد الضغط على صفحة تسجيل الدخول إلى الحساب، فإن العنوان يتغير من "*http*" إلى "*https*"، بالإضافة إلى أيقونة الأمان والتي تظهر في أسفل صفحة الموقع.

SSL est un protocole de sécurité permettant l'encryptage de messages, l'authentification d'un serveur, le maintient de l'intégrité d'un message, et optionnellement, l'authentification d'un client dans une connexion tcp/ip.
TLS (Transport Layer Security) est le successeur de SSL basé sur ce dernier.

- http://www.webopedia.com
- http://www.marche-public.fr
- http://www.linguee.fr

[1] ضياء علي أحمد نعمان، الغش المعلوماتي، الظاهرة والتطبيقات، مطبعة ووراقة الوطنية، بمراكش، ط1 2001.ص33 و كذلك مهران زهير المصري، السياسات الأمنية للمواقع الإلكترونية، مجلة الباحثون ،العدد 40 ، 2010، متوفر على الموقع التالي: http://kenanaonline.com/users/ahmedkordy/posts/330241

البند الرابع : برمجيات الجدران النارية

بشكل عام يمكن القول : إن جدران النار هي عبارة عن برامج تقوم بصد محاولات الاختراق او الهجوم الوافد من شبكة الانترنت، لتهديد الشبكة الداخلية أو النظام المعلوماتي، و تشبه برامج جدران النار حرس الحدود على الساحل، حيث تزود الشبكات بحماية جيدة عن طريق التأكد من شرعية كل شخص يود زيارة الشبكة المحمية، دخولا أو خروجا دون أن يكون مصرحا له بذلك[1] .

1. **أما برمجيات الجدران النارية الحديثة**، و رغم أنها لا تزال تقوم باستخدام اسلوب فلترة وتصفية البيانات الواردة، فإنها تقوم بعمل ما هو أكثر بكثير من إنشاء الشبكات الافتراضية الخاصة، رقابة محتوى البيانات الوقاية من الفيروسات، و حتى إدارة نوعية الخدمة، و هذه الخدمات جميعها تعتمد على ميزة أساسية و هي أن الجدران النارية تقع على طرف الشبكة، و من خلال العقد الماضي، كانت الجدران النارية ببساطة، مجرد أدوات بسيطة تعمل كمنفذ للأنترنت – أو بكلمات أخرى كحراس على طرف الشبكة – تقوم بتنظيم حركة البيانات و حفاظ على امن الشبكة [2]

و قد ظهرت أول الجدران النارية للشبكات في عام 1980 و كانت عبارة عن موجهات تستخدم في تقسيم هذه الشبكات إلى شبكات محلية LAN صغيرة .

و كانت مثل هذه الجدران النارية توضع في مواقعها هذه للحد من انتشار المشاكل التي يواجهها جزء من الشبكة إلى الأجزاء الأخرى .

و قد تم استخدام أول جدران ناري لتحقيق الأمن، في أوائل التسعينات و كانت عبارة عن موجهات لبروتوكول IP مع قوانين فلترة كانت تبدوا كالتالي :

اسمح لفلان بالدخول و النفاذ إلى الملف التالي .أو امنع فلان أو برنامج ... من الدخول نمن المنطقة التالية .

[1]– جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات ، رؤية جديدة للجريمة الحديثة، دار البداية،ط1، 2010 ، ص 246.

[2]– عبد الفتاح مراد، المرجع السابق ، ص 420 .

- اهم قدرات الجدران النارية :

التحقق من هوية المستخدمين : ذلك أول ما أضافه المطورون إلى الجدران النارية الأولى، كانت القدرات القوية للتحقق من الهوية، و اذا كانت السياسات الأمنية التي تتبعها المؤسسة تسمح بالنفاذ إلى الشبكة إلى شبكة خارجية، مثل الانترنت، فانه لابد من استخدام ميكانيكية ما للتحقق من هوية المستخدمين .

و التحقق من الهوية يعني ببساطة التأكد من صحة هوية المستخدم بشكل يتجاوز مجرد التحقق من اسم المستخدم و الكلمات السرية، و التي لا تعتبر بحد ذاتها وسيلة قوية للتحقق من هوية المستخدمين، ذلك انه و على صلة غير خاصة، وصلة غير مشفرة عبر الانترنت، فان أسماء المستخدمين و كلماتهم السرية يمكن نسخها و إعادة استخدامها، أما الأساليب القوية للتحقق من هوية المستخدمين فتستخدم أساليب التشفير مثل الشهادات الرقمية، أو برمجيات حساب الشفرات الرقمية الخاصة .

و بواسطة الشهادات الرقمية، يمكن تفادي هجمات إعادة الاستخدام حيث يتم نسخ اسم المستخدم و كلماته السرية، و إعادة استخدامها إلى الشبكة[1] .

2. **الشبكات الافتراضية الخاصة:** تقوم الشبكات الخاصة بنقل البيانات بسرية عن طريق توثيقها و تشفيرها، باستخدام أكواد و مفاتيح سرية تكون معلومة لدى مختلف أطراف الشبكة الخاصة، و بالتالي يصعب على اي طرف خارجي الاطلاع على محتوى تلك البيانات أو قراءتها حتى تصل ال الطرف المرغوب فيه[2].

3. أنظمة كشف التطفل (*IDS (Intrusion detection systems*)

معظم المنشآت سواء كانت صغيرة أو كبيرة، تحتاج إلى جهاز إنذار ضد السرقة للحفاظ على المعلومات القيّمة لديها، وقد ظهر نظام جديد يغني عن أجهزة الإنذار ويؤدي وظيفتها على أكمل وجه، وهو ما يعرف بنظام كشف التطفل الذي هو في جوهره نظام إنذار ضد السرقة،

[1]- عبد الفتاح مراد ،المرجع السابق ، ص 421 .

[2]- أحمد أمين أبو سعدة ،الدليل العلمي لمتطلبات تطبيق تكنولوجيا المعلومات في المكتبات، الدار المصرية اللبنانية، بدون سنة نشر ،ص 113.

يعمل على مراقبة الشبكة وإصدار إنذارات فيما إذا شك بأن الشبكة تتعرّض للهجوم في وقت ما.

- ويوجد آليتان لكشف التطفل.

1. الكشف عن الوضع الشاذ(*Anomaly detection*) هذه الطريقة مبنية على أساس مراقبة سلوك المستخدمين في النظام الاعتيادي، وتخزين السلوك في النظام، فهي تقوم على أساس مقارنة السلوكيات مع الحزم الإلكترونية لاكتشاف الانحرافات، ومن أبرز مساوئ هذه الآلية، صدور إنذارات إيجابية خاطئة (False Positive Ala*rms*) نتيجة اكتشاف هجمات غير معرّفة.

2. الكشف عن الإساءة (*Misuse detection*) تعتمد على مقارنة الصفات المتعلقة بالحزم، مع الصفات المخزنة في قاعدة البيانات، و من أبرز مساوئ هذه الآلية هو انحصارها فقط على الهجوم المعروف في قاعدة البيانات[1].

3. الطرق التأمينية :و هي عبارة عن مجموعة الحواجز و العراقيل الفنية ذات التقنية المناسبة، التي تقف عائقا دون وصول المتلصصين او المحترفين او غيرهم، توضع من قبل الشركات المنتجة للبرامج .

و من أمثلة هذه الحواجز و العراقيل وضع شفرات معينة أو كلمة سر خاصة للسماح للدخول للبرامج المعدة للاستخدام، كذلك وضع برامج كشف على أنظمة الحاسب الآلي، تتولى بدورها كشف الفيروسات و الملفات الخطيرة و تدميرها أولا بأول[2] ،كذلك وضع آلية عزل برامج المستخدم عند الدخول على شبكة الانترنت .

[1]– مهران زهير المصري، السياسات الأمنية للمواقع الإلكترونية ،مجلة الباحثون، العدد 40 ، 2010، متوفر على الرابط التالي: http://kenanaonline.com/users/ahmedkordy/posts/330241

[2]–عبد الفتاح مراد، التجارة الالكترونية ،البيع والشراء على شبكة الانترنت، البهاء للنشر الالكتروني ،مصر، ص 79 .

البند الخامس: القياسات الحيوية [1]:

هو العلم الذي يستخدم التحليل الإحصائي لصفات الإنسان الحيوية، وأهم استخداماته تكمن في مجال صناعة الكمبيوتر، التي جعلت مفهوم التحليل الإحصائي لدى معظم الناس، بأنه الطريقة المثلى لإثبات هوية الأشخاص باستخدام صفاتهم الفريدة، سبب أهميته هي حقيقة أن الصفات الفيزيائية والسلوكية للإنسان، لا يمكن نقلها للآخرين ولا يمكن للإنسان نسيانها ولا سرقتها .

يمكن تقسيم القياسات الحيوية إلى فئتين: الخصائص الجسدية(المادية/الفسيولوجية)، والخصائص السلوكية، وهي تعتمد على استخلاص البيانات من القياسات التشريحية للشخص. والفئة الثانية أقل ثباتاً من الأولى، وتتغير مع الضغط أو الضعف، كما أنها أقل أماناً. ولكنها تمتلك ميزة عن الفئة الأولى حيث من الممكن أن تكون غير واضحة للشخص، أي يمكن تحديد هويته دون أن يدري أنه خضع لهذه العمليةـــ وهي أكثر قبولاً من قبل الأشخاص لأنها أقل تطفلاً.

والأنواع التي تندرج مسمى القياسات الحيوية لأمن المعلومات ما يلي :

1. تعرف بصمات الأصابع *Fingerprint Scanning* :

بصمة الإصبع [2]هي اثر الختم بالأصبع أي الختم بطرف الأصبع، ولكل إنسان بصمة، ولا توجد بصمة شخص تتوافق مع شخص آخر، واستخدمت أوروبا بصمة الأصابع – في القرن التاسع عشر– في كشف المجرمين وإثبات هوية أصحاب السوابق من خلال دراسات وأبحاث وتجارب قام بها كبار علماء الطب والتشريح وكبار رجال الشرطة[3].

---

[1]– فايزة دسوقي أحمد، بصمة اليد والعين والقياسات الحيوية في أمن المعلومات،2010، مقال متوفر على الرابط التالي: http://www.lahaonline.com/articles/view/37151.htm و كذلك : www.mouwazaf-dz.com

[2]– عرفت الشريعة الإسلامية بصمة الأصبع منذ القدم، حيث قال المفسرون في تفسير قوله تعالى (بَلَىٰ قَادِرِينَ عَلَىٰ أَنْ نُسَوِّيَ بَنَانَهُ) آية 4 من سورة القيامة .

[3]– طارق عبد الله أبو حوه ، مشكلات الحجية القانونية لبصمة الهوية البشرية البيومترية في الاثبات المدني ،مجلة القانون والاقتصاد ،جامعة القاهرة، ص 16.

وتعتبر تقنية تعرف بصمة الأصبع الأشهر والأكثر استخداماً في أمن البيانات[1]،مقارنة بمسح شبكية العين، واستخدام نظام بصمة الإصبع نظام بسيط حيث يتم تسجيل البصمة، ثم تصنف نماذج البصمات التي تم أخذها للشخص وفقًا لليد التي تم أخذها منها والأصابع، كذلك وبعد ذلك يتم استخدام بطاقة بصمة الإصبع، لتحديد بعض النقاط الفريدة لتعرف بصمة الشخص، وتسمى هذه النقاط بعلامات بصمات الإصبع ويمكن استخدامها إذا تم استخدام نظام مضاهاة إلكتروني.

2. شبكية العين *Retina Scanning* :

تعرف الشبكية يتعلق بتسجيل وتحليل أشكال الأوردة الدموية الموجودة في العصب، الموجود في خلفية مقلة والذي يعالج الضوء الداخل من خلال إنسان العين، وطريقة عمل هذه التقنية يتلخص في إطلاق شعاع من الضوء ذو شدة منخفضة داخل مقلة العين، وتسجيل شكل الأوردة في العين، وينبغي أن يكون الشخص قريب جداً من عدسات جهاز مسح الشبكية، ويحدق مباشرة في العدسات، ويظل ساكناً أثناء مرور الضوء داخل إنسان العين، وأية حركة من الشخص قد تتطلب إعادة العملية من البداية.

- وتستخدم العديد من الدول بصمة العين في المجالات العسكرية، خاصة في امريكا وأوروبا، كما تستخدمها الامارات، ومعظم دول الخليج، في كافة منافذها الجوية والبرية والبحرية للتعرف على هوية القادمين والمغادرين .

- كما تستخدم بصمة العين في مجال تأمين خزائن البنوك حيث يضع عميل البنك عينه في جهاز متصل بكمبيوتر، فإذا تطابقتا مع البصمة المحفوظة بالجهاز فتحت الخزينة المطلوبة على الفور، ويمكن كذلك استخدام بصمة العين كدليل إثبات في بعض الجرائم [2].

---

[1]- اخترعت إحدى الشركات اليابانية جهازا لمضاهاة البصمات، و هو الأصغر و الأسرع في العالم لتحقيق الشخصية من خلال بصمات الأصابع ، فالبصمة التي يتم البحث عن صاحبها، توضع الكترونيا على شاشة صغيرة، و يضع المتهم أصبعه على جهاز ماسح ، فتظهر بصمته إلى جوارها، لتجري المطابقة بين البصمتين في نصف ثانية ، بدرجة دقة تصل على (بالمئة 99)،شريف درويش اللبان، تكنولوجيا الاتصال، المخاطر و التحديات و التأثيرات الاجتماعية ، الدار المصرية اللبنانية، مصر، 2000،ص 148.

[2]- علاء بن محمد صالح الهمص ،وسائل التعرف على الجاني، مكتبة القانون والاقتصاد، الرياض،2012، ص113.

3. القزحية *Iris Scanning* :

القزحية (المنطقة الملونة في العين) :و هي العضو الداخلي المحمي من العين، تقع خلف القرنية وأمام العدسات، وتتمثل طريقة عمل نظم تعرف القزحية في إنارة الماسح للقزحية بضوء الأشعة تحت الحمراء غير المرئية، مما يبين تفاصيل أكثر تكون غير مرئية للعين، والتقاط صورة أبيض وأسود ذات درجة وضوح عالية للقزحية، باستخدام كاميرا صغيرة ذات جودة عالية، ثم يحدد النظام حدود القزحية، وينشئ نظام إحداثيات ويحدد مناطق التحليل في هذا النظام.

4. الوجه ***Facial Scanning*** :يعتبر الوجه من السمات الشائعة الاستخدام، لإثبات هوية الأشخاص في حياتنا اليومية، حيث عادة ما نتعرف على هوية الشخص من خلال وجهه، إذا كان معروفاً لدينا مسبقاً، كذلك فإن الوجه هو السمة الحيوية المستخدمة عادة في إثبات الهوية في إجراءات السفر، من خلال صورة الشخص الرقمية أو الفوتوغرافية الموجودة في جواز السفر.

- يتم إثبات هوية الشخص إلكترونياً من ملامح وجهه، وذلك من خلال كاميرا فيديو رقمية تقوم بعمل مسح لصورة الوجه وتخزين أبعاد الوجه المختلفة، مثل البعد بين العينين والأنف والفم وحواف الفك، في قاعدة بيانات والتي عليها يتم المقارنة بعد ذلك وإثبات الهوية على أساسها .

- تحلل تكنولوجيا التعرف على الوجه سمات وجه الشخص باستخدام كاميرا فيديو رقمية، يتم الاحتفاظ بمقاسات كمال بينة الوجه بما في ذلك البعد بين العيون و الأنف و الفم وحواف الفك وذلك في قاعدة بيانات، وتستخدم تلك المعلومات للمقارنة.

- ويوفر التعرف على الوجه عدة ميزات، يلتقط النظام صور وجوه الأشخاص في مناطق عامة، مما يقلل من المشاكل القانونية وحيث أن التقاط الصورة يحدث من مسافة فإن التعرف على الوجه يمكن أن يتم دون أي ملامسة جسدية.

- كما تمنح هذه السمة تقنية التعرف على الوجه إمكانية السرية والتخفي والتي تكون مفيدة في مهمات الملاحقة، وعلى سبيل المثال، يمكن أن تكون السلطات الأمنية العامة بحاجة إلى تحديد موقع أشخاص معينين مثل المجرمين المطلوبين، و إرهابيين مشتبه بهم و الأطفال المفقودين.[1]

5. هندسة اليد *Hand Geometry*

يُستخدم هذا النظام منذ سنوات عديدة، وبشكل خاص في أنظمة متابعة الحضور والانصراف وتسجيل الوقت، يعطي هذا النظام توازنًا جيدًا بين الأداء والدقة وسهولة الاستخدام، ومن السهولة دمجه في أنظمة أخرى، توضع اليد على الجهاز الماسح في المكان المخصص لها، ويقوم النظام بفحص تسعين صفة من بينها شكل اليد ثلاثي الأبعاد 3D، طول وعرض الأصابع، وكذلك شكل مفاصل الأصابع.

6. ضربات لوحة المفاتيح *keystroke Dynamics*:

هذا النظام يقوم تسجيل ضربات الشخص على لوحة المفاتيح، ومن خلال هذه العملية يقوم بمراقبة الوقت بين ضرب مفتاح والانتقال الأصابع لضرب مفتاح آخر، وكذلك يراقب الوقت الذي يأخذه المستخدم وهو ضاغط على المفتاح، وحيث أنه يجب على المستخدم أن يتذكر أسم المستخدم والرقم السري[2].

7. الصوت *Voice Verification*:

للصوت عناصر وخصائص مميزة له مثل نغمة الصوت، وإيقاعه، ونبرته وملامح أخرى تجعل تلك الخصائص محددة لشخص معين، وهذا ما تعتمد عليه نظم تعرف الصوت في التوثق من الشخص، هو مجال بحثي حديث، يحظى باهتمام عدد كبير من مهندسي الحاسب الآلي للعمل على تحسين نظم المحادثة بين الإنسان والآلة.

---

[1] - Arun Ross, Anil Jain, *HAND GEOMETRY*, available on the site http://www.cse.msu.edu/biometrics/hand_geometry.html

[2] – عبدالله بن شائع بيهان، ثقافة أمن المعلومات، كلية المعلمين، قسم الحاسب، جامعة الملك سعود، مركز التميز لأمن المعلومات ،المقال متوفر على الرابط التالي : aalbaihan@ksu.edu.sa

- ويعرف التسجيل الصوتي بصفة عامة بأنه عبارة عن عملية يتم بها ترجمة للتغيرات المؤقتة لموجات الصوت الخاصة بالكلام إلى نوع آخر من الموجات أو التغيرات الدائمة، ويتدخل لإتمام ذلك آلة تترجم موجات الصوت، إلى اهتزازات ذات طبيعة خاصة ويحفظ التسجيل على سلك بلاستيكي ممغنط لحفظ هذه التسجيلات وإعادة ترديدها [1] .

- فمن خلال جهاز*Spectograph* يتم تحليل الصوت البشرى الكترونياً، وتحويله إلى خطوط مقروءة ومن ثم مقارنته مع أصوات المشتبه بهم، وإعطاء الرأي بالمطابقة أو الاختلاف ، ذلك أن نطق الكلمات أو الجمل يختلف من شخص لآخر وان الاختلافات بين عدد من الأفراد تكون أكبر عن الاختلافات في النطق لفرد واحد، وحتى إذا حدثت محاولات تصنع أو تلاعب في الصوت (عن طريق الحديث بالهمس أو غلق الأنف عند الكلام)، فإن ذلك لا يؤثر ولا يترتب عليه أي تغيير في الملامح الأساسية لبصمة صوت الشخص .

8. الحمض النووي[2] *DNA* :

تستخدم قياسات الحمض النووي، على نطاق واسع في الحالات القضائية، وخاصة في حالات الاغتصاب والاعتداء الجنسي لتحديد مرتكبها، ويمكن استخلاص الحمض النووي من أي مصدر جسدي، مثل الشعر أو الدم أو العرق والإفرازات وأية سوائل جسدية أخرى، ولا يمكن أن تتكرر مضاهاة الحمض النووي بين الناس.

ومن الممكن استخدام الحمض النووي في تأمين شبكات المعلومات، وهو يختلف عن القياسات الحيوية الأخرى بعدة طرق:

- يتطلب تحليل الحمض النووي وجود عينة مادية مثل الشعر أو الدم.
- لا تتم المضاهاة في الحمض النووي في الوقت ذاته، وحالياً لا تتم جميع المراحل بشكل آلي.

.7

[1]- عباس العبودي، الحمية القانونية لوسائل التقدم العلمي في الاثبات المدني، الاردن ، 2002، ص 38 .

[2]- DNA هى الحروف الأولى لمصطلح Deaxy Rila Nuclic Acid أي الحامض النووي، وهو عبارة عن مركب كيمائي، معقد ذو وزن جزئي عالي لا يمكن للكائن الحى، الاستغناء عنه يعرف بالدنا، وهى اختصار لكلمة الحامض النووي الديوكسي متروع الاوكسجين. محمد احمد غانم ،الجوانب القانونية والشرعية للإثبات الجنائي بالشفرة الوراثية، دار الجامعة الجديدة،2008، ص 58 .

- مضاهاة الحمض النووي لا تستخدم القوالب أو استخلاص الملامح، ولكنها تمثل مقارنة بين عينات حقيقية[1].

إن السمات الحيوية التي يتميز بها كل إنسان عن الآخر مثل بصمة الإصبع، العين، هندسة الوجه واليد، الصوت، التوقيع وخط الكتابة إلى غير ذلك من السمات حققت إنجازاً كبيراً في الحد والتغلب على الكثير من المشاكل ونقاط الضعف، الذي واجهت الطريقة التقليدية للتحقق من هوية الشخص إلكترونياً باستخدام الكلمات السرية، و بالرغم من درجة الأمان العالية التي حققتها تقنية السمات الحيوية فإنها لا تعبر وسيلة سليمة 100% خالية من الأخطاء، وبديلاً كاملا للكمات السرية، فمن الممكن أن تقع الأجهزة المستخدمة في تقنية السمات الحيوية في الخطأ، عند تحليلها للسمات المتشابهة جداً أو أن يعتريها بعض الخلل فتعطي الضوء الأخضر للإنسان الخاطئ، أو تنفي هوية الإنسان الصحيح .

بالإضافة إلى كونها غير صالحة للاستخدام في جميع الأحوال، فالصوت مثلاُ في حالة الصحة قد يختلف عنه في حالة إصابة الشخص بنزلات البرد، وبالتالي فإنه من غير الممكن التحقق من هويته باستخدام التقنية المعتمدة على التحقق من هوية الشخص صوتياً.

ولذلك فإنه من الممكن استخدام تقنية السمات الحيوية جنباً إلى جنب الكلمات السرية، لتكون مكملا كلاً منها إلى الأخرى للتغلب على العيوب، التي تعتري كلاً منهما في التحقق من هوية الشخص.

الفرع الثالث : الإجراءات الفنية لوقاية المعطيات من الانتهاكات الالكترونية. [2]

تتعدد وسائل الأمن التقنية المتعين استخدامها في بيئة الكمبيوتر و الانترنت، كما تعدد أغراضها و نطاقات الاستخدام، و سنتعرض في هذا الفرع الثالث لتلك الوسائل و الطرق المكافحة التقنية لجرائم الكمبيوتر و الانترنت، ويمكن تقليل فرصة الإصابة بعدوى الكمبيوتر إلى حدها الأدنى إذا اتبعت الإرشادات التالية :

[1] – فايزة دسوقي أحمد ،القياسات الحيوية وأمن المعلومات Information Security – Biometrics ، 2010 ،متوفر على الموقع الإلكتروني http://www.alriyadh.com/2010/04/29/article520979.html

[2] – Lyn Robinson, Installing a Local Area Network , London ,Aslib , 1995, p36.

البند الأول: عدم استخدام البرامج المسروقة :

أهم نصيحة لتقليل الاحتمالات العدوى بالفيروس الكمبيوتر إلى اقل حد ممكن، هي ضرورة تجنب البرامج المسروقة، و التي لوحظ مؤخرا انتشار استخدامها في الجزائر من خلال التعامل مع قراصنة البرامج، الذين تخصصوا في سرقة حقوق الغير فهم درجوا على نسخ البرامج الأصلية، و إنتاجها بكميات كبيرة ثم بيعها في الأسواق المصرية بأسعار زهيدة، كل ذلك بسبب غياب تفعيل القوانين التي تحمي ملكية البرامج الأصلية، مثلما في ذلك مشكلات نسخ الكتب و الشرائط الفيديو و الكاسيت لذلك يصح باستخدام البرامج الأصلية و الابتعاد عن استخدام البرامج المنسوخة و المسروقة، و لا تسمح للغير أيضا باستخدام هذه البرامج على الحاسب الخاص بك فان البرامج الأصلية عادة ما تخلو من الفيروسات، إلا أن أصحاب البرامج يعمدون أحيانا إلى وضع فيروس في برامجهم الأصلية لينشط فقط عند وقوع عمليات نسخ غير قانونية لبرامجهم، فتسبب في مسح كل البيانات المسجلة على الأقراص الممغنطة، مرنة كانت ام صلبة[1] .

البند الثاني : طرق الوقاية من الفيروس التي تصيب الكمبيوتر .[2]

تتخلص طرق الوقاية من عدوى الفيروسات الكمبيوتر فيما يلي ، يجب إتباعها بكل حرص و الا كانت العواقب وخيمة :

---

1 – عبد الفتاح مراد ، شرح جرائم الكمبيوتر و الإنترنت، دار الكتب و الوثائق المصرية ،مصر، ص 409.

2 – LIMOUSIN Solène, Comment protéger son identité sur Internet, Publié le 28/09/2015 ,article sur:

- http://www.supinfo.com/articles/single/390-comment-proteger-son-identite-interne
- http://fr.wikihow.com/prot%C3%A9ger-son-identit%C3%A9-en-ligne
- http://www.meilleurvpn.com/
- http://www.inriality.fr/vie-citoyenne/identite/anonymat/proteger-son-identite
- http://ici.radio-canada.ca/nouvelles/societe/2013/11/07/001-conseil-fraude-protection-identite-internet-securite.shtml
- http://blog.nordnet.com/loeil-sur-le-web/focus/5-astuces-pour-proteger-son-identite-sur-internet.html

- استخدام بعض البرامج التي صممت خصيصا للكشف و الوقاية من الفيروس، مثل البرامج التالية على سبيل المثال لا الحصر *Shot vaccine*.

- امتنع تماما عن التعامل مع قراصنة البرنامج و احرص على استخدام البرامج الأصلية.

- لا تستخدم أية برامج جاهزة تحتوى على الملف المعروف باسم *command.com* فهذا الملف مستهدف لغزوات الفيروس، كما أن هذا الملف ملك الشركة ميكروسوفت المعروفة، و من ثم هي نسخ غير قانونية من الملف و لا يمكن الجزم بخلوها من عدوى الفيروس، قم بحماية وحدة الاسطوانات الصلبة لديك قبل تجربة تشغيل برنامج جديد، و من طرق الحماية المعروفة في هذا الصدد تحويل وحدة التشغيل الاسطوانات المرنة لتعمل و كأنها الاسطوانة الصلبة و ذلك باستخدام الأمر وعندما تتأكد من خلو هذا البرنامج الجديد، من عدوى الفيروسات فانه يمكنك إعادة الأمر إلى نصابها السابق.

- تعدد وسائل و طرق المكافحة التقنية لجرائم الانترنت، من حيث الطبيعة و الغرض، إلا انه يمكن تصنيف هذه الوسائل في ضوء غرض الحماية إلى الطوائف التالية :

الطائفة الأولى : مجموعة وسائل الأمن المتعلقة بالتعريف بشخص المستخدم و موثوقية الاستخدام و مشروعيته، و هي الوسائل التي تهدف إلى ضمان إستخدام النظام أو الشبكة من قبل الشخص المخول بهذا الاستخدام، و تضم هذه الطائفة كلمات السر بأنواعها.

- والبطاقات الذكية المستخدمة بالتعريف، ووسائل التعريف البيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي، ومختلف أنواع المنتجات التي تزود كلمات سر أنية أو وقتية متغيرة الكترونيا، ومفاتيح المشفرة، بل تضم هذه الطائفة ما يعرف بالأقفال الالكترونية التي تحدد مناطق النفاذ[1].

الطائفة الثانية :مجموعة الوسائل المتعلقة بالتحكم بالدخول و النفاذ إلى الشبكة، و هي التي تساعد في التأكد من أن الشبكة و مصادرها قد استخدمت بطريقة مشروعة، و تشمل الوسائل التي تعتمد على تحديد حقوق المستخدمين، أو قوائم أشخاص المستخدمين أنفسهم، أو تحديد المزايا الاستخدامية أو غير ذلك من الإجراءات و الأدوات و الوسائل، التي تتيح التحكم بمشروعية استخدام الشبكة ابتداء.

[1]–عبد الفتاح مراد، المرجع السابق ، ص 416 .

الطائفة الثالثة : مجموعة الوسائل التي تهدف إلى منع إفشاء المعلومات لغير المخولين بذلك، و تهدف الى تحقيق سرية المعلومات، و تشمل هذه الوسائل تقنيات تشفير المعطيات و الملفات، و إجراءات حماية نسخ الحفظ الاحتياطية، و الحماية المادة للأجهزة و مكونات الشبكات، و إستخدام الفلترات و الموجهات.

الطائف الرابعة : مجموعة الوسائل الهادفة لحماية التكاملية (سلامة المحتوى)، و هي الوسائل المناط بها لضمان عدم تعديل محتوى المعطيات من قبل جهة غير مخولة بذلك، و تشمل تقنيات الترميز و التواقيع الالكترونية و برمجيات تحري الفيروسات و غيرها.

الطائفة الخامسة : مجموعة الوسائل المتعلقة بمنع الإنكار (إنكار التصرفات الصادرة عن الشخص)، و تهدف هذه الوسائل إلى ضمان عدم القدرة شخص المستخدم من إنكار انه هو الذي قام بالتصرف، و هي وسائل ذات أهمية بالغة في بيئة الأعمال الالكترونية و التعاقدات على الخط، و ترتكز هذه الوسائل في الوقت الحاضر على تقنيات التوقيع الالكتروني و شهادات التوثيق الصادرة عن طرف ثالث.

الطائفة السادسة : وسائل مراقبة الاستخدام و تتبع سجلات النفاذ أو الأداء، و هي التقنيات التي تستخدم لمراقبة العاملين على النظام لتحديد الشخص الذي قام بالعمل المعين في وقت معين، و تشمل كافة أنواع البرمجيات و السجلات الإلكترونية التي تحدد الاستخدام.[1]

المطلب الثاني : الفجوة الرقمية وكيفية تأمين المعلومات في ظلها

يشكل تأمين المعلومات،ذلك الكم الهائل من المعلومات والبيانات التي تسبح بحرية في فضاء الإنترنت، اليوم تحدياً عالمياً كبيراً ليس فقط على مستوى الحكومات والشركات والمؤسسات الكبرى، وإنما على المستوى الشخصي، فالمعلومات التي يمتلكها كل شخص ما هي إلا جزء من منظومة كبيرة، هي تصب في النهاية في قواعد تلك الكيانات المعلوماتية الكبرى من حكومات و مؤسسات و شركات .

[1]- عبد الفتاح مراد، المرجع السابق ، ص 417 .

لهذا كان رفع الوعي و تعزيز الثقافة الأمنية لدى أفراد المجتمع، ضرورة لابد منها للوصول إلى درجات عالية من أمن المعلومات، و كما أشرفت التغيرات المحيطة بنا على كافة الأصعدة فإننا نعتمد اليوم آليات جديدة للتعامل مع تلك المعلومات.

ولما كانت الطبيعة البشرية هي الحلقة الأضعف في سلسلة أمن المعلومات، فإن اللصوص والمحتالون على الإنترنت، عملوا على استغلالها للوصول إلى أهدافهم عبر اختراق العقول البشرية، ودراسة الحالة النفسية والاجتماعية للمستخدم قبل أن تحوله إلى ضحية لعملية اختراق أو احتيال عبر الإنترنت فيما يعرف بالهندسة الاجتماعية.

الفرع الأول : إشكالية الفجوة الرقمية [1]

تعبر إشكالية الفجوة أو الهوة الرقمية عن الفارق في حيازة تكنولوجيا المعلومات، و الاتصالات بشكلها الحديث، و حيازة المهارات التي يتطلبها التعامل معها بين الدول المتقدمة ،المنتجة لهذه التكنولوجيات و لبرامجها و لمحتوياتها و بين الدول النامية التي لا تساهم في إنتاج هذه التكنولوجيات، وفي صياغة محتوياتها ،وهي أيضا الفارق في توزيع هذه التكنولوجيات على الأفراد بين الدول المتقدمة و الدول النامية، وكذا بمدى النفاذ إلى المعرفة من حيث توفر البنى التحتية اللازمة، للحصول على موارد المعلومات و المعرفة بالوسائل الآلية أساسا، دون إغفال الوسائل غير الآلية من خلال التواصل البشري، إن هذا التعريف يركز على الحد الفاصل بين مدى توافر الشبكات الإتصالاتية، ووسائل النفاذ إليها، وعناصر ربطها بشبكة الانترنت[2].

[1]- إن الفجوة الرقمية هي امتداد لفجوة إعلامية اتصالية بين الشمال و الجنوب و حتى بين دول الشمال نفسها، و تعود جذورها إلى سنوات السبعينات، و تمثلت في سيطرة دول قليلة و على رأسها الولايات المتحدة الأمريكية، على تدفق الأنباء و المعلومات في العالم، و كانت مطالب الدول النامية، و بالخصوص من خلال حركة عدم الانحياز، تنصب حول إقامة نظام إعلامي اتصالي عالمي جديد، يقوم على التوازن في تدفق المعلومات، و كان ذلك من خلال مؤتمرات عديدة تم عقدها منها، قمة الجزائر1973، مؤتمر ليما البيرو1975 ، مؤتمر نيودلهي 1976، مؤتمر كولومبو 1976. ومن خلال اليونسكو أيضا مؤتمر نيروبي، مؤتمر باريس.

[2]- حمزة بعلي، صالح محرز، حناشي توفيق، الفجوة الرقمية بين الدول النامية و الدول المتقدمة، مدرسة الدكتوراه ،الاقتصاد التطبيقي و تسيير المنظمات، كلية العلوم الاقتصادية و علوم التسيير، جامعة الحاج لخضر ،باتنة ،الجزائر، ص 6.

البند الأول : مفهوم الفجوة الرقميَّة *digital dévide*

وتسمى بالإنجليزية *Digital Divide* :هو مصطلح حديث ظهر في علم الحاسوب وعلوم الاجتماع في بداية الألفية الجديدة.

الفجوة الإلكترونية: هي الفجوة بين الذين بمقدورهم استخدام الإنترنت بسبب امتلاكهم المهارة اللازمة والقدرة المادية، وبين الذين لا يستطيعون استخدام الإنترنت، بعض الدراسات تنسب الفجوة الرقمية، إلى الفجوة بين مستخدمي وسائل الاتصالات الحديثة وتقنية المعلومات بشكل عام وغير المستخدمين لهم.[1]

البند الثاني : أسباب اتساع الهوة الرقمية

من الأسباب الرئيسية للفجوة الرقمية بين دول الشمال و الجنوب:

1. الجمود التنظيمي والتشريعي: لعدم توافر البيئة التمكينية التي تتيح مشاركة متوازنة لإحداث التنمية لقطاعات المجتمع الحكومي والخاص فهي غير متوائمة مع اقتصاد المعرفة .

2. سيطرة الولايات المتحدة عالميا على المحيط الجيومعلوماتي[2]:

فالولايات المتحدة هي القطب الوحيد الذي يحكم قبضته على المحيط الجيومعلوماتي، وخاصة فيما يتعلق بالأنترنت، فالولايات المتحدة تتمسك بأن تحتكر المؤسسة الأمريكية،

---

[1]- انطلقتْ في العالَم كله دعواتٌ دوليَّة للقضاء على الفجوة الرقميَّة، مِن بينها مشروع" لاب توب لكلِّ طفل one laptop per child "، والذي رعتْه كبريات الشركات المصنِّعة لأجهزة) الكومبيوتر واللاب توب (وشركات البرمجة العالمية، وهذا) اللاب توب (مخصَّص للأطفال من سن 6 – 12 سنة، صغير ، خفيف الوزن ومفاتيحه خضراء ولامِعة، مقاوم للماء وضد الكسْر، ويعمل بالطاقة الشمسيَّة ليتحدَّى ظروفَ انقطاع الكهرباء المتواصلة في الدول الأشد فقرًا، وهو يُعلِّم الأطفال الكتابة والقراءة، ويحتوي داخلَه على ألف كتاب، وعلى مِئات الأنشطة والتدريبات المتنوِّعة، ومزوَّد بأكثر مِن لغة، كما ظهرت أيضًا في عام 2004 مبادرة 50× 15(50x15 Initiative)، التي طمحتْ في تحقيق هدف أساسي؛ وهو ضمانُ وصول الإنترنت، وتمتُّع 50 % من سكَّان العالَم بخدماته بحلول عام 2015، وقدْ هدفت المبادرة أيضًا لنشر معامل للتعلُّم، تهدف لنشْر الوعي والحلول التكنولوجية لمختلف لقضايا التي يُواجِهها العالَم .التفاصيل متوفرة على الرابط التالي : http://www.alukah.net/culture/0/62352

[2]- حمزة بعلي ، صالح محرز ، حناشي توفيق، المرجع السابق، ص 11.

مسئولية تسيير المهام الأساسية للأنترنت[1].

3. سيطرة حكومات الدول النامية على الوضع المعلوماتي محليا، فحكومات الدول النامية تسيطر على منافذ المعلومات تحت دعوى حماية الأمن القومي.

البند الثالث : آثار الفجوة الرقمية

المتأمل لواقع الثورة التكنولوجية الرقمية يجد أنها لا تزال فى بداياتها الأولى في البلدان النامية، وهو الأمر الذي أحدث ما يسمى الفجوة الرقمية بين تلك البلدان ودول العالم الأول، والفجوة الرقمية هي مصطلح يستخدم لوصف واقع نشأ جراء الثورة التكنولوجية، التى شملت كل الميادين، وتعنى الحصول غير المتساوي للتكنولوجيا في معناها العام بين الدول الغنية المتقدمة والدول النامية الفقيرة، بحيث تتحول تلك الدول الفقيرة إلى دول تابعه ومستهلكة للتكنولوجيا، التي تصنعها الدول المتقدمة، وتؤثر الفجوة الرقمية بصورة سلبية كبيرة على جميع الجوانب الاجتماعية والاقتصادية والسياسية في المجتمعات النامية ودول العالم الثالث، ويمكن إجمال أبرز آثار الفجوة الرقمية في التالي:

1. عدم إمكان تكيف الاقتصاد النامي مع الاتفاقيات الدولية.
2. انخفاض المستوى العلمي وانعزال الفكر في الدول النامية.
3. انخفاض الوعي التكنولوجي والتواصل مع العالم.
4. تزايد حدة الفقر الاقتصادي والمعلوماتي.

[1]–ومن أبرز مظاهر ذلك تشبثها بأن تحتكر مؤسسة ICANN الأمريكية مسئولية تسيير المهام الأساسية للانترنت internet governanceمما يثير القلق من أن تصبح الانترنت ضيعة أمريكية خاصة،تأسست في سنة 18 سبتمبر 1998، يقع مقرها في مارينا دل راي –كاليفورنيا ,وهي مختصة بتوزيع و إدارة عناوين الاي بي وأسماء المجال...

ICANN :The Internet Corporation for Assigned Names and Numbers.

La Société pour l'attribution des noms de domaine et des numéros sur Internet est un organisme à but non lucratif responsable de la sécurité, la stabilité et la coordination mondiale du système d'identificateurs uniques de l'Internet.

5. زيادة الفكر المتطرف من خلال عدم التفاعل مع الفكر العالمي وتوالد الأحقاد ضد الدول المتقدمة واعتبار أنها العدو الوحيد.

6. غياب القنوات العصرية لتبادل المعلومات بين صناع القرار والمواطنين في الدول النامية.

7. غياب الشفافية المعلوماتية في المجتمع، وانعدام الحق في المعرفة.[1]

البند الرابع : دور الحكومات في سد الفجوة الرقمية

يمكن للحكومات أن تساعد على سد الفجوة الرقمية بالإجراءات التالية:

1. ممارسة الإرادة السياسة لدفع مبادرات الفجوة الرقمية.

2. تعزيز تحرير قطاع الاتصالات وإتاحة المستوى الصحيح من التنظيم، لغرس الثقة وتعزيز المنافسة في تقديم الخدمات، بما يؤدي إلى زيادة الكفاءة التشغيلية وتخفيض التكلفة على المستعمل[2].

3. منح الاستقلال للهيئات التنظيمية، لكفالة حصول جميع المواطنين على فرصة الاستفادة من التكنولوجيات الرقمية الجديدة، ولكي تكون سوق الاتصالات جذابة للاستثمارات الرأسمالية.

4. إنشاء مراكز المعلومات العامة في جميع المدارس والأماكن الأخرى المفتوحة أمام الجمهور، أو في جميع الوحدات الجغرافية الإدارية غير المركزية في إطار زمني محدد.

5. إتاحة التدريب على استعمال تكنولوجيات المعلومات والاتصال والإنترنت.

---

[1]- فتحي شمس الدين، الفجوة الرقمية في دول العالم الثالث ،مجلة الأهرام للكمبيوتر و الانترنت و الاتصالات، لغة العصر، 20-2-2016، مقال منشور على الرابط التالي : http://aitmag.ahram.org.eg/News/38391.aspx

[2]- حققت غالبية الدول العربية تقدما كبيرا نحو التحول لاقتصاديات قائمة على المعرفة، من خلال إدخال تحسينات كبيرة في نشر تكنولوجيا المعلومات والاتصالات، منذ منتصف التسعينيات ،كما نما قطاع الهاتف النقال من لا شيء تقريبا في عام 2000- إلى 87 اشتراكا لكل 100 نسمة في عام 2010؛ خلال نفس الفترة، زاد عدد مستخدمي الإنترنت في منطقة الشرق الأوسط إلى عشرة أضعاف، ووصل إلى أكثر من 100 مليون مستخدم، مع تباين واسع بين الدول، بدءا من 12 مستخدم لكل 100 شخص في الجزائر وصولاً إلى 81 مستخدم لكل 100 شخص في قطر. ووفقا لتقرير صادر عن مدار للأبحاث والتنمية وأورينت بلانيت، من المتوقع أن يرتفع الرقم إلى ما يقرب من 197 مليون مستخدم بحلول عام 2017، مع قفز معدل انتشار الإنترنت من حوالي 32٪ في عام 2012 إلى أكثر من 51٪ في عام 2017 – أي أن عدد مستخدمي الإنترنت العرب سيحقق ما يقرب من 3٪ فوق المتوسط العالمي في ذلك الوقت، الفجوة الرقمية العربية والمسيرة نحو اقتصاد المعرفة العربي الحقيقي ، متوفر على الموقع التالي : **http://www.arabbusinessreview.com**

6. التماس حلول تحقق فعالية التكاليف، بقدر أكبر في معدات المستعمل النهائي مثل أجهزة الحاسوب الشخصي منخفضة التكلفة.

7. تشجيع الاستخدام الفعال للبنية التحتية، من خلال صياغة المحتوى الوطني والإقليمي الموجه نحو تعزيز الهوية الثقافية.

8. تنشيط استعمال اللغات في جميع البلدان مع تغطية جميع جوانب الحياة اليومية بهدف تحسين نوعية الحياة.

9. التعبير عن رؤية عالمية أو خطة عمل بأهداف محددة، متدرجة محددة زمنياً لمعالجة الفجوة الرقمية، قبل المؤتمر العالمي التالي لتنمية الاتصالات مثلاً.[1]

10. وضع التشريعات القانونية وجعلها أكثر تطورا، عن طريق ضرورة مسايرتها لخصائص مجتمع المعلومات، والاتجاه إلى المجتمع الرقمي خاصة في مجال حقوق التأليف الفكرية والرقمية، وأمن المعلومات وغيرها[2].

11. تطوير التأهيل والتكوين عن طريق إصلاح التعليم، بمختلف مستوياته خاصة أما التحدي ومقتضيات مجتمع المعلومات، حيث أصبحت تكنولوجيا المعلومات هي العامل الحاسم في تقدم الشعوب وتطورها.

---

[1]- المؤتمر العالمي لتنمية الاتصالات،سد الفجوة الرقمية، 18 مارس 2002،الوثيقة A-166، إسطنبول، تركيا، ص 6.

[2] -En France :l'article 25 de la loi n° 2009-1572 du 17 décembre 2009 relative à la lutte contre la fracture numérique dispose que « Dans les six mois suivant la publication de la présente loi, le Gouvernement remet au Parlement un rapport sur le fossé numérique afin d'apporter des précisions quant aux différentes catégories de la population n'ayant ni équipement informatique, ni accès à Internet dans leur foyer. Ce document étudie également le rapport qu'entretiennent les "natifs du numérique avec Internet dans le but d'améliorer les connaissances quant aux conséquences, sur le travail scolaire notamment, de l'usage d'Internet. Il dégage aussi les pistes de réflexion pour les actions de formation à destination de ces publics et veille également à identifier les acteurs associatifs œuvrant pour la réduction du fossé numérique. Enfin, il établit les conditions de mise en service d'abonnements Internet à tarif social. Dominique Auverlot ,Joël Hamelin ,et autres, Le fossé numérique en France, Rapport du Gouvernement au Parlement ,établi en application ,de l'article 25 de la loi n° 2009-1572 du 17 décembre 2009, relative à la lutte contre la fracture numérique ,avec la collaboration pour l'analyse ,internationale du cabinet conseil BearingPoint,2011, P 23.

12. توظيف وتشجيع إستخدام التكنولوجيا الحديثة والإتصالات في خدمة الإنتاج الفكري، وتعزيز المحتوى الرقمي، وتدعيم البحث العلمي، والإبداع، والإكتشاف والإختراع، فليس المهم إقتناء التجهيزات المتقدمة، وبناء شبكات حديثة فقط بل الأهم من ذلك هو كيف أن نوظف هذه التكنولوجيا وأين نوجهها.

13. زيادة التعاون بين الدول النامية، من خلال تبادل الخبرات والقيام بالمشروعات المشتركة في مجال صناعة المعلومات والمعلوماتية والبرمجيات العلمية والتدريب والبحث العلمي والتطبيقي.

14. القضاء على الأمية المعلوماتية، عن طريق وضع سياسة خاصة بمجال التأهيل والتعليم، وإدخال التكنولوجيا في كل المؤسسات التعليمية والتربوية.

15. تشجيع الترجمة الفورية لمصادر المعلومات المختلفة، خاصة تلك المتاحة بلغة الدول المتقدمة من أجل الإستفادة مكنها و تسهيل الوصول إليها.

16. تشجيع المبادرات الفردية لمختلف المؤسسات المعلوماتية خاصة الناجحة منها و تدعيمها ماديا ومعنويا، والإستفادة منها وتعميمها.[1]

الفرع الثاني : إستراتيجية عربية لمواءمة تقنيات المجتمع الرقمي

ينبغي على العالم العربي أن يستشف مركزا متوازنا في المنظومة الكونية الراهنة، فالتيار المعلوماتي الجارف لكل تضاريس الأرض أمس أمرا ليس من قبيل الاستثناء لبعض المناطق العربية، والمعرفة الرقمية أصبحت تمثل مطلبا جذريا، في تحقيق التكامل المعلوماتي لمجتمع المعلومات العالمي، الذي أصبحت تمثل فيه الحياة الافتراضية جوهر التعاملات الالكترونية.

بيد أن الحياة التخيلية في مفكرة بعض التيارات، تبشر بأفول العصر الورقي وبزوغ مفهوم جديد من المجتمعات وهو "المجتمع اللاورقي"، المجتمع الذي يفترض فيه أن تكون فيه الإدارة والتعاملات الحياتية بدون ورق أي إدارة حياة اليكترونية.

[1]- عامر إبراهيم قندليجي، تكنولوجيا المعلومات وتطبيقاتها، عمان، الوراق للنشر والتوزيع،2002،ص 80.

وإزاء كل التطورات الراهنة والاحتمالات المستقبلية لأدوات مجتمع المعلومات، كان لابد من الإشارة إلى عدة نقاط تتمركز جميعها حول الدولة الافتراضية لمجتمع المعلومات الالكتروني، والذي يدور في فلك الأمن الرقمي .

إن المنطقة العربية هي إحدى المناطق التي يعوزها إلى حد كبير إحداث مثل تلك التغييرات، والتي يجب تسخير إمكانيات تقنية المعلومات والاتصالات فيها كأحد عوامل التغيير.

البند الأول : ورشات التنسيق الإقليمي العربي لتجسير الفجوة الرقمية "برنامج اقتدار"

يوجد العديد من مبادرات الحكومة الإلكترونية في المنطقة العربية على مستويات مختلفة من النطاق والتأثير، وتعمل هذه المبادرات من برنامج اقتدار، على تجسير فجوة التنسيق الإقليمي، وتوفر الدعم الفني والخبرة للبلدان التي تحتاج إليها، وتتألف المبادرة من أربعة مسارات رئيسية متكاملة: ورشات التنسيق بين البلدان العربية، المعهد الإقليمي للحكومة الإلكترونية والبوابة الالكترونية للحكومة الإلكترونية والتدخلات المباشرة.

قد طور برنامج اقتدار مبادرته الخاصة بالحاكمية الإلكترونية، بهدف تسخير التقنية بوصفها أداة لتحديث الإدارة العامة، تقود إلى تنمية وطنية طويلة الأجل، وتتراوح المشاريع تحت مظلة هذه المبادرة بين صياغة السياسات (الحكومات الإلكترونية والإستراتيجيات الإلكترونية)، إلى توجيه التدخلات لتأسيس خدمات قائمة على أساس تقنية المعلومات والاتصالات[1].

[1]– ومن بين الشركاء الذين تعاونوا مع برنامج اقتدار في مشاريع الحاكمية الإلكترونية الجهات التالية:

حكومة البحرين، حكومة جيبوتي، حكومة المغرب، حكومة السودان،حكومة تونس،مكتب المعلوماتية المركزي، البحرين وزارة الاتصالات وتقنية المعلومات، مصر، مكتب وزير الدولة للإصلاح الإداري، لبنان ،وزارة التعليم، المغرب . جامعة الدول العربية المكاتب القطرية لبرنامج الأمم المتحدة الإنمائي، إدارة الشؤون الاقتصادية والاجتماعية التابعة للأمم المتحدة، اليونسكو، لجنة الأمم المتحدة الاقتصادية لإفريقيا، برنامج الأمم المتحدة لمكافحة مرض الإيدز في المنطقة العربية ،منشأة الموارد الإقليمية الفرعية للدول العربية، شركة مايكروسوفت، الاتحاد العربي، المغرب، الاتحاد العربي للأمية مركز المرأة العربية للتدريب والبحوث، جمعية الحاسوب السورية، وفي الجزائر تم الاتفاق على إنشاء 10 مراكز لتكرار نموذج العمل الذي طُوّر في دورة أجيالكم – مشروع أجيالكم هو مبادرة إقليمية لتفعيل دور الشباب أطلقها وبدأ في تنفيذها برنامج اقتدار عام 2004. ويهدف المشروع إلى تفعيل دور الشباب في العالم العربي، وتوفير الفرصة لهم لاستغلال طاقاتهم من خلال استخدام تقنية المعلومات والاتصالات ،لتيسير وتسهيل الحصول على المعرفة والتواصل، وتوفر أماكن الالتقاء بما يمكنهم من التشاور وتبادل المعلومات ،ومناقشة الموضوعات ذات التأثير على حاضرهم ومستقبلهم، لمزيد من التفاصيل أنظر : www.ictdar.org

البند الثاني : بوابة التشارك العربي في الحكومة الالكترونية

تعتبر بوابة التشارك العربي في الحكومة الالكترونية (*e-Gove@ASP*) أداة هامة لفهم التعاون العربي–العربي التي توجد حاجة ملحة له في مجال الحكومة الالكترونية، إن برنامج اقتدار على علم واطلاع تام بالمبادرات العديدة، التي تعمل عليها الحكومات في المنطقة بهدف تأسيس خدمات الحكومة الالكترونية وبرامجها، لأن اقتدار يقدم الدعم المؤثر للعديد من هذه المشاريع.

ومع ذلك هناك القليل إن وجد، من التشارك في الخبرات والدروس المستفادة، وحيث أن اقتدار يؤمن بأن التشارك في المعلوماتية، هو من الأمور المفصلية لصانعي القرار في المنطقة، فقد حرص على أن يكون فاعلا ونشطا في تشجيع مثل هذا التعاون من خلال ورشات العمل الإقليمية بخصوص الحوكمة الإلكترونية، بما في ذلك الحكومة الالكترونية.

ومع ذلك كانت هناك حاجة لتأسيس أداة تكون متاحة باستمرار تحت تصرف الحكومات العربية وصانعي القرار والممارسين والأكاديميين، وتهدف إلى تحسين التدفق المعرفي وتوفر المعلومات، وقد أدى ذلك إلى تطوير بوابة التشارك العربي في الحكومة الالكترونية والتي تم تصميمها لتكون منبرا للتعاون والتشارك المعلوماتي حول الحكومة الالكترونية، وتهدف أيضا إلى تزويد الحكومات بالمعرفة التي تحسن من صنع القرار على المستويين الاستراتيجي والتشغيلي، بالإضافة إلى محاكاة تطور المجتمعات الممارسة والمجتمعات ذات الاهتمام.

الفرع الثالث : التجربة الأمريكية في حماية منظومتها المعلوماتية و تأمينها رقميا .

من المفيد عند الحديث عما يجب إتباعه للوصول إلى منظومة متكاملة لتأمين المعلومات، النظر إلى تجارب الدول المختلفة في هذا الشأن، وخاصة الدول المتقدمة منها والتي وصلت فيها درجة الاعتمادية على الأنظمة الفنية وشبكات المعلومات والاتصالات إلى درجة عالية، حتى تتوافر لنا الرؤية الشاملة لما يجب أن تكون عليه المنظومة الجزائرية في هذا المجال.

وفي هذا الصدد يجب الإشارة إلى أنه بالرغم من تواجد بعض الخصوصيات لهذه الدول، من حيث استخدام وتطبيق تلك التقنيات إلا أنه توجد بعض العناصر المشتركة والأساسية والتي تشكل أولوية أولى للجزائر، وهي التي يجب البدء في تنفيذها دون الانتظار لتكامل أطراف العملية التقنية و القانونية .

وتعتبر التجربة الأمريكية هي التجربة الدولية الرائدة، في هذا المجال والتي يجب التعرض إليها ودراسة جوانبها المختلفة.

فالحديث عن الإطار التشريعي المنظم لضمان سلامة الأمن القومي الأمريكي، نبدأ ب:

1.قانون حرية المعلومات *Freedom of Information Act* لعام 1966 والذي يعد أساسا لتنظيم الحصول على الملفات والمعلومات الحكومية، تحت شعار "الحق في المعرفة"

2. قانون حماية الخصوصية لعام 1974، *(The Privacy Act)*والذي اختص بحماية الخصوصية الفردية في الملفات الخاصة بالمواطنين.

3.وتعاقبت القوانين والتعديلات عليها، والخاصة بحرية المعلومات وتداولها والحق في الحصول عليها، مع الاحتفاظ بدرجة السرية المطلوبة، حتى عام 1996حيث صدر التعديل المسمى حرية المعلومات الالكترونية *(The Electronic Freedom of Information Act- EFIA)*والذي يطالب جميع الجهات بتحويل بعض الملفات إلى الصورة الإلكترونية وإعداد غرف خاصة لإطلاع المواطنين عليها.

4. ثم جاء عام 2002 وحمل معه القانون الفيدرالي لأمن المعلومات [1] ،والذي يعتبر هو القانون الأهم في منظومة قوانين أمن المعلومات الأمريكية، حيث أنه يوفر الإطار العام لتأمين نظم تكنولوجيا المعلومات والاتصالات والمحتوى الرقمي، في كافة الهيئات والمؤسسات الواردة بنص القانون، والذي يطالبها بالعديد من الإجراءات القياسية التي أصدرها المعهد القومي للمعايير القياسية والتكنولوجيا[2].

وتتم الرقابة أيضا من خلال فريق الاستعداد *United States Computer Emergency Readiness Team- (US-CERT).*والذي يعتبر جزئا رئيسيا من وحدة الأمن القومي الافتراضي*National Cyber Security Division*، والذي تم إنشاءه عام *2003* بالتعاون بين كلا من القطاع الحكومي والخاص، بغرض تنسيق الرد والتعامل مع مخاطر التأمين من خلال شبكة الإنترنت، حيث يقوم بإصدار الدوريات بأهم المخاطر الموجودة بالشبكة، ويقوم أيضا

[1] -http://en.wikipedia.org/wiki/Federal...ent_Act_of_2002.

[2] -http://csrc.nist.gov.

بالتعاون مع القطاع الخاص بتطوير نظم التأمين والإصلاح لأنظمة المعلومات والاتصالات ضد الاختراقات المحتملة، وتعتبر هذه هي نقطة الالتقاء فيما يخص تأمين الشبكات وأنظمة المعلومات وشبكات الإنترنت بالولايات المتحدة الأمريكية.

ما يمكننا قوله أيضا هو أن قضية الأمن المعلوماتي أضحت من التحديات الكبرى على الصعيدين الإقليمي والعالمي، لا سيما في ظل تنامي التهديدات الأمنية الإلكترونية، سواء من جهة ارتفاع عدد الهجمات أو الجرائم أو الأضرار الناجمة عنها، إلى خلق تحديات كثيرة أمام النظام القانوني القائم في العديد من الدول ،وخاصة في ما يتعلق بمكافحة هذه الظاهرة، الأمر الذي دعا الفقه والقضاء إلى البحث فيما إذا كانت النصوص القائمة، كافية لمواجهة هذه الجرائم بشتى أنواعها أم أن الأمر يستدعي استحداث قوانين أو نصوص خاصة قادرة على احتوائها ومراعاة طبيعتها و خصوصيتها.

وفي هذا الفلك أقدم المشرع الجزائري إلى سن قوانين تنصب في إطار الأمن الرقمي، والانخراط في معاهدات إقليمية ودولية لتعزيز التعاون الدولي في هذا المجال،الفصل الثاني الجهود الدولية في مجال الأمن المعلوماتي.

الفصل الثاني:

الجهود الدولية في مجال الأمن المعلوماتي.

إذا كان للتقدم التقني واستخدام الحاسب الآلي[1] والانترنت مزايا وإيجابيات، فإن له كما هو شان كل الاكتشافات والاختراعات الجديدة مشاكل وسلبيات، و أحد مظاهر هذا التقدم ظهور صور جديدة من الجرائم لم تكن معروفة في الماضي[2]، وكذا ظهور مشاكل قانونية وفقهية منها فكرة المجرم المعلوماتي الذي بمقدوره استخدام وسائل التقنية الحديثة، أن يتوصل إلى أنظمة الحاسب الآلي في أي مكان في العالم، وكذلك فكرة المال المعلوماتي (غير المادي) المتمثل في البرامج والمعلومات والبيانات أيا كان موضوعها، كل ذلك أدى إلى تعدد الجهود المبذولة سواء على الصعيد الدولي أو المستوى الإقليمي[3].

ولأن النظام القانوني كائن حيوي يعكس ميول واتجاهات واحتياجات المجتمع ونزعاته للتنظيم لجهة وحماية الحقوق الفردية والجماعية، عبر قواعد التشريع في فروعه المختلفة، فمن

---

[1] -عرف الحاسب الآلي بأنه " مجموعة من الأجهزة التي تعمل متكاملة مع بعضها البعض، بهدف تشغيل مجموعة البيانات الداخلة طبقا لبرنامج تم وضعه مسبقا، للحصول على نتائج معينة. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، مصر ،1992 ، ص6 .

[2] – بعد تطور أشكال الجريمة مع استخدام الحاسب الآلي والانترنت واستهدافها لكافة المصالح و الحقوق ، أصبحت الجرائم الإلكترونية تقع على الأشخاص و الأموال والمعلومات ، سواء في القتل أو التحريض على الانتحار و التسبب في الأضرار والمضايقات غير الأخلاقية، و انتهاك سرية البيانات الشخصية، و تحريض القاصرين على أنشطة جنسية غير مشروعة ، و التحرش الجنسي بالقاصرين، و نشر الأشياء الفاضحة المخلة بالحياء و تخريب النظم و المعلومات وخلق البرامج الضارة وإرسالها ،و إدخال معلومات خاطئة إلي نظام الحاسب الآلي، والاحتيال و التلاعب في البطاقات المالية وسرقة المعلومات، و تزوير البريد الإلكتروني، وتشجيع مشروعات المقامرة وترويج المواد الكحولية و المخدرات وتعطيل الأعمال الحكومية، و العبث بالأدلة القضائية وتهديد السلامة، ونشر الإرهاب الإلكتروني وغيرها من الممارسات غير المشروعة، التي ترتكب بواسطة الحاسب الآلي و الانترنت .

[3]– على الصعيد الدولي ،عقدت الأمم المتحدة العديد من المؤتمرات لمواجهة الجرائم الإلكترونية ،وإصدار الكثير من التوصيات ، ففي المؤتمر السابع للأمم المتحدة الخاص بمكافحة الجريمة ومعاملة المجرمين ،أشار المؤتمر إلى جرائم الحاسب الآلي والصعوبات المتعلقة بها، باعتبارها من الجرائم المتعدية الحدود ذات الطابع الاقتصادي، وفي اوت عام1995 عقد المؤتمر الثامن لمكافحة الجريمة ومعاملة المجرمين في هافانا، وكانت الجريمة الإلكترونية والاهتمام بمكافحتها وملاحقتها، أحد الموضوعات التي تم بحثها من خلال ندوة أقيمت لهذا الغرض، كما دعت الوكالات والمؤسسات ذات الطابع الدولي، إلى التدخل لحماية المعلومات وعدم الاعتداء عليها، وفى مقدمة هذه الوكالات منظمة التنمية والتعاون الاقتصادي .

الطبيعي أن تتأثر علاقاته وقواعد مرتكزات التشريع فيه بما خلقته التقنية العالية من آثار وما أنتجته من أنماط جديدة للعلاقات القانونية، عبر حركة تشريعية تعكس استجابة التشريع للجديد والمستجد في هذا الحقل .

والأمن المعلوماتي الأكثر أثارة للجدل، فهو عالم متداخل ومتشابك يطرح السؤال الأهم، هل نحتاج لمواجهة مخاطره إلى إطار قانوني ينظم شؤونه وتحدياته ؟ أم هو تعبير مصور جديد لمجتمع لم تتكامل عناصره بعد، مما يتعين التريث في تنظيمه ؟؟ وأن كان ثمة حاجة للتنظيم القانوني للأمن المعلوماتي، فما الذي أنجزته حتى الآن الدول الغربية و العربية ؟ وما المطلوب منها أن كانت ثمة مهام لم تنـــجز بعد ؟؟.

المبحث الأول : التشريعات الهادفة لاستتباب الحماية المعلوماتية.

لم تواكب التشريعات الداخلية تطور التقنية عموما، ولو كانت هناك بوادر لوضع بعض النصوص إلا أنها بقيت في الغالب محصورة في مجرد حماية لنظام المعالجة الآلية للمعطيات كمفهوم عام و لم تعالج الأفعال المقترفة بشكل مفصل، و التي تتطور بشكل مذهل في الثانية الواحدة و كأنها مسابقة عالمية بين المخترقين و القراصنة، حول من يبتكر أكثر جريمة انترنت تطورا و سرعة، وما ألحقته من خسائر حتى بالدول المتقدمة.

– و بخروج جرائم الانترنت من عالم الهواة إلى عالم الجريمة المنظمة و الحرب الباردة الالكترونية، مازالت الدول و خاصة النامية منها في خطواتها الأولى، لتعريف هذا النوع من الجرائم، وسن بعض القوانين المعاقبة رغم إدراكها لضرورة التصدي لهؤلاء المجرمين، و هو ما أدى بتكافل الجهود لسن قواعد عالمية [1]،تتبع الدول خطاها لتجريم الممارسات اللاأخلاقية عبر الانترنت و الماسة بأمن الأفراد و الدول، و بذلك سيتناول في المطلب الأول **موقف التشريعات الدولية من الجرائم المعلوماتية** و في المطلب الثاني سيتطرق **الاتفاقيات و المعاهدات الدولية و الاقليمية**

المطلب الأول: موقف التشريعات الدولية من الجرائم المعلوماتية.

أن التطور التقني والتكنولوجي الذي نشهده اليوم يسبق بكثير التشريعات التي من المفترض أن تواكبه، لذا يجب على الدول العربية اتخاذ مجموعة من الخطوات والإجراءات الإستراتيجية، على كافة الأصعدة وبالأخص خطوات وإجراءات تدخل ضمن النطاق التنظيمي، لاسيما أن التطور الذي يمتاز بوتيرة متسارعة يجعل الكثير من النصوص والأحكام التنظيمية القائمة غير منطبقة وقد تجاوزها الزمن، فردعا للجرائم المعلوماتية والانترنيت ، كان لابد للدول العربية المتقدمة من اتخاذ كافة الإجراءات القانونية والتي تهدف إلى معاقبة شتى أنواع الاعتداءات على الأنظمة المعلوماتية.

[1] – The Conference of Digital Information Technology, Modren Trends in The Information Technology ,Amman - Jordan 13-15 May 2014.

الفرع الأول : التجربة الأوروبية في حقل أمن المعلومات.

البند الأول : التدخل التشريعي الفرنسي للحد من الإجرام المعلوماتي.

اهتمت فرنسا بتطوير القوانين الخاصة بها للتوائم مع الجرائم لتكنولوجية الحديثة (جرائم الانترنت) [1]، فقد طورت فرنسا قوانينها الجنائية للتوافق مع المستجدات الإجرامية، حيث أصدرت أول قانون خاص بها (*the first special Law*)، في عام 1988، القانون رقم (88-19)[2] ، والذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي العقوبات المقررة لتلك الجرائم كما تم في 1994، تعديل قانون العقوبات لديها ليشمل مجموعة جديدة من القواعد و القانونية الخاصة بالجرائم المعلوماتية، و قد أوكل هذا القانون إلى النيابة العامة سلطة التحقيق فيها، بما ذلك طلب عمل التحريات و سماع الأقوال و الشهود[3].

و الواقع انه فيما يخص الجرائم المعلوماتية فان قانون العقوبات الفرنسي يحتوى على نوعين من القواعد :

1. النوع الأول : يشمل مجموعة القواعد العادية (التقليدية)، و التي يمكن أن تنطبق في حالة ما إذا كانت الجريمة واقعة على المكونات المادية لنظم المعلوماتية، مثل جرائم السرقة و الإتلاف و خيانة الأمم ...الخ، و هذه الجرائم لا تختلف عن جرائم العادية، فهي تأخذ حكمهما الوارد في النصوص العامة .

[1] - G .Zeviar-Geese, The State of the Law on Cyber juridiction and Cyber crime on the Internet,California Pacific School of Law, Gonzaga Journal of International Law, Volume 1. 1997-1998.

[2] - la loi Godfrain - Loi informatique punissant les intrusions dans des systèmes informatisés,5 Janvier 88,loi 88/19 ,proposition de loi, modifiée par le Sénat en deuxième lecture, n°1182 ,rapport de M. André, au nom de la commission des lois, n°1184 ,discussion et adoption le 22 décembre 1987 ,Journal officiel du 6 janvier 1988, dite la loi Godfrain, à mise en place le délit d'accès frauduleux à un Système de Traitement Automatisé de Données, autrement dit un STAD.

[3] -J. Francillon, Les crimes informatiques ET dautres crimes dans le domaine de la technologie informatique en France,Rev. intpen, 1990, vol 64, p. 293.

2. النوع الثاني : فيشمل مجموعة من القواعد الخاصة بجرائم المعلوماتية و التي تمت إضافتهما عندما استفلحت ظاهرة الإجرام المعلوماتي، و الحقيقة انه قد تمت إضافة هذه القواعد إلى قانون العقوبات الفرنسي على مراحل ثلاثة اعتبارا من عام 1978م:[1]

1. في المرحلة الأولى :

صدر قانون 6يناير 1978 م المتعلق بالمعلوماتية و الحريات، والواقع أن هذا القانون كان قاصرا على حماية ما يسمى بالمعلومات الاسمية، و لهذا السبب فان الحماية التي يقدمها قد اقتصرت على حماية الشخصية ***identité*** و الحرية ***liberté*** و سرية الحياة الخاصة للأفراد ***le secret de la vie privée des personnes*** .

و قد استحدث قانون 6 يناير 1978[2] جرائم جديدة لردع مخالفة أحكامه، فالمسؤول عن التعسف في معالجة المعلومات الاسمية، يمكن أن يسال جنائيا بالإضافة إلى مسؤوليته المدنية لو سببت معالجته الخاطئة ضررا لشخص آخر .

و قد أجملت المادة الأولى من هذا القانون، الأهداف التي توخاها المشرع من وراء إصداره بقولها أن "المعلوماتية لابد و أن تكون في خدمة المواطن، و أنها لا ينبغي لها أن تستخدم كوسيلة للاعتداء على الشخصية الإنسانية، و لا على الحقوق الإنسان و لا على الحياة الخاصة و لا على الحريات الفردية أو العامة"، و قد استحدث هذا القانون أنواع من الجرائم يمكن ذكرها في الآتي:

أولا : عدم احترام الشكليات اللازمة و السابقة على معالجة المعلومات الاسمية .

ثانيا : جمع المعلومات الاسمية و الاحتفاظ بها بصورة غير شرعية .

[1]– طارق إبراهيم الدسوقي عطيه ، الأمن المعلوماتي ،النظام القانوني لحماية المعلوماتية، دار الجامعة الجديدة ،بدون طبعة ، 2015، ص 253.

[2] -le législateur intervient une première fois par une loi du 6 janvier 1978 sur l'informatique, les fichiers et les libertés. Quelques années après, la fraude informatique fut prise en considération par le législateur, Notamment par la loi du 5 janvier 1988 relative à la fraude informatique, appelée LOI GODFRAIN. Cette loi crée 6 incriminations qui s'intègrent au code pénal dans un chapitre III, intitulé *"De certaines infractions en matière informatique"*

ثالثا : إنشاء المعلومات الاسمية بطرق غير شرعية [1].

2. في المرحلة الثانية :

لاحظ المشرع استفحال ظاهرة الإجرام المعلوماتي، و لذلك كان لابد من التدخل ثانية لتضمين قانون العقوبات نصوص جديدة من شانها مواجهة هذه الظاهرة، و لهذه الغرض تم التفكير في تقديم مشروع لتعديل قانون العقوبات و قدم هذا المشروع بالفعل إلى البرلمان الفرنسي تحت عنوان "الجرائم في مواد المعلوماتية "أو « *les infraction en matière informatique* ، و لكن لم يتم اعتماد هذا المشروع رغم بقاء الحاجة لمواجهة ظاهرة تضخم الإجرام المعلوماتي في المجتمع الفرنسي، غير انه في شهر أوت 1986م تقدم النائب *JACQUES GODFRAIN* باقتراح قانون تم بالفعل اعتماده بواسطة البرلمان الفرنسي، وصدر به قانون 5 يناير 1988م الذي تم إدماجه في قانون العقوبات الفرنسي [2]و خصص له الفصل الثاني (المواد من 2/462الى 9/462) تحت عنوان بعض الجرائم في المواد المعلوماتية "أو" des certaines *infraction en matière informatique*، والجدير بالذكر أن المخصص لهذه الجرائم تم إلحاقه بالباب المخصص للجنايات والجنح ضد الأشخاص *crimes et délits contre les particuliers*، و بالتحديد بعد الفصل الثاني من هذا الباب المخصص للجنايات و الجنح ضد الملكية « *crimes et délits contre les propriétés*.[3]

1 - Jean Pradel, Les infractions relatives à l'informatique, Revue internationale de droit comparé ,Année 1990 Volume 42 ,Numéro 2, pp. 815-828 .

[2]– طارق إبراهيم الدسوقي عطيه ، نفس المرجع ،254.

[3] - la loi Godfrain du 5 janvier 1988, dans le code pénal des dispositions spécifiques à l'accès et maintien frauduleux ,dans un système de traitement automatisé de données (art. 323-1 Code pénal), des nouveaux problèmes liés à la technologie de l'information ne cessent d'apparaître, Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004 Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an (2 ans) d'emprisonnement et de 100 000 F (15000 euros) (30000 euros) d'amende.

و يشار إلى لجنة التشريعية قد ركزت على كون الهدف من النصوص الجديدة هو ردع الدخول غير المشروع على برامج المعلوماتية، و ذلك باعتبارها الهدف الذي توخاه اقتراح النائب *Godfrain* و هو : "حماية النظام المعلوماتي ذاته ضد أي اعتداء خارجي، فهذه الجريمة تعد بحق التجريم الأساسي الذي أتى به النص الفرنسي الجديد (المقترح) .

و في قانون 1988 احتلت هذه الجريمة مكانا أساسيا، و يمكن القول بأنه إذا طرحنا جانبا مسالة تزوير الوثائق المعلوماتية، فان الجرائم المعلوماتية تنبثق عن – أو تدور حول – جريمة الدخول غير المشروع آلة نظم المعلوماتية « *l'accès frauduleux* » أو البقاء فيها،و بتجريم هذا الفعل يمكن القول بان هذا القانون قد لبى حاجة ملحة جدا بتقديمه الحماية اللازمة لنظم المعلوماتية .[1]

ونظرا لأهمية قانون 5 يناير 1988 الخاص بجرائم المعلوماتية، على اعتبار أنه يمكن الاستفادة منه تشريعيا و فقهيا، فسوف نعرض فيما يلي لاهم ما جاء من نصوص، علما بان هذه المواد قد تم تعديلها جزئيا على عام 1994 كما تم نقلها ضمن أحكام أخرى من قانون العقوبات بعد تعديله .

- مادة وحيدة: يضاف إلى الباب الثاني من قانون العقوبات بعد الفصل الثاني فصلا نصه كالأتي :

مادة 2/462 : "يعاقب بالحبس من شهرين إلى سنة و بغرامة تتراوح ما بين ألفين إلى 50 ألف فرنك آو بإحدى هاتين العقوبتين كل من دخل أو مكث غدرا في نظام المعالجة الآلية للمعلومات آو جزء منه [2].

---

[1] – طارق إبراهيم الدسوقي عطيه، نفس المرجع، 255.

Jean Pradel ,Les infractions relatives à l'informatique ,Revue internationale de droit comparé, ,1990 Volume 42, N 2 , p. 815.

[2] - la loi Godfrain du 88/19 Dans le titre 2 du livre 3 du code pénal,Chapitre 3 , De certaines infractions en matière informatique:

Article 462-2 :Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2.000F à 50.000F ou de l'une de ces deux peines. Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le

و في حالة ما إذا نتج عن ذلك إلغاء أو تعديل المعلومات، التي يحتويها النظام كإتلاف عمله، فان العقوبة تكون الحبس من شهرين إلى عامين و الغرامة من 10 ألاف إلى 100 ألف فرنك .

مادة 3/462: يعاقب بالحبس لمدة تتراوح من ثلاث أشهر إلى ثلاث أعوام و بغرامة من 10 ألاف إلى 100 ألف فرنك أو بإحدى هاتين العقوبتين،كل من اضر أو زيف بطريقة عمديه و إضرارا بحقوق الغير نظام المعالجة الآلية للمعلومات [1].

مادة 4/462: يعاقب بالحبس لمدة تتراوح من ثلاثة أشهر إلى ثلاثة أعوام و بغرامة من 20الف إلى 500 ألف فرنك أو بإحدى هاتين العقوبتين، كل من قام عمدا بطريقة مباشرة أو غير مباشرة و إضرار بحقوق الغير، بإدخال معلومات إلى نظام معلوماتي معين او تعديل أو إلغاء بث المعلومات التي يحتويها[2].

مادة 5/462: يعاقب بالحبس لمدة تتراوح من عام إلى خمسة أعوام و بغرامة يتراوح مقدارها من 20 إلى 2 مليون فرنك، كل من قام بتزييف وثائق معلوماتية مهما كان شكلها أو طبيعتها ، و ذلك إضرار بالغير[3] .

---

système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 10.000F à 100.000F.

[1] - Article 462-3- de la loi Godfrain 88/19:Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 10.000F à 100.000F ou de l'une de ces deux peines.

[2] - Article 462-4 de la loi Godfrain 88/19 :Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 2.000F à 500.000F ou de l'une de ces deux peines.

[3] - Article 462-5 de la loi Godfrain 88/19 :Quiconque aura procédé à la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20.000F à 2.000.000F.

مادة 6/462 يعاقب بالحبس من عام إلى خمسة أعوام و بغرامة تتراوح من 20الف الى 2 مليون فرنك، أو بإحدى هاتين العقوبتين، كل من قام عمدا باستخدام الوثائق المعلوماتية المشار إليها في المادة 5/465.[1]

مادة 7/462: يعاقب على الشروع في الجرائم المنصوص عليها في المواد 2/462 إلى 6/462 بنفس العقوبات الجرائم نفسها [2].

مادة 8/462: كل من شارك في جمعية أو كان عضوا في اتفاق يهدف إلى التحضير لارتكاب فعل او عدة أفعال مادية، لجريمة او عدة جرائم من تلك المنصوص عليها في المواد من 2/462الى 6/462 يعاقب بالعقوبات المقررة لهذه الجرائم أو بالعقوبة المقررة لأخطر هذه الجرائم [3].

مادة 9/462: يمكن للمحكمة أن تأمر بمصادرة المواد المتعلقة بالجاني، و التي تكون قد استخدمت في ارتكاب الجرائم المنصوص عليها في هذا الفصل[4] .

و على ذلك يكون هذا القانون، قد احتوى على عدة أنواع من الجرائم يمكن تقسيمها إلى ثلاث طوائف رئيسية .

---

[1] - Article 462-6 de la loi Godfrain 88/19 : Quiconque aura sciemment fait usage des documents informatisés visés à l'article 462-5 sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20.000F à 2.000.000F ou de l'une de ces deux peines.

[2] - Article 462-7 de la loi Godfrain 88/19: La tentative des délits prévus par les articles 462-2 à 462-6 est punie des mêmes peines que le délit lui-même.

[3] - Article 462-8 de la loi Godfrain 88/19:Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 462-2 à 462-6 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

[4] - Article 462-9 de la loi Godfrain 88/19 :Le tribunal pourra prononcer la confiscation des matériels appartenant au condamné et ayant servi à commettre les infractions prévues au présent chapitre.

- **الطائفة الأولى:** تشمل ثلاثة أنواع من الجرائم، تضمنها المواد من 2/462 الى 4/462 من قانون العقوبات و تهدف هذه الجرائم إلى حماية نظم المعلوماتية ذاتها، تشمل هذه الطائفة بدورها على ثلاث' جرائم مختلفة :

1. الدخول أو البقاء غير المشروع داخل المعلوماتية.*Accès ou maintien frauduleux*
2. الاعتداء على سير نظام لمعلوماتية. *Atteinte portée au fonctionnement d'un système*
3. إدخال معلومات بصورة غير شرعية في نظام المعلوماتية، أو إتلاف المعلومات الموجودة فيه *Intersection ou altération de données ou atteinte a leur transmission*[1]

- **أما الطائفة الثانية:** فتشمل نوعان من الجرائم تناولتها 5/462 الى 6/462 من قانون العقوبات المضافة بقانون 5 يناير 1988 و هاتين الجريمتين هما :[2]

1. تزوير الوثائق المعالجة معلوماتيا ..*Falsificauon des documents informatisés*
2. استخدام الوثائق المعالجة معلوماتيا المزورة. *Usage des documents informatisés falsifiésé*

- **وعن الطائفة الثالثة** : فهي تشمل عقوبتان تهدفان إلى الردع و تغليظ العقاب في المقام الأول، و نصت عليهما المواد من 7/462الى 9/462 و هما :

1- عقوبة الشروع في الجرائم السابقة، و التي تهدف إلى ردع النشاط الإجرامي لعصابات المعلوماتية.

2- عقوبة مصادرة الأدوات المستخدمة في الجريمة، أو المتحصلة عنها .

3. المرحلة الثالثة : تمثل اهتمام المشرع الفرنسي بالإجرام المعلوماتي في الرغبة في تعديل قانون العقوبات الفرنسي، و تضمينه أحكام جديدة للحد من هذا النوع من الجرائم، فقد تم تعديل قانون العقوبات الفرنسي في عام 1994 تحقيقا لهذا الغرض، وكان من مقتضى هذا التعديل،

---

[1] - A. Eric Caprioli, Les moyens juridiques de lutte contre la cybercriminalité, www.caprioli-avocats.com.
Première publication, Revue Risques n°51, Les cahiers de l'assurance, Ed. LGDJ/SEDDITA, juillet-sept 2002, p. 50-55.

[2] - طارق إبراهيم الدسوقي عطيه، نفس المرجع، ص 257.

إضافة فصلا ثالثا للباب الثاني من القسم الثالث من القانون العقوبات، و تمت تسمية هذا الفصل الثالث "الاعتداءات على نظم المعالجة الآلية للمعلومات " ...و يتكون من المواد 1/323 إلى 7/323:[1]

1. و تعالج المادة 1/323 من قانون العقوبات الجديد، مسألة الدخول أو البقاء غير المشروع إلى نظام المعالجة الآلية للمعلومات *Accès ou mantien frauduleux dans un système de traitement automatisé*.[2].

[1] - La Cour d'appel de Paris a considéré dans un arrêt du 5 avril 1994 que " l'accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers d'un système de traitement automatisé de données, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication ".
Quid, pourtant, si le système n'est pas protégé ? La Cour d'appel de Paris, dans un arrêt en date du 30 octobre 2002, a jugé que la possibilité d'accéder à des données stockées sur un site avec un simple navigateur, en présence de nombreuses failles de sécurité, n'est pas répréhensible.
Elle a, ainsi, reformé le jugement du Tribunal de grande instance de Paris, qui avait estimait que l'existence des failles de sécurité ne constituait " en aucun cas une excuse ou un prétexte pour le prévenu d'accéder de manière consciente et délibérée à des données dont la non-protection pouvait être constitutive d'une infraction pénale ".
En effet, l'article 226-17 du Code Pénal réprime le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles qu'elles ne soient pour préserver la sécurité de ces informations et notamment d'empêcher communiquées à des tiers non-autorisés.
http://www.murielle cahen.com/publications/p_intrusion.asp

[2]- article 323/1du code pénal français, Edition : 2015-11-22-

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système

- de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.
- Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de100 000 € d'amende

.

- Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende.
- http://codes.droit.org/cod/penal. Edition : 2015-11-22-

2. أما في المادة 2/323 من قانون العقوبات الجديد [1]فتعالج الاعتداءات الإرادية على سير نظم المعالجة الآتية للمعلومات، بحيث يترتب على ذلك تعطيل سير النظم أو إعاقته، والعقوبة التي أقرتها هذه المادة عن الأفعال من هذا القبيل، هي السجن لمدة ثلاث سنوات و الغرامة التي تصل إلى 300 ألف فرنك فرنسي، و هذه المادة عبارة عن ترديد لمحتوى المادة 3/462 من قانون العقوبات القديم.

3. و المادة 3/323 من قانون العقوبات الفرنسي الجديد تعالج الاعتداءات الموجودة داخل هذه المادة لهذا النوع من الأفعال هي نفس العقوبات المقررة عن الأفعال المنصوص عليها في المادة 2/323 سافلة الذكر، و هذه العقوبات هي عبارة عن السجن لمدة ثلاث سنوات و الغرامة التي تصل إلى 300 ألف فرنك فرنسي .

4. أما الشروع في ارتكاب هذا النوع من الجرائم فقد نصت عليه المادة 7/323 من قانون العقوبات الفرنسي الجديد و التي تعاقب على الشروع بنفس هذه العقوبات[2].

5. هذا و تعالج المادة 4/323 من قانون العقوبات الجديدة[3]، الأفعال الصادرة عن عصابات الإجرام المعلوماتي *associations de malfaiteurs* ،في حالة لو كانت هذه الأفعال تشكل واحدة أو أكثر من الجرائم المنصوص عليها في المواد من 1/323 الى 2/323

---

[1] - 323-2 du C.P.F Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé
de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.
Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat,la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende .

[2] - Article 323-7 :La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines. Modifié par Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004

[3] - Article 323-4-La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. Modifié par Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004

-Article 323-4-1:Lorsque les infractions prévues aux articles 323-1 à 323-3-1 ont été commises en bande organisée et à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à dix ans d'emprisonnement et à 300 000 € d'amende. Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4

سافلة الذكر، و العقوبات المنصوص عليها في هذه المادة هي العقوبة او اشد العقوبات المقررة للفعل ذاته في المواد السابقة [1]. *falsification des documents*

6. أما تزوير الوثائق معلوماتيا فقد عالجته المادة 1/441 من قانون العقوبات الجديد [2] *informatisés*، و الوثائق المعالجة معلوماتيا في معنى هذه المادة يقصد بها، الشرائط... *disques*... و شرائط الكمبيوتر *bandes magnétiques* الممغنطة ..الخ.

7. بالإضافة إلى ذلك فقد نصت المادة 5/323 في سبع بنود منها على مجموعة من العقوبات التكميلية[3]،بالإضافة إلى العقوبات الأصلية سابقة الذكر، و تتراوح هذه العقوبات

---

[1] - 323-7 du C.P.F–La tentative des délits prévus par les articles 323-1 à323-3-1 est punie des mêmes peines. –

[2] –Article 441-1:Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques.

Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45 000 euros d'amende. Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002.

[3] –Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

- 1 – L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
- 2 –L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
- 3 –La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
- 4 – La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
- 5 – L'exclusion, pour une durée de cinq ans au plus, des marchés publics;
- 6 – L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

و هي كثيرة، بين الحرمان من الحقوق المدنية و السياسية و نشر القرار الصادر بالإدانة في الجرائد و الأماكن لمعدة للنشر.[1]

البند الثاني : الولايات المتحدة الأمريكية

في عام 1976م صكت الولايات المتحدة الأمريكية، [2]قانونا يتعلق بحماية أنظمة الحاسوب كما حدّد معهد العدالة القومي، خمسة أنواع رئيسية للجرائم المعلوماتية وهي: جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحاسب الآلي، دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب.

وفي عام 1986م صدر تشريع يحمل الرقم (1213) ،عرّف فيه جميع المفردات الضرورية لتطبيق القانون على الجرائم المعلوماتية، كما وضعت المتطلبات الدستورية اللازمة لتطبيقه، وعلى اثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي[3].

كما صدر أيضا في الولايات المتحدة على المستوى الفدرالي (قانون أمن الحاسوب لسنة 1987)[4]والذي يقضي باتخاذ الوكالات الفدرالية خطوات ملائمة لتأمين وحماية أنظمة حواسيبها، وينظم هذا القانون مستويات الحماية والرقابة عليها والمسؤولية عن اغفالها، وتوالت بعد ذلك في التسعينات التعديلات والتشريعات الفرعية والقطاعية ذات العلاقة بأمن المعلومات[5].

- 7 - L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

[1]- طارق إبراهيم الدسوقي عطيه ، نفس المرجع، ص 260

[2] - See : Anne Fitzgerald, Australia, E-crim, proposed legislation, Computer and Telecomm unications Law Review, 2001, 7(2), N17-18.

[3]- جعفر حسن جاسم الطائي،جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، دار البداية، 2007،الأردن،ص ص 229-230 .

[4] - The Computer Security Law of 1987, Public Law No. 100-235 (H.R. 145), (Jan. 8, 1988).

[5] - Nancy F. Du Charme Robert F. Kemp ,Copyright Protection for Computer Software in Great Britain and the United States, A Comparative Analysis, Santa Clara High Technology Law Journal ,Volume 3,P260.

أما على مستوى الولايات، فقد سنت جميع الولايات، قوانين خاصة أو عدلت قوانين العقوبات لديها، بما يكفل النص على تجريم أنشطة جرائم الحاسوب مع تباين فيما بينها سواء من حيث صور النشاط المجرم، أو من حيث آلية التعامل مع محل الاعتداء، فقد نصت قوانين بعض الولايات، على المساواة بين معطيات الحاسوب والأموال المادية من حيث الحكم القانوني، مما يتيح انطباق نصوص التجريم التقليدية على جرائم الحاسوب باعتبارها تستهدف المعطيات المتخذة حكم الأموال المادية بنص القانون الصريح، من هذه الولايات مثلا، ولاية ألاسكا، التي أدخل قانونها الجديد الإتلاف المعلوماتي ضمن الأموال التي تخضع لنصوص الإضرار بالمال، وكذلك ساوى قانونها بين غش الإنسان وغش الآلة، وكذلك ولاية فرجينيا التي نص قانونها على اعتبار وقت أو خدمات الحاسوب، أو خدمات المعالجة الآلية للبيانات أو المعلومات أو البيانات المخزنة ذات الصلة بذلك مالا، – وبهذا الحكم يتحقق انطباق نصوص التجريم التقليدية فيما يتصل بالاعتداء على المال[1].

ولكن غالبية الولايات، سنت نصوص تشريعية صريحة في تجريم أنشطة إساءة استخدام الحاسوب، فنصت قوانين كل من أريزونا، كاليفورنيا، كولورادو، دبلاوار، فلوريدا، جورجيا، الينوى، متشجان، ميسوري، مونتانا، نيومكسيو، رودايسلاند، تينسي، أوتاوا، سكونسيت. على تجريم إتلاف القيم المعلوماتية غير المادية، وغش الحاسوب، والاستخدام غير المصرح به للحاسوب، وسرقة وقت أو خدمات الحاسوب، وإعاقة استخدامه، والتوصل غير المصرح به لتعديل أو تغيير أو إنشاء أو استخدام البيانات المخزنة في نظام الحاسوب.[2]

ولا يزال النشاط متناميا في هذا الميدان – سن قواعد وقوانين جديدة في ميدان الإجراءات الجنائية الخاصة بجرائم الكمبيوتر والانترنت، كما شهدت هذه السنوات موجة سن القواعد الخاصة بحماية وسائل ومعايير الأمن المعلوماتي .

ويمكن استظهار الاتجاهات الحديثة للحماية من جرائم تقنية المعلومات بما يلي :

---

[1] -Merwe vander ,computer crimes and other crimes against information technology in south africa .R .I.D.P.1993.P 554.

[2] -American Bar Association ,Task Force on the Federalization of Criminal Law, Report: Report on the Federalization of Criminal Law, 1998 A.B.A. SEC. CRIM. JUST. REP. 2, http://www.abanet.org/crimjust/fedreport.html.

1- إقرار قواعد إجرائية جديدة، في حقل الأصول الجزائية تنظم عمليات تفتيش نظم الكمبيوتر وقواعد الملاحقة والضبط و الإثبات والتحقيق، إضافة إلى إقرار عدد من القواعد التي تحمي الخصوصية فيما يتخذ من إجراءات جنائية في ميدان جرائم التقنية، وما يمكن تسميته بضمانات المتهم المعلوماتي .

2- تنامي التشريعات الناظمة لتقديم خدمات الانترنت ومواصفاتها القياسية (المعايير وقواعد حماية المستخدم) .

3- تنامي التشريعات في ميدان حماية الأطفال والأقليات من مخاطر الانترنت (الحماية من المحتوى الضار) .

4- تنامي الحركة التشريعية للحماية من مخاطر الاستيلاء على أرقام البطاقات المالية، إضافة إلى تطوير قواعد الحماية الجنائية والمدنية للبطاقات المالية والنقل الالكتروني للأموال .

5- وضع قواعد أصولية لإدارة مواقع النشر الالكتروني والمسؤولية عما يرد فيها .

6- تشكيل فرق تدخل سريع بشأن الحوادث والاعتداءات على شبكة الانترنت، وعلى البرمجيات وفي ميدان التصنت والتجسس الصناعي.

7- وضع استراتيجيات التشفير ودراسة مدى ملاءمتها مع حرية تدفق البيانات (معايير الأمن المعلوماتي) .

8- اعتماد استراتيجيات أمنية وقانونية في ميدان التجارة الالكترونية وما يتصل بها من حقوق المتعاقدين عبر شبكات الاتصال والانترنت .

9- ابرام اتفاقيات دولية وثنائية حول الاختصاص في ميدان جرائم التقنية.

10- اعتماد استراتيجيات أمنية وطنية وإقليمية ودولية وتدابير تشريعية، بشأن حماية النظم التقنية الصناعية وحماية امن المعلومات، والحماية من أنشطة منظمات الإجرام في ميدان المقامرة على الشبكات، وغسل الأموال وترويج المخدرات والدعارة .

11- تطوير المواصفات القياسية لخدمات الحوسبة والاتصال والانترنت[1]

البند الثالث : بريطانيا

سن المشرع البريطاني قانون مكافحة التزوير والتزييف سنة 1981 [2] وقانون إساءة استخدام الحاسوب لسنة 1990- (*Computer Misuse Act*) وبدء سريانه بتاريخ 29 اوت1990، وقد خلق هذا القانون ثلاث جرائم جديدة لمواجهة جرائم الاختراق والتوصل غير المصرح به، لتعديل معطيات الحاسوب وإتلافها بشكل عام، وجرائم إدخال الفيروس بشكل خاص هذه الجرائم هي :

أ - الدخول غير المصرح به لنظام الحاسوب (النشاط الرئيسي للعبث أو التطفل)

ب - نفس الفعل السابق، ولكن بقصد ارتكاب أو تسهيل ارتكاب فعل آخر.

ج- التعديل أو التحوير غير المصرح به لنظام الحاسوب بقصد إضعاف أو تعطيل النظام.

وبالرغم من أن الاستجابة البريطانية للتدابير التشريعية الجديدة في حقل تقنية المعلومات، وصفت بأنها متأخرة عن غيرها من الدول الأوروبية، ومتأخرة بالتأكيد عن الاستجابة الأمريكية، إلا أن السنوات الأخيرة وتحديدا الأعوام من 1998 وحتى الآن تشهد تميزا في التجربة البريطانية سواء من حيث محتوى التنظيم او الحلول التشريعية المقررة، ليس في نطاق امن المعلومات فحسب، بل في نطاق حماية البيانات الشخصية والخصوصية وتنظيم حرية البيانات والمعلومات، وفي مختلف الفروع الاخرى لقانون تقنية المعلومات[3].

[1]- يونس عرب ،الاتجاهات التشريعية للجرائم الالكترونية، هيئة تنظيم الاتصالات ،سلطنة عمان ،2-4 ابريل 2006.

[2] - Forgery and Counterfeiting Act, 1981 27th July 1981, An Act to make fresh provision for England ,and Wales, and Northern Ireland, with respect to forgery, and kindred offences; to make fresh provision for Great Britain, and Northern Ireland, with respect to the counterfeiting of notes and coins and kindred offences. c.45 Forgery and Counterfeiting Act ,1981, LONDON, ISBN 0 10 544581 9 . http://www.legislation.gov.uk/

[3] -See :Ian Walden, update on the computer misuse act 1990, Journal of Business Law, 1994, Sep, p.p522-527.

البند الرابع: الدنمارك

سنّت الدنمارك قانونها المتعلق بجرائم الحاسب الآلي والأنترنت [1]، في 06 جوان 1986[2]، والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي أو التزوير أو أي كسب غير مشروع ،سواء للجاني أو لطرف ثالث أو التلاعب غير المشروع ببيانات الحاسب الآلي، كإتلافها أو تغييرها أو الاستفادة منها.

إن التجربة الأوروبية في حقل امن المعلومات، هي التجربة الأكثر نضجاً في العالم، فعلى المستوى الوطني كانت الدول الأوروبية، من أوائل الدول التي تعاملت مع الظاهرة تعاملا واقعيا عبر دراسات معمقة للواقع ولطبيعة المشكلات وللحلول والتدابير الأفضل، فلم تكن تجربة متسرعة لكنها لم تكن أيضا بطيئة من حيث الاستجابات، بل على العكس كانت استجابات مبكرة في حدود متطلبات الواقع، ولان فهم الظاهرة أساسا واخذ التدابير على ضوء هذا الفهم فهو أهم ضمانات النجاح، فان إدراك الدول الأوروبية العالمية لظاهرة جرائم الكمبيوتر وإدراكها أيضا توقف فعالية المكافحة على مستوى انسجام التدابير التشريعية لدى دول العالم بوجه عام[3]، ولدى الدول الأوروبية على نحو خاص، فقد اتجهت الجهود الأوروبية لتوحيد التدابير التشريعية وخطط المكافحة، وشكلت هيئات أوروبا التشريعية والتنفيذية الأداة الفاعلة لتحقيق هذا الانسجام، فكان للأدلة التوجيهية التي وضعها الاتحاد الأوروبي مبكرا منذ الثمانينات الأثر الفاعل في تحقيق الانسجام بين التدابير التشريعية الأوروبية، وعلى مدى خمسة عشر عاما مضت ، جاءت الاتجاهات التشريعية الأوروبية قريبا متماثلة تقريبا أو متقاربة بشأن التعامل مع ظاهرة جرائم الكمبيوتر والانترنت .

---

[1] -See: Ian Walden, Op. Cit. 522-527

[2] -Codification du Code pénal ,Codification n° 886/1992, amendé en dernier lieu par la Loi n° 385 du 20 mai 1992,
http://www.wipo.int/wipolex/fr/details.jsp?id=1115.
Mann, David & Sutton Mike, Net crime, Brit. J. criminal, Vol, 38, No. 2, Spring 1998, pp. 219- 220.

ومع تطور الظاهرة ومع الشعور بان ما أنجز – وهو كثير – لم يعد كافيا بسبب الحاجة إلى مزيد من التوحد، ومزيد من الانسجام، والاهم من ذلك، مؤسسة جهود التعاون بين دول أوروبا في حقل المكافحة، جاءت مبادرة المجلس الأوروبي المتمثل بوضع مشروع اتفاقية عالمية لجرائم الكمبيوتر، ونركز تاليا على معالجة هذه الاتفاقية باعتبارها الرؤية الأوسع والأحدث للإطار القانوني للحماية من جرائم الكمبيوتر في بيئة أوروبية بل والعالم دون إغفال ما سبقها من أنشطة على المستوى الوطني لكل دولة، مكتفين بإيراد نماذج من الجهود الوطنية [1].

الفرع الثاني: التجربة العربية في حقل أمن المعلومات.

إن السؤال الذي يطرح نفسه بحدّة هو: أين نحن كمجتمعات عربية، من هذا التطور العاصف للعلوم والتكنولوجيا؟. من هذا الاتساع الهائل لنطاق المعلوماتية ودورها!

من الواضح أننا لا نزال في موقع المتلقي السلبي لا المنتج، لثمار وإنجازات الثورة العلمية التكنولوجية في كل مراحلها، ولا نزال على مسافة سنوات ضوئية عن مرحلتها الأخيرة المتمثلة بثورة الاتصالات والمعلوماتية (غير أن ذلك لا يجعلنا بمنأى عن آثارها السلبية). – إن مجتمعاتنا لاتزال في بدايات الدخول حقبة (المرحلة الصناعية) بمفهومها المتطور، في حين أن الدول المتطورة أصبحت في قلب ما يسمى (مرحلة ما بعد الصناعة).

وهذا ما يضاعف الهوّة بيننا وبينها, ويزيدها عمقًا واتساعًا، إن ثقافة التغيير والتأقلم مع متطلبات التطور المعرفي لم تصل إلى مجتمعاتنا بعد.

إننا بحاجة ماسّة إلى إعادة النظر في مقاربتنا لمفهوم (المعرفة التكنولوجية و الأمن المعلوماتي)، وفي وعينا لحقيقة أن دخولنا هذا الفلك، هو السبيل الوحيد لنجاحنا في مواجهة تحديات العصر ولاحتلال موقع لائق بين الأمم.

ليس في العالم العربي ما يستحق الوقوف عنده كثيرا، فلا توجد أي دولة عربية قد قامت بسن قوانين جديدة (*NEW LAWS*)، خاصة بها أو حتى تحديث قوانينها الخاصة لتستوعب

[1] – جعفر حسن جاسم الطائي، المرجع السابق، ص ص 231 – 232 ،يونس عرب، نماذج من التشريعات المختلفة في مجال مكافحة الجرائم الالكترونية ،المرجع السابق، متاح على الرابط التالي:

www.arablaw.org , lawoffc@nol.com.

تلك المستجدات الإجرامية، فالدول العربية لا زالت بعيدة كل البعد عن ذلك التطور القانوني الذي يحاول اللحاق بالتطور الإجرامي.

إن البلاد العربية ليس فيها عملية لسن قوانين جديدة، ولا حتى تعديل لتلك القوانين لكي تستوعب الأحداث و المستجدات الجديدة الإجرامية و منها جرائم تكنولوجيا المعلومات، و ان ما نجد فيها هو عملية تطويع للقوانين السابقة و محاولة إدخال الجرائم الالكترونية تحت بعض نصوصها ، ناسين أو متناسين طبيعة هذا النوع من الجرائم ، وكذلك حجم الخسائر المادية و النوعية التي تخلفها، وملابسها أو الغموض الذي يكشف لحظة ارتكاب الجريمة الإلكترونية، وكذلك تناسوا النتائج المترتبة من ارتكاب تلك الجرائم، وبذلك تؤكد الأمة العربية على تمسكها بالتخلف و لا بديل عنه و الدليل على ذلك يؤكد رجال القانون العرب من خلال عدم التعديل في القوانين القديمة، و لا سن قوانين حيث قوانين حديثة تتوافق و معطيات العصر الجديد ، عصر تكنولوجيا المعلومات .

هناك قرار صادر عن مجلس وزراء العدل العرب بجامعة الدول العربية بشأن مشروع قانون عربي استرشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها[1]، يتكون من 27 مادة وضع من خلالها القواعد الأساسية التي يتعين على التشريعات العربية الاستعانة به عند وضع قانون لمكافحة الجرائم الإلكترونية[2]، كما تسعى الدول العربية إلى إنشاء منظمة عربية تهتم بالتنسيق في مجال مكافحة الجرائم الإلكترونية والتشجيع على قيام اتحادات عربية تهتم بالتصدي لتلك الجرائم وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهتها عن طريق نظام الأمن الوقائي[3] .

و قد عقد مؤخرا في مقرّ المركز العربي للبحوث القانونية والقضائية – جامعة الدول العربية الأيام العربية الخامسة لأمن الفضاء السيبراني، وذلك بالتعاون مع المرصد العربي لسلامة

---

[1]– أنظر الملاحق التي ترافق هذه الرسالة .

[2] – اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم 495 - 19 – 2003/10/8 ؛ ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417 –2004/21 .

[3] – كما بدأ الإدراك بأهمية الموضوع، يتزايد في بعض التشريعات العربية مثل التشريع التونسي الذي كان له فضل السبق بين الدول العربية، في سن قانون خاص بالتجارة الإلكترونية ،وهو القانون رقم 83 لسنة 2000 الصادر في أغسطس سنة 2000 في شأن المبادلات والتجارة الالكترونية، حيث تم بموجب الفصل 8 من إنشاء ، كما أصدرت الأردن قانونا رقم 85 /2001 بشأن المعاملات الإلكترونية، ومن هذه القوانين : قانون الإثبات السوداني لعام 1973مادته (37).

الفضاء السيبراني، بتاريخ 2015/12/1 وفي الجلسة الختامية، صدر عن المؤتمر التوصيات التالية[1]:

- الدعوة إلى إنشاء هيئة وطنية لحماية البيانات ذات الطابع الشخصي، والحريّات ومراكز الاستجابة لطوارئ الإنترنت.
- دعوة الدول العربية إلى توقيع الإتفاقية الدولية لمكافحة الجريمة السيبرانية.
- الدعوة إلى إنشاء هيئة وطنية لتطبيق مواصفات شهادات الهوية الرقمية (الإمضاء/التوقيع الرقمي)، ولمنح خدمات التصديق الإلكتروني بما يدعم التوسّع عن تقديم خدمات الحكومة الإلكترونية والتعاملات المالية، من خلال تطبيقات التليفونات المحمولة ومواقع الإنترنت.
- الدعوة إلى وضع الصيغ القانونية للتمكّن من التصدّي للجريمة الإلكترونية، وحماية الفرد من مستخدمي الإنترنت والمعلوماتية.
- دعوة الدول العربية إلى إستكمال تشريعاتها الداعمة للأمن السيبراني، واستكمال المؤسسات، التي تؤمّن تحقيق ذلك كمراكز الإستجابة لطوارئ الإنترنت.
- الدعوة إلى تفعيل الخطوات اللازمة، لإخراج القانون العربي النموذجي لأمن الفضاء السيبراني لتعميمه على الدول العربية.
- دعم البحث العلمي والتدريب وتنمية القوى البشرية المعنية بالأمن السيبراني.
- التعاون الدولي لمواجهة الجرائم الإلكترونية العابرة للحدود عبر الفضاء السيبراني المفتوح.
- الدعوة إلى خلق حدود وقوانين تحمي الطفل من تعرّضه للإساءة عبر الفضاء السيبراني وترفع من مستوى الوعي لديه.
- الدعوة إلى تطوير منظومة الإنترنت البيئية.
- الدعوة إلى تطوير الثقافة المجتمعية ورفع الوعي لدى مختلف المستخدمين.
- وضع آلية للتنسيق والتعاون بين الهياكل العربية المعنية بالأمن السيبراني، تفعيلاً للإتفاقية العربية لمكافحة جرائم تقنية المعلومات وحماية المجتمعات العربية، وضمان أمنها الثقافي والإجتماعي.

[1]- الأيام العربية للأمن السيبراني ،أفق التعاون لحماية الفضاء السيبراني، اليوم الخامس، بيروت 2015/12/01.

- الدعوة إلى تعزيز مفهوم الوعي الشبكي ضمن إستراتيجية متكاملة تجمع مؤسسات الدولة وهيئات المجتمع الدولي والمتخصّصين.

وفي مجال التشريع صدر في الدول العربية التشريعات الآتية :

1.النصوص التشريعية و التنظيمية الجزائرية المتعلقة بتكنولوجيا المعلومات:

- القانون رقم 2000- 03 المؤرخ في 05 أوت 2000 المتعلق بالقواعد العامة بالبريد والمواصلات السلكية واللاسلكية.

- القانون رقم 09-04 المؤرخ في 2009/08/05 الذي تضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها.[1]

- المرسوم تنفيذي رقم 98 – 257 المؤرخ في 03 جمادي الأول الموافق 25 أوت 1998 الذي يضبط شروط وكيفيات إقامة خدمات "أنترنات" واستغلالها. (الجريدة الرسمية عدد 63 بتاريخ 26 أوت 1998)

- المرسوم تنفيذي رقم 09 – 410 المؤرخ في 10 ديسمبر 2009 الذي يحدد قواعد الأمن المطبقة على النشاطات المتصلة بالتجهيزات الحساسة.

- القانون رقم 05 -10 المؤرخ في 20 جوان 2005 المعدل والمتمم للأمر رقم 75 – 58 المتضمن القانون المدني.- الإعتراف بالكتابة الإلكترونية كوسيلة إثبات في المادة 323 مكرر 1:" يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، شرط إمكانية التأكد من هوية الشخص الذي أصدرها، وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها". [2]

- الأمر رقم 75- 58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني المعدل والمتمم، يكرس الأساس القانوني للتوقيع الإلكتروني في مواده من 323 مكرر إلى 327 من

[1]- قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430، الموافق 05 /08 /2009،ج.ر.ر رقم 47.

[2]- الجريدة الرسمية عدد 44 بتاريخ 20 جوان 2005 .

الأمر رقم 75 – 58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني المعدل والمتمم (الجزء المتعلق بطرق الإثبات)

- الأمر رقم 75 – 59 المتضمن القانون التجاري المعدل والمتمم، يعترف في المادتين 414 و502(القسم المتعلق بالأوراق التجارية) بالتعامل بأية وسيلة تبادل إلكترونية بالنسبة لحامل رسالة الصرف (السفتجة) أو التقديم المادي للشيك .
- الأمر رقم 66 - 155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية، المعدل والمتمم بالقانون رقم 15-04المؤرخ في 10 نوفمبر 2004.[1]
- المرسوم التنفيذي رقم 01 – 123 المؤرخ في 09 ماي 2001 المعدل والمتمم، يعطي صلاحيات لسلطة ضبط البريد والمواصلات السلكية اللاسلكية، بمنح الرخصة المتعلقة بإنشاء واستغلال خدمات التصديق الإلكتروني مرفقا بدفتر الشروط .
- المرسوم التنفيذي رقم 07 – 162 المؤرخ في 30 ماي 2007 المعدل والمتمم للمرسوم التنفيذي رقم 01- 123 المؤرخ في 09 ماي 2001 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات، بما فيها اللاسلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية و واللاسلكية، أخضع خدمات التصديق الإلكتروني لنظام الرخصة[2] .
- القانون رقم 05 -02 المؤرخ في 16 فيفري 2005 المعدل و المتمم للأمر رقم 75 – 59 المؤرخ في 26 سبتمبر 1975 المتضمن القانون التجاري، يدرج هذا القانون في مادتيه 414 و 502 التبادل الإلكتروني في التعاملات التجارية .
- القانون رقم 04 – 14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66 – 155 المتضمن قانون الإجراءات الجزائية[3] ، تنشأ لدى وزارة العدل مصلحة لنظام آلي وطني لصحيفة السوابق القضائية مرتبطة بالجهات القضائية .

---

[1]- قانون رقم 04-15 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966والمتضمن قانون العقوبات، ج.ر.ر71.

[2]- صدر هذا القانون بتاريخ 07 جوان 2007،ج.ر.ر 37.

[3]- صدر هذا القانون بتاريخ 10 نوفمبر 2004.ج.ر.ر. 71 .

- القانون رقم 08 – 04 المؤرخ في 23 جانفي 2008 المتضمن القانون التوجيهي للتربية، يشير هذا القانون في مادتيه 02 و 04 إلى التكوين واكتساب المعارف في مجال تكنولوجيا الإعلام والاتصال وإدماجه في المحيط التربوي و مجتمع المعرفة[1].
- القانون رقم 15 - 04 المؤرخ في 01 فيفري 2015 المتضمن تحديد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية العدد 06 بتاريخ 10فيفري 2015[2].

2. وفي تونس قانون رقم 83 / 2000 بشان المبادلات والتجارة الالكترونية3.
3. وفي المملكة الأردنية الهاشمية قانون رقم 85 / 2001 بشان قانون ألمعاملات الإلكترونية (قانون مؤقت) إلا أنه أصبح نهائيا بقانون جرائم أنظمة المعلومات 2010 [4].
4. وفي دبي قانون رقم 2 / 2002م بشان المعاملات والتجارة الالكترونية[5] .
5. وفي البحرين مرسوم بقانون رقم 28 لسنة 2002[6] م بشان المعاملات الالكترونية المعدل بالقانون رقم 13 / 2006 [7].
6. وكذلك في مصر قانون رقم 15 / 2004 بشان المعاملات الإلكترونية [8]، مشروع مكافحة الجرائم المعلوماتية المصري و كم كان حرص المشرع المصري عظيمًا في مواكبة النهضة التكنولوجية والمعلوماتية التي يعيشها العصر، فأصدر قانون خاص للاتصالات [9](رقم10

---

[1]- صدر هذا القانون بتاريخ 27 جانفي 2008، ج.ر.ر 04 .

[2]- صدر هذا القانون في 20 ربيع الثاني 1436، الموافق ل 10فبراير 2015، العدد 06

[3]- قانون رقم 83 / 2000 صدر بتاريخ 2000/08/09، الرائد الرسمي للجمهورية التونسية، عدد64.

[4]- قانون رقم 85- 2001 ، بتاريخ 31-12-2001.،ج.ر. رقم 4534 ،

[5]- صدر بتاريخ 30ذي القعدة 1422هج،الموافق ل 12فبراير2002م.

[6]- صدر بتاريخ8رجب1423هـ ،الموافق 14سبتمبر2002 ،ج.ر.ر2547.

[7]- صدر بتاريخ 1 جمادى الأولى 1427هـ ،الموافق 28 مايو 2006م ،ج.ر.ر2741.

[8]- قانون رقم 15 / 2004 صدر في ربيع الأول سنة 1425 هـ ،الموافق 21 ابريل سنة 2004 م،و كذلك المرسوم رقم 109 لسنة 2005 بشأن الأمر التوجيهي لإنفاذ القانون رقم 109 لسنة 2005 بشأن التوقيعات الالكترونية وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

[9]- وعُرِّف الاتصالات في هذا القانون في (م1/ف3) بأنها: (أية وسيلة لإرسال أو استقبال الرموز، أو الإشارات، أو الرسائل، أو الكتابات أو

/2003م) لتأمين نقل وتبادل المعلومات، وقانون آخر للتوقيع الإلكتروني (رقم 2004/15م) لتأمين معاملات الأفراد عبر شبكة المعلومات الدولية "الإنترنت"، فضلاً عن أنّ هناك جهودًا تبذل لإصدار قانون خاص بالمعاملات الإلكترونية لسلامة وتأمين المعاملات المختلفة من كافة جوانبها القانونية والجنائية، وهناك دراسات جادة لإعداد مشروع قانون لمكافحة الجريمة المعلوماتية.

7. وفي دولة الإمارات العربية المتحدة، قانون رقم 2 / 2006 بشان مكافحة جرائم تقنية المعلومات[1].

8. وفي اليمن قانون رقم 40 / 2006 بشان أنظمة الدفع والعمليات المالية والمصرفية الالكترونية.[2]

9. وفي المغرب ظهير شريف رقم 129 – 07 – 1 صادر في 19 من ذي القعدة 1428 ،30 نوفمبر 2007 بتنفيذ القانون رقم 05 /53 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، الجريدة الرسمية رقم 5584 الصادرة يوم الخميس 6 ديسمر 2007.

10. وفي قطر مرسوم بقانون رقم 16 لسنة 2010 إصدار قانون المعاملات والتجارة الالكترونية[3].

11. نظام مكافحة الجرائم المعلوماتية السعودي (2007م): سَنَّت المملكة العربية السعودية نظام مكافحة الجرائم المعلوماتية، الذي أقرّه مجلس الوزراء الموقر برئاسة خادم الحرمين الشريفين الملك عبد الله بن عبد العزيز نظام مكافحة جرائم المعلوماتية، الصادر بالمرسوم الملكي رقم م/ 17 وتاريخ: 8/3/ 1428 هـ بناءً على قرار مجلس الوزراء رقم: (79) وتاريخ: 7/3/ 1428ه ـالذي يهدف إلى الحد من نشوء الجرائم المعلوماتية، وذلك بتحديد تلك الجرائم والعقوبات المقرَّرة لها.[4]

الصور، أو الأصوات، وذلك أياً كانت طبيعتها، وسواء كان الاتصال سلكياً أو لاسلكيًّا).

1- قانون رقم 2 / 2006 صدر بتاريخ 30 ذي الحجة 1426هـ ،الموافق 30 يناير 2006، العدد رقم 442 من الجريدة الرسمية .

2- قانون رقم 40 / 2006 صدر بتاريخ 8ذو الحجة1427هجرية ،الموافق ل 28 ديسمبر 2006م.

3- مرسوم2010/16،صدر بتارخ20-10-1431الموافق ل 28-09-2010،ج.ر .رقم 9.

4- وجاء في المادة الثانية من هذا النظام: (يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي إلى ما يأتي:

1 – المساعدة على تحقيق الأمن المعلوماتي.

البند الأول: جهود سلطنة عمان في مواجهة الجرائم المتعلقة بشبكة الإنترنت

محاولات المشرع العماني [1] في التصدي للجرائم المتعلقة بشبكة الإنترنت، [2] جاءت من خلال قانون المعاملات الإلكترونية، حيث جرم المشرع في المادتين (52، 53) من قانون المعاملات الإلكترونية 2008/69م بعض الأنماط السلوكية التي من شأنها هز ثقة الجمهور بالتعاملات التي تتم في العالم الرقمي، ومن أهم هذه الجرائم :

الفئة الأولي: الإتلاف المعلوماتي.

تقع هذه الجريمة بالاعتداء على الوظائف الطبيعية للحاسب الآلي وذلك بالتعدي على البرامج *LOGICAL* والبيانات *DATA* المخزنة والمتبادلة بين الحواسب والشبكات الداخلية أو العالمية ويكون ذلك عن طريق التلاعب بالبيانات، سواء بإدخال معلومات مصطنعة أو إتلاف معلومات مخزنة بالحواسب، والمتبادلة عبر الشبكة العالمية *GLOBAL NET* بمحوها أو تعديلها أو تغير نتائجها أو بطريقة التشويش على النظام المعلوماتي، مما يؤدي إلى سير عمل النظام الآلي بصوره المختلفة ويكون هذا الإتلاف العمدي للبرامج والبيانات ومحوها أو تدميرها إلكترونيا بصفة كاملة، وتأخذ جريمة الإتلاف في نطاق المعلوماتية، إما صورة الإتلاف المادي وهذا بالاعتداء على المكونات المادية للحاسب *HARD WARE* أو صورة الاعتداء على البرامج أو البيانات *SOFT WARE* والمعلومات المخزنة في قواعد الحواسب.

ويرى البعض أن الإتلاف الواقع على المكونات المادية للحاسب الآلي يخرج عن إطار

---

2 – حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

3 – حماية المصلحة العامة، والأخلاق، والآداب العامة.

4 – حماية الاقتصاد الوطني).

[1]– شهاب بن أحمد الجابري ،الإطار العام لقانون المعاملات الإلكترونية 2008/69م ، ندوة قانون المعاملات الإلكترونية الأولي ، صلالة أغسطس ،2008،

[2]– دخلت خدمة الإنترنت إلى سلطنة عمان في عام 1997م وبنهاية الربع الثالث من 2010 كان عدد المشتركين في خدمة الإنترنت الثابت 68,201 مشترك ، في حين بلغ عدد مشتركي خدمة الانترنت المتنقل في ذات الفترة 1,626,896 مشترك ، وبلغ عدد مقاهي الإنترنت التي تم تسجيلها في عام 2009 م 315 مقهى ، وكان من الطبيعي حيال هذا التزايد المستمر في عدد المشتركين في هذه الشبكة، والمستخدمين لها أن تحاول السلطنة جاهدة مواجهة الاستعمالات السيئة لشبكة الإنترنت، وما ينجم عنها من أضرار سواء بالنسبة للمجتمع أو الأفراد.لمزيد من التفاصيل: التقرير السنوي لهيئة تنظيم الاتصالات 2009 ص 4.46 ,P Telcom ,Sector Indicators Rebort Q2010 .

الجريمة المعلوماتية، على اعتبار أن هذه الأخيرة تتصل بالأفعال التي تشكل اعتداء على المعلومات المبرمجة ونظم معالجتها، باستخدام طرق ووسائل خاصة .

وبالتالي فلا حاجة إلى إفراد نصوص خاصة لإتلاف المكونات المادية للحاسب الآلي، حيث أنه في الإمكان تطبيق النصوص التقليدية عليها[1].

ومع ذلك تناولت بعض التشريعات إتلاف المكونات المادية للحاسب الآلي في نصوص خاصة، ترتبط بالجريمة المعلوماتية منها على سبيل المثال المادة 502 من قانون العقوبات الخاص بولاية كاليفورنيا الأمريكية، التي تجرّم إتلاف وتخريب أنظمة المعالجة الآلية للمعلومات بمكوناتها المادية والمعنوية[2] ،وأيضا المادة 374 من قانون العقوبات القطري 2004/11 التي نصت على معاقبة كل من يتلف أو يخرب عمدا وحدات الإدخال أو الإخراج أو شاشة الحاسب الآلي مملوك للغير، أو الآلات أو الأدوات المكونة له، بالحبس مدة لا تجاوز ثلاث سنوات وبالغرامة التي لا تزيد عن العشرة آلاف ريال قطري.

وقد يقع الإتلاف على المكونات أو الكيانات المنطقية – المعنوية – للحاسب الآلي والتي يقصد بها كل العناصر غير المادية، التي يتكون منها نظام الحاسب الآلي كالمعلومات والبيانات والبرامج على اختلاف أنواعها ووظائفها .

وهنا يتبادر التساؤل حول مدى صلاحية هذه المكونات كمحل لجريمة الإتلاف بالصورة الكلاسيكية المعروفة، عندما لا يترتب على المساس بها إتلاف أي من العناصر المادية، التي يتكون منها نظام المعالجة الآلية للحاسب الآلي، وبالتالي تطبيق النصوص التقليدية الخاصة بها على إتلاف هذه المكونات المنطقية.

وللخروج من دائرة الخلاف والنقاش وللنأي عن اللجوء إلى القياس الذي يتعارض مع مبدأ الشرعية، أوجد المشرّع العماني حلا تشريعيا لذلك، حيث جرّم إتلاف المكونات المنطقية لأنظمة الحاسب الآلي، بنص مستحدث خاص بها وهو نص البند الأول من المادة 52 من قانون

[1] -Waslk Martin, crime and computer ,Oxford University ,press 1991, p136 , Vergucht (Pascal), op. cit, p .123.

[2] -Conley (Jonhn M) & Bryan (Robert M) , A survey of computer crime legislation in United States , I.C.T.L , Vol .8.1, 1999, P41 .

المعاملات الإلكترونية[1] حيث نص على "مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون الجزاء العماني أو أي قانون آخر، يعاقب بالسجن لمدة لا تتجاوز سنتين و بغرامة لا تتجاوز 5000 ر.ع (خمسة آلاف ريال عماني) أو بإحدى هاتين العقوبتين كل من : "تسبب عمداً في تعديل غير مرخص به في محتويات أي حاسب آلي، بقصد إضعاف فاعليته أو منع أو تعويق الدخول إلى أي برنامج أو بيانات محفوظة فيه، أو إضعاف فاعلية ذلك البرنامج أو إضعاف الاعتماد على تلك البيانات إذا تم ذلك التعديل بإحدى الطرق الآتية:

1. شطب أي برنامج أو بيانات محفوظة في الحاسب الآلي.
2. إضافة أي برنامج أو بيانات إلى محتويات الحاسب الآلي.
3. أي فعل يسهم في إحداث ذلك التعديل.

ويتضح لنا من خلال النص السابق أن السلوك الإجرامي يتحقق بالإتلاف ويعني بها إفناء هذه المعلومات وإهلاكها كليا أو جزئيا، أو بالإضافة ويعني بها إضافة كلية أو جزئية للمحتويات الموجودة في الحاسب الآلي، وهاتين الصورتين وردتا على سبيل المثال وليس الحصر بدليل أن المشرع أورد في نهاية البند عبارة (أي فعل يسهم في إحداث ذلك التعديل)،هذا من ناحية ومن ناحية أخرى نجد أن المشرّع العماني وهو يجرم هذه الجريمة لم يحدد الجهة التي تتبع لها البيانات، فهو لم يضع شروطا تتعلق بطبيعة البيانات و المعلومات محل الإتلاف، و لم يشترط تبعيتها لجهة معينة، وإنما جاء النص عاما ليشمل كافة أنواع المعلومات والبيانات سواء أكانت تابعة لجهة حكومية أو خاصة.

ومن ناحية ثالثة لم يحدد وسائل معينة تتم بها عملية الإتلاف المعلوماتي، مما يعني أن النص يتسع ليشمل كافة الطرق الفنية والتقنية المستخدمة في إتلاف المعلومات، بما في ذلك استخدام البرامج الخبيثة كالفيروسات والقنابل المعلوماتية وبرامج الدودة وغيرها، ومن ناحية رابعة نجد أن الجريمة تقوم بمجرد القيام بأحد الأفعال الإجرامية، كما وأن العقاب على إتلاف المعلومات لم يرتبط بالدخول غير المصرح به إلى نظام الحاسب الآلي.

ومن حيث العقوبة نجد أن المشرّع قرر لهذه الجريمة نوعين من العقوبة سالبة للحرية وهي

[1]- موسى مسعود أرحومة، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، دار النهضة العربية، ص 335.

الحبس بحد أقصى سنتين، ومالية تتمثل في الغرامة بحد أقصى 5000ريال، والأصل العام هو أن يتم الحكم بالعقوبتين معا والاستثناء هو الحكم بإحداهن.

الفئة الثانية: الإختراق المعلوماتي

إختراق أنظمة الحاسبات الآلية أو مواقع الانترنت، يعد من أخطر الجرائم التي تهدد المعلوماتية، سيما وأن العديد من تلك الأنظمة تمتلكها الحكومات، وتحوي بطيها العديد من الملفات والمعلومات ذات أهمية قصوى، ليس بالنسبة للدولة صاحبة النظام وإنما بالنسبة للأفراد أيضا مما يشكل اعتداء على خصوصية الفرد.[1]

من هذا المنطلق نجد أن المشرع العماني كان حريصا على تجريم هذه الفئة المستحدثة، من الجرائم بنصوص خاصة أوردها في المادة 52 من قانون المعاملات الالكترونية[2]

الفئة الثالثة : الاعتداء على معلومات أو بيانات مشفرة :

تشفير [3]المعلومات أو البيانات، دليل على أنها ذات طابع خاص يقتضي الأمر أن تكون سرية، لا ينبغي الاطلاع عليها من قبل أي شخص غير معني أو غير مختص .

من هذا المنطلق نجد المشرع كان حريصا على توفير الحماية الجنائية لهذه النوعية من البيانات، حيث جرم من خلال المادة 52 مجموعة الأفعال التي تشكل اعتداء على معلومات أو بيانات مشفرة، وفرض عقوبتين الأولي سالبة للحرية، تتمثل في السجن بحد أقصى سنتين والثانية غرامة مالية بحد أقصى 5000 ريال عماني أو بإحداهن، وهذه الأفعال هي :

1. كشف مفاتيح لفض التشفير أو فض تشفير معلومات[4] .

---

[1]- موسى مسعود أرحومة ،المرجع السابق، ص 336 و ما بعدها .

[2]- المشرع العماني أيضا جرم الاختراق المعلوماتي، بنص آخر وهو نص البند الثاني من المادة 276مكرر من قانون الجزاء العماني، حيث نص على " يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين وبغرامة من مائة ريال إلى خمسمائة ريال ،أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسب الآلي في ارتكاب إحدى الأفعال التالية :..... الدخول غير المشروع على أنظمة الحاسب الآلي ".

[3]- يقصد بالتشفير :عملية تحويل نص بسيط أو وثيقة نصية أو رسالة الكترونية، إلى رموز غير معروفة أو مبعثرة يستحيل قراءتها أو معرفتها بدون إعادتها إلى هيئتها الأصلية، المادة الأولى من قانون المعاملات الإلكترونية 2008/69م

[4]- نص المشرع في البند الرابع من المادة 52 هذا السلوك الإجرامي حيث نص على " ... قام بطريقة غير مشروعة بكشف مفاتيح لفض التشفير أو فض تشفير معلومات مودعة لديه.

2. الاستعمال غير المشروع لعناصر تشفير شخصية: جرم هذا الفعل في البند الخامس من ذات المادة حيث نص على " ... استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بتوقيع غيره"، وهو خاص بعناصر التشفير المتعلقة بالتواقيع الإلكترونية، والصورة الجرمية لهذا الفعل تتمثل في أن قيام استعمال عناصر تشفير تتعلق بتوقيع الكتروني، يخص أحد الأشخاص دون وجه حق من قبل الجاني.

3. اختراق أو اعتراض أو فض بيانات مشفرة [1]:

4. فض بيانات أو معلومات مشفرة في غير الأحوال المصرح بها [2]:

الفئة الرابعة : التزوير الإلكتروني[3]:

التزوير[4] هو تزيين الكذب وتحسينه بطريقة تكون اقرب إلى قبول السامع[5] وهو تحسين الشيء ووصفة بخلاف صفته، حتى يخيل إلى من سمعه أو رآه خلاف ما هو به على الحقيقة،

---

[1]– جرم هذا الفعل في البند السادس من المادة 52 حيث نص على"...اخترق أو اعترض معلومات أو بيانات مشفرة أو قام بفض شفرتها عمداً دون مسوغ قانوني، وتضاعف العقوبة إذا كانت المعلومات أو البيانات تتعلق بسر من أسرار الدولة."

[2]– جرم هذا الفعل في البند السابع من ذات المادة حيث نص على "... قام عمداً بفض معلومات أو بيانات مشفرة بأية طريقة، في غير الأحوال المصرح بها قانوناً." والمشرع في هذا السلوك لم يشترط تبعية المعلومات أو البيانات المشفرة لجهة معينة، أو تخص الدولة وإنما ترك المجال مفتوحا، ليشمل كافة البيانات أو المعلومات بشرط أن تكون مشفرة ، أيضا المشرع اشترط لقيام الجريمة أن يتم الفض دون وجه حق بمعني أن يتم في غير الأحوال المصرح بها.

[3]– عامر محمود الكسواني، التزوير المعلوماتي للعلامة التجارية، دار الثقافة للنشر و التوزيع، عمان،2014 ،ص 133.

[4]– التزوير هو كذب يقع في محرر ، فلا يمكن تصوره إلا بتغيير الحقيقة، فان لم يكن هناك تغيير للحقيقة فلا يمكن القول بوجود جريمة التزوير، لمطابقة هذه المعلومات للحقيقة ،ولو كان من شأن هذه البيانات إصابة الغير بضرر فإذا قام شخص بتدوين معلومات في وثيقة على إنها معلومات مزورة، فإذا هي معلومات حقيقية فلا تقوم جريمة التزوير.

- ✓ لا يشترط أن تكون جميع البيانات مغايرة للحقيقة بل يكفي بعضها .
- ✓ يشترط أن يكون تغيير الحقيقة متقنا بحيث لا يمكن اكتشافه بل يستوي أن يكون واضحا
- ✓ لا يشترط أن يكون تغيير الحقيقة متقنا بحيث لا يمكن اكتشافه
- ✓ إعدام ذاتية المحرر لا يعتبر تزوير كإتلافه أو شطب محتوياته أو وضع مادة عليها
- ✓ يعتبر تزوير إذا حصل التغيير في المحرر بعلم أو تفويض من صاحب المحرر كما لو قيام شخص بكتابة محرر وإمضائه بطلب من صاحب الشأن أو تفويض منه.
- ✓ لا يعتبر تزوير إذا حصل التغيير في حدود حقه ولذلك لا عقاب على الصورية مادام يتصرف في حدود حقه انظر ، جمال إبراهيم الحيدري، شرح أحكام القسم الخاص من قانون العقوبات، ج 1،مطبعة الفائق : بغداد ،1998،ص48.

[5]– أحمد بن محمد بن علي الفيومي، المقرئ المصباح المنير في غريب الشرح الكبير، مكتبة لبنان، 1987 ،ص 99 ، وبن يعقوب الفيروز آبادي مجد الدين، القاموس المحيط، مؤسسة الرسالة ،2005 ، الطبعة 8، ص 515.

فهو تمويه الباطل بما يوهم أنه حق[1].

والتزوير الإلكتروني هو تغيير الحقيقة في المستند الإلكتروني، بإحدى طرائق التغيير ويترتب عليه ضرر على الغير.[2]

والتزوير في المجال المعلوماتي يعتبر من أخطر صور الغش وأكثرها ضررا، من هذا المنطلق حرص المشرع العماني على تجريم التزوير الالكتروني، بنص خاص هو نص البند 14 من المادة 52 من قانون المعاملات الإلكترونية حيث نص على " مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون الجزاء العماني أو أي قانون آخر ،يعاقب بالسجن لمدة لا تتجاوز سنتين و بغرامة لا تتجاوز 5000 رع (خمسة آلاف ريال عماني) أو بإحدى هاتين العقوبتين كل من زور سجلاً إلكترونياً أو توقيعاً إلكترونياً أو استعمل أيا من ذلك مع علمه بتزويره "".

والتزوير المجرم بالنص السابق هو التجريم الواقع على المحررات أو السجلات الالكترونية[3] أو على التواقيع الالكترونية[4].

هذا من جهة ومن جهة أخرى، التجريم لم يقتصر على فعل التزوير، وإنما امتد ليشمل استعمال المحرر المزور، وهنا يشترط أن يكون الجاني عالما بأنه يستعمل محرر مزورا.

الفئة الخامسة : الاعتداء على التواقيع الإلكترونية :

التوقيع الإلكتروني يعتبر هو حجر الأساس في إنجاز أية معاملة إلكترونية، وبالتالي كان لزاما توفير الحماية الجنائية له وهذا هو بالفعل ما قام به المشرع العماني من خلال قانون المعاملات الإلكترونية، الصادر بالمرسوم السلطاني 2008/69م حيث جرم العديد من الأفعال

---

[1]- أبو زكريا محيي الدين يحيى بن شرف النووي ، المنهاج شرح صحيح مسلم بن الحجاج، دار إحياء التراث العربي ،ابنان،ط2 ،443/2 .

[2]- عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية، دار الوراق ودار النيربين للطباعة والنشر والتوزيع ، الرياض، 2005 ،ص 375 .

[3]- عرفت المادة الأولى من قانون المعاملات الإلكترونية 2008/69م السجل الإلكتروني بأنه " العقد أو القيد أو رسالة المعلومات التي يتم إنشاؤها أو تخزينها، أو استخراجها أو نسخها أو إرسالها، أو إبلاغها أو تسلمها بوسائل إلكترونية على وسيط ملموس أو أي وسيط آخر و يكون قابلا للتسلم بشكل يمكن فهمه "

[4]- عرفت المادة الأولى من قانون المعاملات الإلكترونية 2008/69م التوقيع الإلكتروني بأنه " التوقيع على رسالة أو معاملة إلكترونية، في شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع متفرد، يسمح بتحديد شخص الموقع وتمييزه عن غيره.

قانون مكافحة جرائم تقنية المعلومات 2011/12 أتت فكرة القانون من منطلق رغبة المشرع العماني، في سد النقص التشريعي في هذا المجال، وكون النصوص الواردة في سلسلة التشريعات السالف ذكرها، لم تعد كافية لمواجهة هذه النوعية من الجرائم.

تم البدء في صياغة هذا القانون في الربع الأخير من 2008 و الانتهاء من إعداد المسودة الأولى منه في الربع الثالث من 2009 وإحالته إلى الجهات المختصة لإبداء ملاحظاتها عليه، وصدر في الربع الأول من عام 2011 بموجب المرسوم السلطاني 2011/12 .

البند الثاني: المعالجة القانونية للجريمة المعلوماتية في التشريع المغربي: [1]

إختلف بدوره المشرع المغربي حول إمكانية أو عدم إمكانية معاقبة الجرائم المعلوماتية وفقا لنصوص القانون الجنائي التقليدية، فذهب اتجاه إلى انه بالإمكان معالجة الجرائم المعلوماتية، طبقا للنصوص التقليدية في القانون الجنائي المغربي، عن طريق اتخاذ تأويل واسع للجرائم التقليدية ضد الأموال، مع أخذ الحيطة تجنبا للاصطدام مع مبدأ شرعية التجريم، وبذلك فانه يتعين على القضاء أن يكون على معرفة بتأويل النصوص القانونية، وبدون ذلك ستكون هناك مخاطرة بان تبقى تلك الجرائم خارج نطاق القانون الجنائي[2] .

اما الاتجاه الثاني يرى عدم كفاية نصوص القانون الجنائي، و انه من الصعب تطبيق القواعد العامة التقليدية في القانون الجنائي على سائر مظاهر المعلوماتية، فالجرائم ضد الاموال

---

[1] – نجد أول قضية ذات علاقة بالإجرام المعلوماتي، سنة 1985 بشأن تسهيل مستخدمي المكتب الوطني للبريد والمواصلات، لتحويلات هاتفية لفائدة بعض المشتركين بصورة غير مشروعة، ولقد توبع المتهمون بمقتضى الفصول 202و241و248و251و129 من مجموعة القانون الجنائي المغربي، وقد تمت الإدانة في المرحلة الابتدائية على أساس الفصل 521 المتعلق بالاختلاس العمدي لقوى كهربائية، في حين تمت تبرئتهم في مرحلة الاستئناف. "حكم ابتدائية البيضاء بانفا رقم4236-4 الصادر بتاريخ13-11-1985 ،ملف جنحي تلبسي عدد 85-7383 "

كما أدانت نفس المحكمة في قضية أخرى حائزا لبطاقة الائتمان والأداء استعملها بصورة تعسفية، وذلك استنادا للفصلين540و574 من مجموعة القانون الجنائي المتعلقين بالنصب وخيانة الأمانة، حيث تمت إدانتهم بثلاثة سنوات حبسا، لكن القضاء ألاستئنافي برا ساحة المتهم بحجة أن العناصر المكونة لهذه الجرائم لا تتوفر في النازلة المعروضة. *حكم ابتدائية البيضاء آنفا، رقم167-1 صادر في 5-1-1990 ملف جنحي تلبسي عدد 14209-89.

[2] -M. elmernissi, Rapport introductive, revue marocaine de droit et d économie de développement , n 11-1986.p 19.

يقصد بها حماية الاموال المادية في حين ان البرامج و المعلوماتية بطبيعتها غير مادية[1] ، فرغم قيمتها الاقتصادية الا انه انه لا يمكن مقارنتها بالأموال المادية مما يستدعي ايجاد نصوص خاصة، لاحتواء الجرائم الواقعة عليها لسد هذا الفراغ التشريعي[2].

وكان يجب الانتظار حتى أواخر سنة 2003 ليضع المشرع المغربي حدا لهذا الخلاف الفقهي، من خلال تدخله بمقتضى القانون رقم 03-07[3] ، مضيفا إلى القانون الجنائي المواد من 3/607 إلى 11/607 و معاقبا على الجرائم الحاسب الآلي تحت عنوان المس بنظم المعالجة الآلية للمعطيات، لكن ما المقصود بنظم المعالجة الآلية للمعطيات ؟

ان هذا التغيير نظم المعالجة الآلية المعلوماتية، يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، كما انه تعبير متطور يخضع للتطورات السريعة و المتلاحقة في مجال الحاسبات الآلية، لذلك فقد أحسن المشرع المغربي صنعا بعدم تحديد المقصود بها بما ان التعريفات تبقى دائما مسالة من اختصاص الفقه و القضاء .

إلا انه يمكننا في هذا الصدد الاستئناس بالتعريف الذي وضعه مجلس الشيوخ الفرنسي، أثناء الأعمال التحضيرية لمشروع قانون الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات، حيث عرف هذا الأخير على انه " كل مركب يتكون من وحدة أو مجموعة وحدات معالجة و التي يتكون كل منها من الذاكرة و البرامج و المعطيات و أجهزة الإدخال و الإخراج، و أجهزة الربط و التي يربط بينها مجموعة من العلاقات و التي عن طريقتها يتم تحقيق نتيجة معينة و هي معالجة المعطيات [4].

---

[1] - Ali makouar. m.droit et informatique, rapport de synthèses , revue marocaine de droit et d économie de développement-n 11.1986.p186.

[2]- تضاربت أحكام القضاء المغربي، في الموضوع بين إمكانية الاعتماد على قواعد القانون الجنائي، في تجريم الجرائم المعلوماتية من عدم إمكانية الاعتماد عليها .

[3]- - قانون الجرائم الواقعة على نظم المعالجة الآلية للمعطيات، الصادرة بتنفيذه الظهير رقم 197-03-01- بتاريخ 11نوفمبر 2003،ج رسمية5171، ص 4284.

[4]- علي عبد القادر قهوجي، مرجع سابق ، ص 593.

و قد تضمن القانون 03-07 مجموعة من النصوص تجرم الدخول غير المصرح به إلى نظام معالجة الية المعطيات، بالإضافة إلى تجريم المس بنظم المعالجة الآلية للمعطيات، لكن بمقارنة بسيطة بين كل من التشريعين المغربي و الفرنسي يلاحظ وجود بعض الفوارق بينهما و تتمثل في:

- نص المشرع المغربي على جريمة تزوير الوثائق المعلوماتية في الفصل 7/607 اذا كان من شان هذا التزوير الحاق ضرر بالغير، اما المشرع الفرنسي فبعدما كان ينص على هذه الجريمة في المادتين 5/462 و 462 /6 من قانون الغش في المعلوماتية سنة 1988 قرر عند صدور القانون الجنائي الجديد لعام 1992 الغاء المادتين السابقتين و اضافة هذه الجريمة الى تزوير المحررات العادية، بتعديل المادة 441 من القانون الجنائي .

- و من خلال التعرض لموقف المشرعين يمكن القول إن موقف المشرع الفرنسي أجد بالتأييد على أساس إن تجريم كل من الفعلين التزوير و المساس بنظم المعالجة الآلية للمعطيات يقوم على حماية مصلحة مختلفة، فالمصلحة من تجريم المس بالمعطيات المعالجة أليا فهو حماية تلك المعطيات نفسها.

- بالإضافة إلى ذلك فانه بالرجوع إلى المادة 7/607 من ق.ج نجد أنها تنص على انه "دون الإخلال...يعاقب كل من زور أو زيف وثائق المعلومات أيّا كان شكلها من شان التزوير أو التزييف إلحاق الضرر بالغير..."، فانه من الواضح هنا أن المشرع المغربي عندما اعتبر أن تزوير وثائق المعلومات أي كان شكلها يمكن أن يلحق الضرر بالغير، أضفى و لو بشكل ضمني على تلك المحررات قوة ثبوتية، لان التزوير لكي يعتبر جريمة يجب أن يقع على محررات لها قوة الإثبات، و لا يمكن تصور إن الوثيقة أو المحرر يمكن أن تلحق ضررا بالغير إلا إذا كانت لها حجية في الإثبات، مما يجعلنا نتساءل عن مدى توافق هذه المادة مع ما هو منصوص عليه في القانون المدني ؟ ذلك لان المشرع الفرنسي منذ عام 1980 أعطى للوثائق الصادرة عن الحاسوب و المعالجة الكترونيا حجية في الإثبات ثم قام بتجريم تزويرها، أما المشرع المغربي فقد نص على تلك الجريمة دون أن يحدد النطاق الذي تكون فيه تلك المحررات حجة في الإثبات[1].

[1] – محمود محمد أبو فروة، الخدمات البنكية الالكترونية عبر الانترنت، دار الثقافة للنشر و التوزيع،ط1 ،2009، ص 82.

- و على العموم فان الحماية القانونية لأمن المعلومات وحدها غير كافية، على اعتبار أن طبيعة الانترنت كشبكة مفتوحة عالميا، تجعل معرفة مرتكب الجريمة المعلوماتية أمرا من الصعوبة بمكان، لذلك لا بد من الاستعانة بالوسائل الوقائية الكفيلة بحماية امن تلك المعلومات و التي تتمثل في الوسائل التقنية للحماية.

- هذا و قد أصبحت البيانات الشخصية المعالجة الكترونيا ذات أهمية على المستوى الدولي، وهذا ما جعل الأمم المتحدة تتبنى عام 1989 دليلا يتعلق باستخدام الحوسبة في عملية تدفق البيانات الشخصية، وبتاريخ 1990/12/14, تبنت الهيئة العامة دليل تنظيم استخدام المعالجة الآلية للبيانات الشخصية[1].

- سار المشرع المغربي مع التوجه التشريعي، في العديد من الدول التي تهدف تحقيق حماية فعالة للبيانات الشخصية إلى إصدار :

أولا :القانون المغربي. رقم 08-09المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي الصادر بتاريخ 18 فبراير2009[2]

- يتضمن هذا التشريع 51 مادة موزعة على ثمانية أبواب. وتبدو أهمية هذا القانون في كونه سيساهم في تقوية ثقة المستهلك المغربي في المعاملات الالكترونية والاستفادة من مزايا التجارة الالكترونية، وسيشكل هذا التشريع كذلك أداة هامة [3].

- وما يهم ضمن القانون المغربي رقم 08-09 هو الباب السابع الخاص بالعقوبات، والذي جاء بمجموعة من النصوص التي تحمي عمليات المعالجة وتحمي المعطيات الشخصية المعالجة، ومن أهم المواد نجد المادة53 التي عاقبت بالغرامة من 20000درهم إلى 200000 درهم في حالة رفض المسؤول عن المعالجة حقوق

[1] - Francesco Miani, le cadre réglementaire des traitements de données personnelles, effectues au sein de l'union européenne, revue trimestrielle de droit européen, Dalloz,n2, 2000, p283.

[2] – الصادر بتاريخ 18 فبراير 2009 والصادر بتنفيذه الظهير رقم 15-09-1 الصادر بتاريخ 18 فبراير2009 الموافق 22 صفر 1430.

[3]– يمكن الحصول على هذا القانون من الجريدة الرسمية المغربية عدد5700 بتاريخ 23 فبراير 2009، ص552.

الولوج أو التصريح أو التعرض، المنصوص عليها في المواد7 و 8 و9 من القانون رقم 08 -09.[1]

- كما جرمت المادة 63 عملية نقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام المادتين 43و44 من هذا القانون.[2]

ثانيا : القانون المغربي رقم 53/05 المتعلق بالتبادل الالكتروني للمعطيات القانونية، [3]

ولقد سعى المشرع المغربي إلى تهيئة بيئة قانونية، تناسب التطور المذهل في مجال المعاملات التي تتم بطرق الكترونية، وبالتالي الانتقال من مرحلة التعامل الورقي إلى مرحلة التعامل الالكتروني، ويأتي في هذا السياق صدور القانون المغربي رقم 53-05 المتعلق بالتبادل الالكتروني للمعطيات القانونية.[4]

وإذا كان القانون رقم 05-53 أثر بشكل أساسي على فصول قانون الالتزامات والعقود المغربي، بفعل تعديل بعض نصوصه أو إضافة أخرى جديدة متصلة بالبيئة المعلوماتية، إلا انه يتضمن كذلك مجموعة من النصوص الزجرية[5]، والتي تساهم في مكافحة الجرائم المعلوماتية، نذكر منها المادة 29 التي تعاقب كل من يقدم خدمات للمصادقة الالكترونية المؤمنة خلافا للمادة20 أو دون أن يكون معتمدا أو من يواصل نشاطه رغم سحب اعتماده.[6]

ومن اجل ضمان سلامة تبادل المعطيات القانونية بطريقة الكترونية وضمان سريتها وصحتها، فرض المشرع حماية خاصة لوسائل التشفير، من خلال المادة32 التي تجرم استيراد أو

---

[1] – تنص المادة53 يعاقب بغرامة من 20000 إلى 200000 درهم عن كل مخالفة كل مسؤول عن معالجة المعطيات ذات الطابع الشخصي، يرفض حقوق الولوج أو التصريح أو التعرض، المنصوص عليها في المواد7و8و9 .

[2] – تنص المادة60 يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من 20000 درهم إلى 200000 درهم أو بإحدى هاتين العقوبتين، فقط كل من نقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام المادتين 43 و44 من هذا القانون.

[3]– صدر مؤخرا مرسوم رقم518-08-2 بتاريخ 21ماي2009 موافق 25 جمادى1 1430، بشان تطبيق المواد13و14و15و21و23 من القانون رقم 05-53 المتعلق بالتبادل الالكتروني للمعطيات القانونية.

[4]– هذا القانون صدر بتنفيذه الظهير رقم 129-7-1 بتاريخ 30نوفمبر2007 الموافق 19 من ذي القعدة 1428.

[5]– من خلال الباب الثالث من القسم الثاني من هذا القانون، والذي عنوانه العقوبات والتدابير الوقائية ومعاينة المخالفات.

[6]– تنص المادة29 يعقب بغرامة من 10000 إلى 100000 درهم وبالحبس من ثلاثة أشهر إلى سنة كل من قدم خدمات للمصادقة الالكترونية المؤمنة ،دون أن يكون معتمدا وفق الشروط المنصوص عليها في المادة21 أو واصل نشاطه رغم سحب اعتماده أو اصدر أو سلم أو دبر شهادات الكترونية مؤمنة خلافا لأحكام المادة20 .

استغلال أو استعمال إحدى الوسائل أو خدمة من خدمات التشفير، دون الإدلاء بالتصريح أو الحصول على الترخيص، كما انه يمكن للمحكمة الحكم بمصادرة وسائل التشفير المعنية.[1]

البند الثالث : أبعاد الأمن المعلوماتي في مصر

بدأت عمليات تمديد البنية التحتية الرقمية في مصر عام 1992. ومنذ ذلك التاريخ، تتخذ مصر عددًا من الإجراءات لكفالة أمنها السيبراني؛ الأمر الذي أهلها لاحتلال مرتبة متقدمة في مؤشر الأمن السيبراني GCI[2] التابع للاتحاد الدولي للاتصالات، الذي يُعنَى بأمن المعلومات على مستوى 193 دولة؛ ففي تصنيف ديسمبر 2014، جاءت مصر في المرتبة التاسعة مكررة على مستوى العالم. وجاءت فرنسا وإسبانيا والدانمارك وكولومبيا وجمهورية موريشيوس في المرتبة التاسعة كذلك.

أما على صعيد الدول العربية، فلقد جاءت مصر في المرتبة الثالثة، بعد دولة قطر وسلطنة عمان.

والواقع أن قضية الأمن السيبراني في مصر ذات أبعاد تنظيمية وقانونية وفنية؛ وذلك على النحو التالي:

أ. الإطار التنظيمي:

تعتبر وزارة الاتصالات وتكنولوجيا المعلومات في مصر هي الجهة المنوطة بها كفالة الأمن السيبراني. وتنظم الوزارة جهودها عبر صياغة استراتيجيات وخطط، كالخطة القومية للاتصالات في عام 2000، والاستراتيجية القومية لتكنولوجيا المعلومات والاتصالات في عام 2007. وفي عام 2013، أعلنت الوزارة عن "إستراتيجية 2020" التي ترتكز على 3 أهداف رئيسية:

[1]- تنص المادة32 يعاقب بالحبس لمدة سنة وبغرامة مبلغها100.000 درهم كل من استورد أو صدر أو ورد أو استغل أو استعمل، إحدى الوسائل أو خدمة من خدمات تشفير دون الإدلاء بالتصريح أو الحصول على الترخيص، المنصوص عليهما في المادتين13و14، يجوز للمحكمة أيضا أن تحكم بمصادرة وسائل التشفير المعنية) .

[2] - Global Cybersecurity Index

1. التحول نحو مجتمع رقمي.
2. تطوير صناعة تكنولوجيا المعلومات والاتصالات.
3. تحويل مصر إلى مركز رقمي عالمي.

ب. الإطار القانوني:

وقّعت مصر على عدد من الاتفاقيات والمعاهدات الدولية المتعلقة بالأمن السيبراني، كما تم إقرار قوانين تساعد على تنظيم الأمن السيبراني؛ منها قانون الملكية الفكرية (قانون رقم 82 لسنة 2002)، وقانون الاتصالات (قانون رقم 10 لسنة 2003)، وقانون التوقيع الإلكتروني ولائحته التنفيذية (قانون رقم 15 لسنة 2004.)، هذا بالإضافة إلى الأخذ ببعض مواد قانون الطفل[1]، كالمادة 116 مكرر (أ) المتعلقة بتجريم استغلال الأطفال والاعتداء عليهم عبر الإنترنت، وقانون المحاكم الاقتصادية (قانون رقم 120 لسنة 2008). وكذلك يتم الرجوع إلى عدد من مواد قانون العقوبات (قانون رقم 58 لسنة 1937)، وقانون الإجراءات الجنائية)قانون رقم 150 لسنة 1950 المعدل)، وقانون الأحوال المدنية (قانون رقم 143 لسنة1994)؛ حيث تجرم المادة 72 من قانون الأحوال المدنية أي شروع في الاطلاع أو الحصول على المعلومات المخزنة على أجهزة الحاسب الآلي أو محاولة التصرف في المعلومات، كما توضح المادة العقوبات التي تترتب على تلك الأفعال.

ج. الإطار الفني:

تم تأسيس عدد من الكيانات للإسهام في تحقيق الأمن السيبراني؛ من أهمها:

أولا. **المركز المصري للاستجابة للطوارئ المعلوماتية "سيرتCERT" :** قام الجهاز القومي لتنظيم الاتصالات، بتأسيس المركز المصري للاستجابة للطوارئ الحاسب الآلي (سيرت) في ابريل

[1]- قانون رقم 12 لسنة 1996 وتعديلاته بالقانون رقم 126 لسنة 2008.

2009، حيث يعمل به فريق من ستة عشر متخصصا بدوام كامل، ويقدم الفريق المتخصص الدعم الفني على مدار 24 ساعة لحماية البنية التحتية الحيوية للمعلومات .

ويقدم المركز المصري للاستجابة للطوارئ المعلوماتية (سيرت) منذ عام 2012 الدعم لمختلف الجهات عبر قطاعات تكنولوجيا المعلومات والاتصالات، والخدمات المصرفية والحكومية من أجل مساعدتهم على مواجهة تهديدات الأمن السيبراني، بما في ذلك هجمات الحرمان من الخدمة.

وتتمحور مهمة المركز المصري للاستجابة للطوارئ المعلوماتية (سيرت) حول توفير نظام للإنذار المبكر ضد البرمجيات الخبيثة والهجمات الإلكترونية، التي تنتشر بنطاق واسع ضد البنية التحتية الحيوية للمعلومات المصرية [1].

- الأهداف :

1. وضع إطار تشريعي ملائم للأمن المعلوماتي، بمشاركة القطاع الخاص والمجتمع المدني واسترشادا بالخبرة الدولية والمبادرات ذات الصلة

2. وضع إطار تنظيمي مناسب للأمن المعلوماتي، بالإعتماد على الخبرة الدولية لإنشاء نظام وطني للأمن السيبراني ومراكز استجابة للطوارئ

3. تأسيس البنية التحتية اللازمة لضمان الثقة في المعاملات الإلكترونية وحماية الهوية الرقمية، مثل البنية التحتية للمفاتيح العامة ومكاتب الائتمان بمشاركة القطاع الخاص

4. وضع وتنفيذ برامج لبناء القدرات البشرية، اللازمة لتفعيل نظام الخدمات الإلكترونية في جميع القطاعات، وذلك بالتعاون مع القطاع الخاص والجامعات والمنظمات غير الحكومية

5. التعاون مع الدول الأخرى والمنظمات الدولية، ذات الصلة بمجالات الأمن السيبراني والخدمات الإلكترونية .

[1]- ان المركز المصري للاستجابة للطوارئ المعلوماتية (سيرت)،لديه العديد من اتفاقيات التعاون مع فريق الطوارئ للحاسوب بالولايات المتحدةUS-CERT،ووكالة أمن الإنترنت الكورية KISA في مدينة سيول، والهيئة الماليزية للأمن السيبراني، كما أن سيرت عضو في فريق الاستجابة لطوارئ الحاسوب التابع لمنظمة المؤتمر الإسلامي.

6. رفع الوعي العام بفوائد الخدمات الإلكترونية، للأفراد والشركات والمؤسسات وبأهمية الأمن المعلوماتي[1].

- **الإنجازات:**

1. افتتاح مبنى المركز المصري للاستجابة للطوارئ المعلوماتية الجديد، في ديسمبر عام 2013.
2. حصول المركز على عضوية اللجنة التوجيهية لفريق الاستجابة لطوارئ الحاسوب، التابع لمنظمة المؤتمر الإسلامي في نوفمبر عام 2013.
3. احتل المركز المرتبة الثالثة حسب مؤشر الأمن المعلوماتي العالمي للاتحاد الدولي للاتصالات في أكتوبر عام 2013.
4. تنظيم ورشة العمل الأولى للأمن السيبراني، وذلك في شهر مايو عام 2013 في القرية الذكية، تحت رعاية الجهاز القومي لتنظيم الاتصالات لمناقشة آخر الأبحاث والتطورات في مجال الأمن السيبراني، حيث قدمت أوراق البحث في مختلف المجالات
5. تشكيل اللجنة الوطنية لحماية الطفل على الإنترنت في مارس عام 2013
6. حصول فريق طوارئ الحاسب الآلي المصري، على العضوية الكاملة في منتدى فرق الاستجابة لقضايا الأمن *(FIRST)*[2] في عام 2012، وهو المنتدى الدولي الرئيسي

---

[1] www.mcit.gov.eg/Ar/Project_Updates/443/TeleCommunications/Cyber_Security.

2 - **FIRST**: is the global Forum for Incident Response and Security Teams

FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents reactive as well as proactive.

FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

Apart from the trust network that FIRST forms in the global incident response community, FIRST also provides value added services. Some of these are:

لفرق سيرت المشاركة في التدريبات السيبرانية العملية، التي نظمها فريق الاستجابة لطوارئ الحاسوب بآسيا والمحيط الهادئ (*APCERT*)[1] وفريق الاستجابة لطوارئ الحاسوب التابع لمنظمة المؤتمر الإسلامي (*OICCERT*)[2] والاتحاد الدولي للاتصالات والشراكة الدولية متعددة الأطراف لمكافحة الإرهاب السيبراني في عام 2012.

7. عرض إطار الأمن السيبراني المصري، في واحدة من الجلسات الرئيسية لمنتدى حوكمة الإنترنت في عام 2012 في أذربيجان .

8. المشاركة في مؤتمر بودابست للفضاء الإلكتروني في أكتوبر 2012 في المجر .

9. تنظيم البعثات الخاصة إلى فنلندا واستونيا، لاستكشاف فرص التعاون في مجال الأمن السيبراني من خلال فرق الاستجابة لطوارئ الحاسوب، وكذلك في مجال التوقيع الإلكتروني

10. مشاركة مصر في ورشة العمل الإقليمية العربية، حول حماية الأطفال على الانترنت بالاتحاد الدولي للاتصالات، حول "الجوانب القانونية لحماية الأطفال على الإنترنت في

- access to up-to-date best practice documents
- technical colloquia for security experts
- hands-on classes
- annual incident response conference
- publications and web services
- special interest groups

Currently FIRST has more than 300 members, spread over Africa, the Americas, Asia, Europe and Oceania. https://www.first.org

[1] -AP-CERT - Asia Pacific Computer Emergency Response Team , APCERT (Asia Pacific Computer Emergency Response Team) is a coalition of CSIRTs (Computer Security Incident Response Teams), from 13 economies across the Asia Pacific region. APCERT organizes an annual meeting called APSIRC conference, and the first conference was held in March 2002, Tokyo , Japan
More Info: http://www.apcert.org/

[2] - The Organisation of The Islamic Cooperation (OIC) has approved and accepted the Resolution on "Collaboration of Computer Emergency Response Team (CERT) Among the OIC Member Countries". The Resolution was approved during the 35th Session of the Council of Foreign Ministers of the OIC Meeting in Kampala, Uganda on 18 – 20 June 2008. The Resolution No 3/35-INF. http://www.oic-cert.org/en/index.html

المنطقة العربية" [1]التي استضافتها وزارة البريد وتكنولوجيات الإعلام والاتصال في الجزائر بالعاصمة الجزائرية يومي 24 -25 يونيو 2012

11. وفي ديسمبر 2012، بدء تشغيل خدمة اختبار الاختراق .

12. وفي سبتمبر 2009، بدأت خدمة رقمنه تحليل الطب الشرعي .

13. وفي يوليو 2009، تم إتاحة خدمة الرصد والاستجابة للحوادث على مدار 24 ساعة يوميا طوال الأسبوع[2].

14. أول قانون لجرائم الإنترنت في مصر2015 جاء في مقدمة القانون التعارف والمفاهيم التي نص عليها القانون في المادة الأولى، حيث يقصد بتقنية المعلومات أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تستخدم لتخزين، وتطوير، وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكياً أو لا سلكياً .

ويعاقب القانون بالحبس مدة لا تقل عن سنتين كل من أتلف، أو عطل، أو دمر، أو شوه، أو غير، أو عدل مسار، أو ألغى كلياً أو جزئياً، بدون وجه حق، البرامج أو البيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه، أياً ما كانت الوسيلة التي استخدمت فى الجريمة، فإذا كانت هذه البرامج أو البيانات أو المعلومات تخص الدولة أو أحد الأشخاص الاعتبارية العامة تكون العقوبة السجن[3].

1- و يعاقب في المادة السادسة من قانون جرائم تقنية المعلومات المصري بالغرامة 50 ألفا لكل من يعطل عمل المواقع :

يعاقب بالسجن وبغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 250 ألف جنيه كل من أدخل إلى شبكة معلوماتية ما، من شأنه إيقافها عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها، أو إعاقتها، أو التنصت عليها أو اعتراض عملها.

[1] -httpS://www.aimcouncil.org.

[2] - httpS://www.mcit.gov.

[3]- المادة الخامسة من قانون مكافحة جرائم الإنترنت في مصر، الذي تم اعتماده في مارس 2015.

فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة، أو تدار بمعرفتها، تكون العقوبة السجن المؤبد أو المشدد، وغرامة لا تقل عن 100 ألف جنيه ولا تجاوز 500 ألف جنيه[1]، ويعاقب القانون بالحبس مدة لا تقل عن ستة أشهر، كل من التقط أو اعترض بدون وجه حق أي معلومات أو بيانات أو أرقام أو رسائل أو حروف أو شفرات أو صور، مما هو مرسل عن طريق شبكة معلوماتية، أو أحد أجهزة الحاسب الآلي وما في حكمها أو تنصت عليها، فإذا كان فعل الاعتراض أو الالتقاط أو التنصت، قد وقع على معلومات أو بيانات أو أرقام أو حروف أو شفرات أو صور تخص الدولة أو أحد الأشخاص الاعتبارية العامة، تكون العقوبة السجن وغرامة لا تقل عن 100 ألف جنيه ولا تجاوز 500 ألف جنيه[2].

ويعاقب أيضا بالحبس وبغرامة لا تقل عن 20 ألف جنيه ولا تجاوز 100 ألف جنيه، أو بإحدى هاتين العقوبتين كل من أتلف أو عطل أو أبطأ أو شوه أو أخفى، أو غير تصاميم أو محتوى موقعاً خاصاً بشركة أو مؤسسة أو منشأة بدون وجه حق، فإذا وقعت الجريمة على موقع يدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكاً لها، أو يخصها، تكون العقوبة السجن وغرامة لا تقل عن 100 ألف جنيه ولا تجاوز 500 ألف جنيه[3].

1. الحبس والغرامة لكل من يسرق بريد الكتروني لآخرين :

يعاقب بالحبس وبغرامة لا تجاوز 5 آلاف جنيه، كل من استخدم بريداً إلكترونياً لا يخصه فى أمر يسيء إلى صاحب البريد، كما يعاقب بالحبس وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرة آلاف جنيه كل من اصطنع بريداً إلكترونياً أو موقعاً، ونسبه زوراً إلى شخص طبيعي أو اعتباري، فإذا استخدم الجاني البريد أو الموقع المصطنع في أمر يسيء إلى من اصطنع عليه، تكون العقوبة الحبس الذي لا تقل مدته عن سنتين، وإذا وقعت الجريمة على أحد الأشخاص الاعتبارية العامة تكون العقوبة السجن.

2. الحبس سنتين لكل من ينشئ موقعا يحرض على ارتكاب جرائم[4] :

[1]- الفقرة الثانية من المادة السادسة من قانون جرائم تقنية المعلومات المصري 2015.

[2]- المادة السابعة من قانون جرائم تقنية المعلومات المصري 2015.

[3]- المادة الثامنة من قانون جرائم تقنية المعلومات المصري 2015.

[4]- المادة الرابعة عشر من قانون جرائم تقنية المعلومات المصري 2015.

أشار القانون إلى أنه يعاقب بالحبس مدة لا تقل عن سنتين كل من أنشأ، أو ساهم في إنشاء، موقعاً على شبكة معلوماتية، يهدف إلى الترويج لارتكاب أية جريمة من المنصوص عليها في قانون العقوبات، أو أي من القوانين الخاصة .فيما يعاقب بالحبس المسئول عن الإدارة الفعلية لأي شخص اعتباري، إذا تعرض الموقع أو البريد الإلكتروني المخصص للكيان الذي يديره لأي جريمة من الجرائم المنصوص عليها في هذا القانون، و لم يبلغ بذلك الجهات الرسمية المختصة وقت علمه بالجريمة .

3. غلق المواقع المهددة للأمن القومي : [1]

فيما منح القانون جهات التحري والضبط المختصة، إذا ما رصدت قيام مواقع تبث من داخل الجمهورية، أو خارجها، بوضع أية عبارات أو أرقام أو صور أو أفلام، أو أية مواد دعائية، أو غيرها، من شأنها تهديد الأمن القومي، أن تعرض محضراً بذلك على جهات التحقيق وتطلب الإذن بحجب المواقع أو المواقع محل البث، أو حجب بعض روابطها، وتقوم جهة التحقيق بعرض طلب الإذن على محكمة الجنايات، منعقدة في غرفة مشورة خلال أربع وعشرين ساعة مشفوعاً بمذكرة برأيها، وتصدر محكمة الجنايات قرارها في الطلب، في ذات يوم عرضه عليها، إما بالقبول أو الرفض .ويعاقب بالحبس الذي لا تقل مدته عن ثلاث سنوات، وبغرامة لا تقل عن 500 ألف جنيه ولا تجاوز مليون جنيه، كل مزود خدمة امتنع عن تنفيذ القرار الصادر من محكمة الجنايات بحجب أحد المواقع أو الروابط المشار إليها في الفقرة الأولى من المادة 19 من ذات القانون.

فإذا ترتب على الامتناع عن تنفيذ القرار الصادر من المحكمة وفاة شخص أو أكثر أو الإضرار بالأمن القوم، تكون العقوبة السجن المؤبد أو المشدد، وغرامة لا تقل عن 3 ملايين جنيه ولا تجاوز عشرين مليون جنيه.

وينص القانون إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بواسطة شخص اعتباري خاص، يحكم في حالة الإدانة، فضلاً عن العقوبة المقررة عن الجريمة، بوقف نشاطه مدة مساوية لمدة العقوبة، أو مدة ثلاث سنوات على الأكثر، وفى الحالات التي يتعين

[1]- المادة التاسع عشر من قانون جرائم تقنية المعلومات المصري 2015.

لمزاولة النشاط فيها للحصول على ترخيص من إحدى الجهات الحكومية، وكان الشخص الاعتباري المدان بأي جريمة منصوص عليها في هذا القانون لم يحصل على الترخيص، فيحكم فضلاً عن العقوبات المقررة للجريمة بالغلق .

4.عزل الموظفين العموميين المتورطين في جرائم الإنترنت :

إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون، بمعرفة أحد الموظفين العموميين وكان ذلك أثناء وبسبب تأديته لوظيفته، فيجب عند الحكم بالإدانة، أن تحكم المحكمة بعزلة من وظيفته، ويعاقب المسئول عن الإدارة الفعلية للشخص الاعتباري بذات العقوبات عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون، متى ثبت علمه بها، وكان إخلاله بواجبات الإدارة قد سهل وقوع الجريمة، ويكون الشخص الاعتباري مسئولاً بالتضامن عن الوفاء بما يحكم عليه من عقوبات مالية بموجب أحكام هذا القانون، مع المدانين بارتكابها .

وألزم القانون مزودي الخدمة باتخاذ كافة الإجراءات والتدابير التقنية اللازمة، نحو حفظ وتخزين محتوى النظام المعلوماتي ،أو أي وسيلة لتقنية المعلومات وكذا حفظ وتخزين بيانات خطر سير حركة رسائل البيانات وذلك لمدة تسعين يوماً[1].

ثانيا: هيئة تنمية صناعة تكنولوجيا المعلومات :لقد تم تأسيس تلك الهيئة بموجب القانون رقم 15 لسنة 2004، ويقع ضمن اختصاصاتها الأساسية الإشراف على تطبيق قانون التوقيع الإلكتروني؛ حيث إنها قد تأسست عقب صدور ذلك القانون، بالإضافة إلى ذلك، فهي تختص بالاهتمام بقضايا العاملين في مجال التوقيع الإلكتروني.

ثالثا: المجلس الأعلى للأمن السيبراني: أصدر القرار بإنشائه في ديسمبر من عام 2014، و يكمن دور المجلس الأساسي في "وضع إستراتيجية لمواجهة الأخطار السيبرانية، والإشراف على تنفيذها".

[1]- المادة السادسة و العشرون من قانون جرائم تقنية المعلومات المصري 2015.

ونافلة القول أن مصر تتعرض لعدد من التهديدات السيبرانية يصعب التصدي لها؛ وذلك لأن الفضاء الافتراضي من الصعب السيطرة التامة على محتواه؛ فالجماعات المتطرفة على سبيل المثال، دومًا ما تجد سبلًا بديلة. وفي مواجهة التهديدات، قد يكون فرض قدر من الرقابة على استخدامات الإنترنت وسيلة فعالة؛ وذلك على غرار ما تقوم به العديد من الدول الديمقراطية المتقدمة، كالولايات المتحدة الأمريكية والمملكة المتحدة البريطانية. ولكن في الوقت ذاته، يجب أن يراعى توافر مجموعة من الشروط فيها، كعدم انفراد جهة واحدة بممارسة الرقابة على استخدامات الإنترنت[1]، وألا تنتهك الرقابة خصوصيات المواطنين، وأن تتم رقابة المجال الخاص (المحادثات والرسائل والمكالمات الخاصة) بموجب إذن مسبق من الجهات الرسمية المعنية، وألا يكون الهدف من الرقابة تقييد وقمع الحريات ومنع المواطنين من ممارسة حقوقهم المشروعة المكفولة لهم بموجب الدستور[2].

البند الرابع: المملكة العربية السعودية :

تتميز المملكة العربية السعودية باعتمادها على القرآن الكريم والسنة النبوية المطهرة، شريعة وحكما في جميع شؤون الحياة، ومن هذا المنطلق فإن التعاملات المرتبطة بتقنية المعلومات ، كغيرها من مجالات الحياة، يجب أن تخضع للأحكام الشرعية المستمدة من الكتاب والسنة، وفي ضوء تلك الأحكام تقوم الجهات المعنية بوضع اللوائح المحددة لحقوق والتزامات الأطراف المختلفة، كما تقوم الهيئات الأمنية والقضائية والحقوقية بتنزيل تلك الأحكام واللوائح على القضايا المختلفة وفض النزاعات الناتجة عنها .

وبالرغم من إدراك أهمية وجود وتطبيق أحكام وأنظمة تقنية المعلومات، فإن الجهود المبذولة لدراسة وتنظيم ومتابعة الالتزام بتلك الأحكام، لا يزال في مراحله الأولية، وما تم في هذا الشأن لا يتجاوز مجموعة من القرارات المنفصلة واللوائح الجزئية، التي لا تستوعب القضايا

1- كما هو قرار وزير الداخلية المتمثل في إجراء الممارسة المحدودة رقم 22 لسنة 2014/2013؛ وذلك لتوريد ما أطلق عليه منظومة قياس الرأي العام"، في سياق "مشروع رصد المخاطر الأمنية لشبكات التواصل الاجتماعي، الأمر الذي دفع عددًا من الجماعات الحقوقية إلى إقامة دعوى قضائية أمام محكمة القضاء الإداري في 17 يونيو 2014، الدعوى رقم 63055لسنة 2014.

2-نوران شريف ،تهديدات الأمن السيبراني في مصر.. هل الرقابة هي الحل؟ كتب بتاريخ 26/04/2015 ،متوفر على الموقع التالي: http://www.rcssmideast.org/

المستجدة في أعمال تقنية المعلومات، كما لا توجد بصورة منظمة ومعلنة أقسام أمنية ومحاكم مختصة، ومنتجات إعلامية لشرائح المجتمع المختلفة[1].

ولقد صدرت في المملكة العربية السعودية بعض الأنظمة واللوائح والتعليمات، والقرارات لمواجهة الاعتداءات الإلكترونية، ونصت تلك الأنظمة على عقوبات في حال المخالفة لهذه الأنظمة والتعليمات واللوائح فمن ذلك[2] :

1. **نظام حماية حقوق المؤلف الجديد 1424هـ ولائحته التنفيذية** ،الصادر بالمرسوم الملكي رقم م/41 بتاريخ 2 رجب 1424هـ[3]، وهذا النظام يمنع جميع صور استنساخ البرامج، وإذا تم ضبط أي مخالفة من منشأة تجارية، أو مصانع، أو شركات تعتمد على الحاسب الآلي في أعمالها وتستخدم برامج غير أصلية في تشغيل الجهاز، فإنها ستكون عرضة لتطبيق العقوبات الواردة في النظام، فقد نص في الباب الثاني الموسوم بالمخالفة وإجراءات ضبطها في الفصل الأول منه، تحت عنوان المخالفات ومسئولية الاعتداء على حق لمؤلف فنجد :

- **المادة الحادية عشر : مسئولية الاعتداء**

أولاً : يعتبر معتدياً على حق لمؤلف، كل من يحصل على نسخة أصلية لأي مصنف فكري، ويقوم باستغلاله كتأجيره أو تحويره أو السماح لآخرين بتصويره أو استنساخه، أو غير ذلك من التصرفات التي تؤثر أو تعيق المؤلف عن ممارسة حقوقه.

ثانياً : تعتبر المنشئات مسئولة، عن أي مخالفات يرتكبها أحد العاملين بها على أي مصنف فكري، إذا ثبت علمها أو تقصيرها، مثل الاحتفاظ ببرامج حاسب أو أشرطة مسموعة أو مرئية مزورة أو منسوخة، أو إجراء صيانة لجهاز إلكتروني محمل ببرامج مزورة أو مفكوك الشفرة أو نحو ذلك من مصنفات.

---

[1]- صالح بن محمد المسند، عبد الرحمان بن راشد المهيني، جرائم الحاسب الآلي، الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية و التدريب، أكاديمية نايف العربية، ع 29، الرياض، 2000، ص 151.

[2] – عبد الرحمن بن عبد الله السند، المرجع السابق، ص 388.

[3]- حل هذا النظام محل نظام حماية حقوق المؤلف، الصادر بالمرسوم الملكي ذي الرقم(م/11)،المؤرخ في1410/5/19هـ

ثالثاً : يعتبر تعدياً على حقوق المؤلف،ومخالفاً أحكام النظام وهذه اللائحة، كل من أعاد إنتاج مصنفات محمية، أو باع هذه المصنفات أو استوردها أو صدرها أو تولى نقلها أو نشرها أو تأجيرها وهو يعلم بالمخالفة.

- **المادة الثانية عشر : التعدي على المصنفات الأدبية[1]:**

أولاً : يعتبر في نطاق الاستخدام الشخصي، كل استعمال للمصنف الفكري بقصد الاستخدام الشخصي الخاص، دون سواه مثل استنساخ المصنف بغرض الاحتفاظ بالنسخة الأصلية، والكتابة على النسخة المستنسخة أو لترجمة فقرات منه أو لكتابة تعليقات تعبر عن الرأي الشخصي، وما تعدى هذه الأغراض اعتبر تجاوزاً لحدود الاستخدام الشخصي.

ثانياً : يعتبر تعديا كل استخدام للمصنف،يتخطى مفهوم الاستخدام الشخصي في مثل الحالات التالية:

1. استخدام ونسخ المصنف أو الاستعانة به واستغلاله لأداء مهام وظيفية.
2. استخدام المصنف لأغراض تجارية أو استهداف الربح.
3. استخدام المصنف بطرق لا يسمح بها المؤلف.
4. تأجير المصنف أو استنساخه أو السماح لأخرين باستنساخه أو تحويره بحجة امتلاك نسخه أصلية.
5. أي تصرفات تعيق المؤلف من ممارسة حقه الأدبي أو المالي.

ثالثاً : يعد تعدياً على حق المؤلف،استنساخ المصنف بقصد توفير نسخ منه للاستغلال التجاري أو لبيعه على طلبه العلم، أو المؤسسات التعليمية أو غير ذلك.

رابعاً : امتلاك صاحب العمل لنسخه أصليه من المصنف لا يعطيه حق استنساخها

[1]- نظام حماية حقوق المؤلف الجديد 2003 ولائحته التنفيذية، الصادر بالمرسوم الملكي رقم م/41 بتاريخ 29أوت 2003م.

وتوزيعها على موظفين منشآته بحجة أنها استخدام شخصي.

- **المادة الثالثة عشر : التعدي على المصنفات السمعية والبصرية والبث الإذاعي.**

يعتبر تعدياً على حق المؤلف في المصنفات السمعية والمرئية والإذاعية، عند تجاوز طرق الاستخدام التي حددها من يملك حقها، ومن أمثلة ذلك ما يلي:

1. إذاعة المصنف للجمهور دون الحصول على ترخيص مسبق من أصحاب الحق، مثل استخدام الإذاعة أو الموسيقى أو الفيديو أو البث الفضائي في المحلات التجارية، والمطاعم والفنادق والأندية والمستشفيات ونحوها من الأماكن،التي يكون فيها مرتادين أو تجمعات بشرية.
2. كسر الحواجز الاحترازية بغرض عرض المواد الإذاعية بطرق غير نظامية.
3. استنساخ المواد المذاعة بغرض عرضها أو تأجيرها أو بيعها.
4. إضافة أو إزالة شرائح إلكترونية لأجهزة العرض،بهدف تجاوز الجهاز إمكانيات الحدود التي صنع بها بغرض التعدي على حقوق الآخرين.

- **المادة الرابعة عشر : التعدي على حقوق الأداء [1]:**

يعتبر تعدياً على حقوق الأداء، إذا تم أداء المصنف في الحفلات المدرسية أو نحوها، ما لم تحصل الجهة المؤدية للمصنف على موافقة مسبقة من أصحاب الحقوق، لأدائه ويعتبر استخداماً نظامياً وفقاً لما ورد في المادة 15 البند 8 من النظام، إذا كان الأداء للمصنف في غرفة الدرس التطبيقي بغرض التعليم.

كما يعتبر تعدياً على حقوق المؤلف كل استنساخ للمصنف أثناء أدائه كتصويره بغرض استغلاله أو نقله للجمهور بدون موافقة أصحاب الحق.

[1]- نظام المملكة العربية السعودية المتعلق بحماية حقوق المؤلف 2003م.

- **المادة الخامسة عشر : فك التشفير للأجهزة الإلكترونية:**

يعتبر تعدياً على حقوق المؤلف كل عمل يؤدي إلى إزالة المعلومات الاحترازية الأصلية من الأجهزة الإلكترونية، التي أنتجها الصانع، ويعد متعدياً كل من يسهل ذلك مثل:

1. إزالة أو إضافة شرائح إلكترونية أو غير إلكترونية لأجهزة العرض والاستقبال بغرض تجاوز الحدود التي وضعها الصانع.

2. إلغاء البرنامج الأصلي المشغل، لأجهزة العرض والاستقبال وتحميلها ببرامج مزورة بغرض تجاوز الحدود والإمكانيات التي صمم لها الجهاز.

- **المادة السادسة عشر : الاعتداء على برامج الحاسب الآلي**

أولاً : تتمتع بالحماية برامج الحاسب الآلي وبرامج ألعاب الحاسب، سواء كانت بلغة المصدر أو بلغة الآلة باعتبارها أعمالاً أدبية.

ثانياً : يعتبر تعديا على حق المؤلف، كل استخدام للبرامج تخالف الاستخدامات التي يحددها صاحب الحق مثل:

1. استنساخ البرامج وبرامج الألعاب.

2. تأجير البرامج أو برامج الألعاب أو الترخيص بالاستخدام الجماعي لها، بدون وجود وثائق تخول المؤجر، بممارسة هذا الحق بعد موافقة الوزارة عليه.

3. تحميل الشبكات الداخلية أو الأجهزة ببرامج مستنسخة.

- **المادة السابعة عشر : مسئولية محلات الصيانة.**

تعتبر محلات ورش تقديم خدمات الصيانة لأجهزة العرض والاستقبال الإلكترونية مسئولة ومعتدية على حق المؤلف، عند ضبط أجهزة لديها مفكوكة الشفرة أو محملة ببرامج مزورة أو تستخدم في أعمال الصيانة برامج مزورة.

ونجد في المادة الثامنة عشر من الفصل الثاني، ما تتخذه المملكة العربية السعودية من إجراءات لضبط المخلفات والتحقيق فيها[1].

البند الخامس : الإمارات العربية المتحدة

تفوقت حكومة الإمارات العربية المتحدة، على الدول الأوروبية في مجال الجاهزية لمواجهة مخاطر الأمن الإلكتروني[2]، وحماية البنية التحتية الوطنية والحيوية للدولة ضد التهديدات الإلكترونية المتنامية، وفقاً لما أعلنه خبراء على مستوى هذه الصناعة.

وفي هذا السياق قالت سافيثا بهاسكار[3]: "يبرهن التصنيف المثير للإعجاب لدولة الإمارات العربية المتحدة، على مدى فعالية وانتشار نطاق عمل الهيئة الوطنية للأمن الإلكتروني، كما يبرهن على مكانة حكومة الإمارات العربية المتحدة ضمن الدول الأكثر ابتكاراً في العالم في مجال تحديد أولويات الأمن الالكتروني."

ولمواجهة العدد المتنامي والمتطور للهجمات الإلكترونية، أطلقت الهيئة الوطنية للأمن الإلكتروني في الإمارات العربية المتحدة خلال العام 2014 برنامج الأمن الإلكتروني الوطني، الذي يُلزم الهيئات الحكومية بتقديم تقارير عن حالة البنية التحتية للأمن الإلكتروني الذي لديها، وذلك كجزء من الجهود الرامية إلى خلق بيئة وطنية رقمية آمنة.

---

[1]- المادة 18 من نظام حماية حقوق المؤلف 2003،يكون ضبط ما يقع من مخالفات لأحكام النظام واللائحة في أي من الحالات التالية-:

1. بناءً على شكوى أو بلاغ خطي مقدم من أصحاب الحقوق أو من يمثلهم.
2. الجولات الميدانية المعتادة والمفاجئة لمفتشي الوزارة على المنشآت العامة والمحلات التجارية التي تستخدم في نشاطا أياً من المصنفات الفكرية.

[2]- واحتلت دولة الإمارات العربية المتحدة، المركز الـ17 عالميا في التصنيف الأخير لـ "المؤشر العالمي للأمن السيبراني"، الصادر عن الاتحاد الدولي للاتصالات التابع لهيئة الأمم المتحدة، لتتفوّق بذلك على عدد من الدول الأوروبية. ويقوم هذا المؤشر بقياس عدة جوانب لقطاع الأمن الإلكتروني، بما فيها التشريع، واللوائح، والامتثال، وبناء القدرات، والتعاون الدولي.
نُشر في جريدة العرب ، بتاريخ 2016/01/17، العدد: 10157، ص18 متوفر على الرابط التالي :
http://www.alarab.co.uk
أنظر كذلك : معاوية الخالد، الإمارات تتفوق على العديد من الدول الأوروبية في الجاهزية لمواجهة مخاطر الأمن الالكتروني، كتب بتاريخ 14 يناير 2016 ، متوفر على الرابط التالي : https://aitnews.com/2016.

[3] -Directeur des Opérations de la société de conseil Kondo Brocevo, dans le domaine de l'information, et de la technologie d'experts en sécurité e -domaine.

ومن خلال هذا البرنامج، ستتمكن الهيئة الوطنية للأمن الإلكتروني أيضاً من مراقبة أنظمة الأمن الإلكتروني في الهيئات الحكومية، وإجراء اختبارات للأمن الإلكتروني، والتدخل بهدف تعزيز أمن الأنظمة[1].

لتفعيل التعاون الدولي العربي،لابد من التركيز على أربع موضوعات رئيسية لابد من العمل على تعظيم وجودها و الآخذ بها و هي كالأتي :

1- الانضمام إلى المعاهدات الدولية، التي تعمل على زيادة التعاون و التنسيق بين الجهود التي تبذلها في مجال مكافحة الانترنت .

2- إدخال تلك المعاهدات الدولية إلى حيز التنفيذ الفعلي، أي تنفيذ ما تنص عليه تلك الاتفاقيات من إجراءات دون أي إبطاء .

3- العمل على وجود أكبر قدر ممكن من التناسق و التطابق فيما بين قوانين الدول المختلفة و المتعلقة بمكافحة جرائم الانترنت، فلا يكون الفعل الذي تم ارتكابه جريمة في بلد ما و غير معاقب عليه في قانون بلد آخر، فمن هنا يجد المجرمون الملاذ الآمن الذين يلجؤون إليه دون أي اعتبار لما ارتكبوه من جرائم.

4- تعاون جميع الدول في تسليم المطلوبين امنيا، الى الدول التي تطالب بهم لارتكابهم جرائم الانترنت [2].

أضف إلى ما سبق، أن مسؤولية المجتمع الواحد لم تعد الدولة المعنية بهذا المجتمع قادرة على توفيرها في زمن العولمة، و عليه بات لزاما على كل مجتمع من المجتمعات، بل كل فرد و

---

[1] -Une étude a révélé récemment que près d'un tiers des entreprises dans les Émirats arabes unis a rapporté les attaques électroniques au cours des 12 derniers mois. L'étude a montré que les entreprises qui sont exposées attaques électroniques dans les EAU ont besoin entre deux semaines et un mois pour se remettre des effets de ces attaques, et plus de la moitié des personnes interrogées ne sont pas de savoir qu'ils sont ciblés par les cyber-criminels, alors que détient 50 pour cent de l'ensemble de ces dispositions spéciales pour les entreprises d'urgence dans l'éventualité d'une lettre d'attaque. Abdelaziz Derdouri.La Cyber Sécurité : Etat des lieux en Algérie
Cybersécurité|décembre 19, 2014 http: www.ssri.dz

[2]- محمد منير الجنيهي و ممدوح محمد الجنيهي، جرائم الانترنت و الحاسب الالي ووسائل مكافحتهما، دار الفكر الجامعي ،مصر،2004،ص 111و ما بعدها .

منظمة التعاون معا، في سبيل تحقيق امن المواطن أولا و من ثم المجتمع فالدولة، انطلاقا من قوله تعالى "و تعاونوا على البر و التقوى و لا تتعاونوا على الإثم و العدوان".[1]

المطلب الثاني : الاتفاقيات و المعاهدات الدولية و الاقليمية .

بات مؤكدا أن جرائم تكنولوجيا المعلومات هي جرائم عابرة للحدود، أي أنها لا تتم و تنتهي في أراضي دولة بعينها، وعليه فالتعاون الدولي هو من أهم سبل مكافحة جرائم الانترنت، و ملاحقة مرتكبيها، فبغير التعاون الدولي يزداد معدل ارتكاب تلك الجرائم و يطمئن مرتكبوها من عدم إمكانية ملاحقتهم، إذ يكون من السهل التنقل من دولة إلى أخرى تبيح القوانين السارية بها ارتكبوها من جرائم [2].

تعد المعاهدات الدولية التي تنضم إليها العديد من الدول هي النموذج الذي يكون هذا التعاون الدولي في ذلك المجال، و مثال ذلك أيضا التعاون الدولي بمؤتمر الأمم المتحدة السابع،

و الذي عقد عام 1985، لمنع الجريمة المنظمة، حيث اعتمد خطة عمل ميلانو، و التي اوصت بعد توصيات حيال التعامل مع الجريمة المنظمة و القضاء عليها.

ثم تبعه المؤتمر الثامن لمنع الجريمة بفترويلا عام 1990، فالمؤتمر الوزاري العالمي بالمعني بالجريمة المنظمة في نابولي بإيطاليا عام 1994، والذي عبر عن إدارة المجتمع الدولي بتعزيز التعاون الدولي و إعطاؤه الأولوية لمكافحة الجريمة المنظمة يضاف على ذلك، الإجتماع الإقليمي التحضيري و الذي عقد عام 1998، والذي تم فيه إقرار المبادئ التوجيهية لمنع الجريمة المنظمة و مكافحتها.

الفرع الأول: معاهدات لمكافحة الجريمة عموما:

حددت جملة من تدابير مكافحة الجرائم المتصلة بالحواسيب،في اطار مؤتمر الامم الحادي عشر لمنع الجريمة والعدالة الجنائية المنعقد في بانكوك في الفترة 18- 25 / 2005/4

[1]- جعفر حسن جاسم الطائي، المرجع السابق، ص 236.

[2] - For more about, the international solution see, Yaman Akdaniz, Clive Walker and David Wall (eds.), The I nternet, Law and Society, Longman Pearson Education, 2000, P. 12.

و الذي جاء من بين صفحاته ضرورة التعاون الدولي على المستوى القضائي لتخطي حدود الدولة الواحدة للتحقيق في الجريمة، و يمكن الاعتماد في مجال جرائم الانترنت على اختصاصات المنظمة الدولية للشرطة الجزائـــــــية ***interpol***، المنشأة بموجب المؤتر الدولي المنعقـــد في بروكســـل في الفترة من 6-1946/6/9 و الذي يقوم على مبادئ التعاون الأمني الدولي، بالنسبة ل 182 دولة عضو، لتقفي اثر المجرمين ومتابعة الجريمة، ومن الأمثلة على دور الانتربول في جرائم الانترنت،ما حصل في لبنان عندما تم توقيف احد الطلبة الجامعيين، من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصرة دون العاشرة من عمرها من موقعه على الشبكة، و ذلك اثر تلقي برقية من الانتربول في ألمانيا بهذا الخصوص وللمنظمة عدة مكاتب مركزية إقليمية في كل من: طوكيو ، نيوزيلندا، نيروبي ، أذربجان ، بيونس ايرس، لتسهيل مرور الرسائل.

و بانعقاد المجلس الأوروبي في لكسمبورج عام 1991،أنشأت الشرطة الأوروبية لملاحقة جناة الجرائم العابرة للحدود،و في نفس السياق أقام مجلس الوزراء العرب مكتب عربي للشرطة الجنائية يهدف لتنمية التعاون بين الشرطة العربية، ويعد إجراء تسليم المجرمين من أهم الإجراءات يدخل من جهة ضمن التعاون الدولي ومن جهة ساهم كثيرا في متابعة جناة جرائم المعلوماتية، والذي كان موضوع اتفاقيات دولية وإقليمية مثل اتفاقية الرياض لتعاون دول الخليج 1994،اتفاقية التعاون الأمني و تسليم المجرمين للمملكة العربية السعودية 1982،اتفاقية بين الجزائر و بلجيكا سنة1970،و الاتفاقية الأوروبية لتسليم المجرمين 1957.

الفرع الثاني : اتفاقية بودابست لمكافحة جرائم الانترنت2001 [1]:

شهدت العاصمة الماجرية بودابست،في أواخر عام 2001 أولى المعاهدات الدولية التي تكافح جرائم الانترنت. [2]

و مواكبة للتطور فقد ابرم المجلس الأوروبي اتفاقية ببوداست في 2001/11/8 ووضعت للمصادقة في 2001/11/23،و التي تضمنت التعريف بأهدافها،و وضعت قائمة للجرائم التي يجب على الدول المصادقة عليها ان تجرمها في قوانينها الداخلية .

وتعد الأولى في مجال مكافحة جرائم الانترنت و شملت العديد من جرائم الانترنت منها: الإرهاب، تزوير بطاقات الائتمان، دعارة الأطفال [3] وتعمد الاتفاقية إلى تنسيق القوانين الجديدة

---

[1] -Le 23 novembre 2001 les pays membres du Conseil de l'Europe ainsi que les États-Unis, le Canada, le Japon et l'Afrique du Sud, ont adopté la convention sur la cybercriminalité, aboutissement d'un long processus de négociations (vingt-sept versions antérieures et quatre années de négociations officielles). Il s'agit d'une convention pénale à vocation internationale destinée à lutter contre le cybercrime . En 2007, seuls 14 États avaient ratifié la convention sur les 47 signataires.

Par ailleurs en 2003, a été ouvert à la signature le protocole additionnel à la convention sur la cybercriminalité, qui visait à élargir le champ d'application de la convention aux infractions de propagande raciste ou xénophobe commis via les réseaux internet. Ce protocole, non ratifié par les États-Unis, prévoit par ailleurs des mesures facilitant l'extradition et l'entraide judiciaire.

La France a ratifié ces deux textes par la loi n° 2005-493 du 19 mai 2005 autorisant l'approbation de la Convention du Conseil de l'Europe sur la cybercriminalité et du protocole additionnel à cette Convention.

La convention sur la cybercriminalité de 2001 poursuit trois objectifs déterminés :

- l'harmonisation des législations des États signataires ;
- la modernisation de ces législations, notamment en matière procédurale ;
- l'amélioration de la coopération internationale en matière d'extradition et d'entraide répressive

[2]- جعفر حسن جاسم الطائي، المرجع السابق ،ص 227

[3] -la «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle :

a. un mineur se livrant à un comportement sexuellement explicite;

في دول عديدة، وجاءت نتيجة مشاورات طويلة بين الحكومات واجهزة الشرطة و قطاع الكمبيوتر، وصاغ نصها عدد من الخبراء في مجلس أوروبا بمساعدة عدة دول منها الولايات المتحدة.

كما تعد الاتفاقية الوحيدة المتعددة الأطراف المعنية بمكافحة الجرائم التي تتم باستخدام أو ضد الكمبيوتر و باستخدام شبكة الانترنت، و هي تمثل ركيزة أساسية منذ دخولها حيز النفاذ،في الأول من جويلية لعام 2004 [1]على مستوى الدول أعضاء مجلس الاتحاد الأوروبي

و كما سبق الإشارة، فلقد وقعت عليها العديد من الدول من غير أعضاء مجلس اوروبا مثل كندا و اليابان و جنوب إفريقيا، كما صادقت عليها الولايات المتحدة الأمريكية [2].

---

b. une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;
c. des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite, Convention sur la cybercriminalité, Budapest, 23.11.2001,Disponible sur:
conventions.coe.int/Treaty/fr/Treaties/Html/185. 23/11/2001.

- أما الفصل الخامس فيتضمن الأحكام الختامية ويضم المواد من 36 – 48 .

[1] -5 Ratifications incluant au moins 3 Etats membres du Conseil de l'Europe En 01/07/2004:

La Convention est le premier traité international sur les infractions pénales commises via l'Internet et d'autres réseaux informatiques, traitant en particulier des infractions portant atteinte aux droits d'auteurs, de la fraude liée à l'informatique, de la pornographie enfantine, ainsi que des infractions liées à la sécurité des réseaux. Il contient également une série de pouvoirs de procédures, tels que la perquisition de réseaux informatiques et l'interception.

- Son principal objectif, énoncé dans le préambule, est de poursuivre "une politique pénale commune destinée à protéger la société contre le cybercrime, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale".Détails du traité n°185 ,Convention sur la cybercriminalité,https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185.

[2] – للاطلاع على النص الكامل لاتفاقية الإجرام السيبيري، و لمعرفة مزيد من التفاصيل حول تطبيق هذه الاتفاقية، يرجى مراجعة الموقع الالكتروني الخاص بالمجلس الأوروبي .

- http://www.coe.int/t/e/legal-affairs/legal-co-operation.
- http://www.conventions.coe.int/treaty/EN/treaties/html/185.htm .

كما أن هذه الاتفاقية بمثابة دعوة موجهة إلى دول العالم[1] للتفاعل مع الانترنت جاءت نتيجة محاولات عديدة منذ ثمانيات القرن العشرين حتى ظهرت بشكلها النهائي في 2001/11/23 م،في بودابست وقعت عليها ثلاثون دولة أوروبية بما في ذلك الدول الأربعة من غير الأعضاء في المجلس الأوروبي، المشاركة في إعداد هذه الاتفاقية و في كندا و اليابان و جنوب أفريقيا و الولايات المتحدة الأمريكية .

و قد تضمنت هذه الاتفاقية الأقسام التالية:

1. القسم الأول: تحديد المصطلحات
2. القسم الثاني: الخطوات الواجب اتخاذها في إطار التشريع الوطني
3. القسم الثالث: التعاون الدولي
4. القسم الرابع: الشروط النهائية حول الانضمام إلى الاتفاقية

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

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

---

[1] - Budapest, 23/11/2001 - Traité ouvert à la signature des Etats membres et des Etats non membres qui ont participé à son élaboration et à l'adhésion des autres Etats non membres

[2] -*Titre 4 - Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes*

Article 10 - Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes, "Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle définie par la législation de ladite Partie, conformément aux

- المسؤولية الجنائية للأشخاص المعنوية[1] .

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

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

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

إن الانسجام ضروري بالنسبة إلى القوانين الأساسية، كما بالنسبة إلى القوانين الإجرامية و على كافة الدول إن تعيد تقييم و مراجعة قواعد الإثبات و التفتيش و إلقاء القبض و التنصت الالكتروني و ما شابه ذلك لتشمل المعلومات الرقمية و أنظمة الكمبيوتر الحديثة و أنظمة الاتصالات الحديثة و الطبيعة العالمية لشبكة الانترنت، أما التنسيق الأكبر للقوانين الإجرامية فيمكن أن يسهل التعاون في التحقيقات التي تشمل سلطات قطاعية متعددة .

إضافة إلى القوانين الملائمة من المهم أيضا تطور الحكومات و أجهزة تطبيق القانون، و قدراتها على تطبيق هذه القوانين يحتاج إلى تطوير الخبرات في مجال الجريمة التي ترتكب عبر

---

obligations que celle-ci a souscrites en application de la Convention universelle sur le droit d'auteur révisée à Paris le 24 juillet 1971, de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle" …,Convention sur la cybercriminalité, Budapest, 23.11.2001.

[1] –Article 12 – Responsabilité des personnes morales

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour faire en sorte que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, sur les bases suivantes: un pouvoir de représentation de la personne morale;
b. une autorité pour prendre des décisions au nom de la personne morale;
c. une autorité pour exercer un contrôle au sein de la personne morale. ..Convention sur la cybercriminalité, Budapest, 23.11.2001.

الشبكات الإلكترونية، و تحقيق مشاركة فعالة للمعلومات بين الدوائر داخل الدولة المعنية و بين مختلف الدول، يضاف إلى ذلك ضرورة تخطي هذه المشاركة الأجهزة التقليدية، لتطبيق القوانين بحيث تشمل أجهزة الأمن القومي و أجهزة الاستخبارات – كما أن من الأمور الأساسية تشكيل وحدات متخصصة في تطبيق القانون، للتعامل مع المسائل المتعلقة بهذا النوع من الجرائم على البلد المعني، بإمكان هذه الوحدات أيضا أن توفر أساسا للتعاون الدولي الرسمي و غير الرسمي، المستند إلى شبكات ثقة بين مسؤولي تطبيق القوانين في مختلف البلدان، ويمكن للتعاون في لجان مشتركة مؤلفة من ممثلي عدد من الدول أن يكون مفيدا جدا، و هناك قضايا كان فيها التعاون الدولي فعالا للغاية، بالفعل يمكن ان يولد التعاون الناجح تعاونا مماثلا في أماكن أخرى و يحقق المزيد من النجاح

و لقد جاء في اتفاقية الأوروبية للجرائم المعلوماتية الموقعة بتكليف من المجلس الأوروبي، و التي أبرمت لمساعدة الدول في مكافحة جرائم الانترنت، في مادتها 24[1] جملة من الأفعال التي يمكن أن يطبق بشأنها أسلوب تسليم المجرمين منها : الدخول غير المشروع، الاعتراض غير المشروع ، جرائم الإباحية و صور الأطفال الفاضحة .

كما تضمنت الاتفاقية جانب آخر من التعاون انصب هذه المرة حول تدريب أعوان الأمن، لإكسابهم خبرات عملية مثل ما ورد في التوصية الصادرة عن اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم المعلوماتية بدول مجلس التعاون الخليجي ، وما نص عليه البند "د" من القرار الصادر بشأن الجرائم ذات الصلة بالحاسب الآلي من مؤتمر الأمم المتحدة لمنع الجريمة و معاملة السجناء هافانا 1990،و قد اشترط في المتدرب خبرة لا تقل عن خمس سنوات في مجال تكنولوجيا المعلومات و إدارة الشبكات حتى يتمكن من تلقي تدريب متخصص، وهي عملية شملت الكثير من الأجهزة الأمنية عبر العالم مثل كندا و الجزائر التي أعدت برنامج لمدارس الأمن و الدرك الوطني و أرسلت قضاة للتدريب في الولايات المتحدة الأمريكية.

[1] – Convention sur la cybercriminalité ,Budapest, 23.11.2001.,*Titre 2 Principes relatifs à l'extradition* ,Article 24,Extradition ,Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère… Voir l'annexe n °1.

و تعد الولايات المتحدة الأمريكية، من الدول المتطورة تقنيا في مجال مكافحة الجرائم المعلوماتية والشبكات، وهي تساعد على تدريب أجهزة الشرطة و قضاة الدول الأخرى، بتمكينها من تعزيز قدراتها على ضبط مشاكل الجرائم الالكترونية، قبل أن تفلت منها زمام الأمور فقد أوجدت وزارة العدل الأمريكية مكتب للمساعدة و التدريب لتطوير أجهزة الادعاء العام في الدول الأخرى،و يعمل إلى جانبه البرنامج الدولي للمساعدة و التدريب (ICITAP)[1]لتوفير المساعدات لأجهزة الشرطة بالدول النامية .

ورغم وجود بعض العقبات التي تعرقل التعاون الدولي، مثل عدم وجود نموذج موحد للنشاط الإجرامي، فيجب إيجاد تشريعات داخلية تقرب وجهات النظر، حتى يأخذ التعاون مجراه مثل قانون حماية الملكية الفكريـــة، و الإجراءات الجزائية، التشفير...، و تساهم الاتفاقيات و الصكوك الصادرة عن منظمة الأمم المتحدة كثيرا في استخدام تقنيات خاصة للتخفيف من شدة اختلاف النظر القانونية مثل التسليم المراقب، المراقبة الالكترونيـــــــة و غيرها من أشكال المراقبة وهو ما أخذت به الجزائر في تعديلها لقانون الإجراءات الجزائية.

وقد تناولت الاتفاقية الأوروبية للإجرام المعلوماتي في مادتها 29 على سرية حفظ البيانات المعلوماتية المخزنة[2]، و حق كل طرف ان يطلب من الآخر الحفظ السريع للمعلومات المخزنة، عن طريق إحدى الوسائل الالكترونية الموجودة داخل النطاق المكاني للطرف الآخر، و التي ستكون محلا لطلب المساعدة من الطرف الأول، بغرض التفتيش أو الدخول، ضبط أو الكشف على البيانات المشار إليها، وهو الطلب الذي يجب الاستجابة إليه طبقا للمادة 30[3] من الاتفاقية،

---

[1] - ICITAP :International Criminal Investigative Training Assistance Program. https://www.allacronyms.com/ICITAP

[2] -Section 2– Dispositions spécifiques ,Titre 1 – Entraide en matière de mesures provisoires, Article 29 – Conservation rapide de données informatiques stockées
1. Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données, Convention sur la cybercriminalité, Budapest, 23.11.2001.

[3] - Article 30 – Divulgation rapide de données conservées
1. Lorsqu'en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie

وعلى المعني تقديم المساعدة للطالب على وجه السرعة، للكشف عن هوية مؤدي الخدمة و مصدر الاتصال، و قد أجازت اتفاقية المساعدة للدخول للبيانات المحفوظة طبقا للمادة31 [1] منها، وسمحت المادة 32 [2] من الاتفاقية بالدخول للبيانات المخزنة خارج نطاق الحدود بشرط وجود اتفاقيات أو أنها بيانات متاحة للجمهور .

وأقرت المادة 33 [3] وجوب تعاون الدول الأطراف، في حالة التجارة غير المشروعة،

---

requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de service et la voie par laquelle la communication a été transmise.
2. La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement :
a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou
b. si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels,Convention sur la cybercriminalité, Budapest, 23.11.2001.

[1] - Titre 2 – Entraide concernant les pouvoirs d'investigation ,Article 31 – Entraide concernant l'accès aux données stockées
1. Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, et de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29... ,Convention sur la cybercriminalité, Budapest, 23.11. 2001

[2] - Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public Une Partie peut, sans l'autorisation d'une autre Partie, :
a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou
b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique. ,Convention sur la cybercriminalité, Budapest, 23.11.2001

[3] - Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic
1. Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et procédures prévues en droit interne.
2. Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans

وركزت الاتفاقية في المادة 34 [1]على البيانات المتداولة بالاتصالات عبر الشبكة، و قد دعت الاتفاقية الدول الأعضاء لإنشاء نقطة اتصال، تعمل لمدة 24 ساعة لتامين المساعدة المباشرة للتحقيقات و استقبال الأدلة ذات الشكل الالكتروني.

و تثور مسالة الاختصاص في جرائم الانترنت، و التي تبقى رهينة إبرام اتفاقيات توحد نظريات الاختصاص و تتبنى نفس الإجراءات لحل هذا مشكل، ومواكبة الجريمة ،ولقد سمحت الاتفاقية للطرف في الحالات الطارئة طلب المساعدة القضائية الدولية عملا بالمادة 25 منها[2]،عن طريق وسائل الاتصال السريعة " فاكس ، بريد الكتروني... " والذي يتلقى الرد بنفس الطريقة[3].

une affaire analogue au niveau interne ,Convention sur la cybercriminalité, Budapest, 23.11.2001.

[1] - Article 34 – Entraide en matière d'interception de données relatives au contenu
Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique ,ainsi l' Article 35 – Réseau 24/7, Chaque Partie désigne un point de contact joignable 24 heures sur 24, sept jours sur sept, afin d'assurer la fourniture d'une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et données informatiques…,Convention sur la cybercriminalité, Budapest, 23.11.2001.

[2] -Article 25/3 ,Principes généraux relatifs à l'entraide ,Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris le cryptage si nécessaire), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication, Convention sur la cybercriminalité, Budapest, 23.11.2001.

[3]– يونس عرب، الاتجاهات التشريعية للجرائم الالكترونية، ورشة عمل " تطوير التشريعات في مجال مكافحة الجرائم الالكترونية " هيئة تنظيم الاتصالات / مسقط – سلطنة عمان 2-4 ابريل 2006 متاحة باللغة العربية على الموقع التالي:
http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime.

الفرع الثالث : الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

وقع وزراء الداخلية والعدل العرب على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[1] ،التي تهدف لتعزيز التعاون بين الدول الأعضاء ضد جرائم تقنية المعلومات، والتي تهدد أمنها وسلامة مجتمعاتها، وتهدف كذلك للأخذ "بالمبادئ الدينية والأخلاقية السامية، لاسيما أحكام الشريعة الإسلامية وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم."

وتعرف الاتفاقية تقنية المعلومات بأنها: "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها وتطويرها ومعالجتها وتبادلها، وفقاً للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكياً في نظام أو شبكة".

تتكون الاتفاقية من 43 مادة، منها 21 مادة في باب التجريم، وثمان مواد إجرائية تتعلق بحقوق السلطات جمع المعلومات وتتبع المستخدمين، وضبط المواد المخزنة على الحواسيب الشخصية والأجهزة التقنية والخدمية- السيرفرات- للأفراد والكيانات.

ويتضمن الفصل الرابع المكون من 14 مادة تنظيم التعاون بين الدول الأعضاء في تبادل معلومات المستخدمين، وإتمام الإجراءات القضائية والقانونية في التحقيق والاحتجاز[2].

وتطالب مواد الفصل الثاني من الاتفاقية الدول الموقعة عليها؛ بأن تقوم بإصدار قوانين تجرم عدد من الأفعال ومنها: "الدخول غير المشروع والاستمرار فيه مع كل أو جزء من تقنية

---

[1]- انضمت الجزائر إلى الاتفاقية العربية بموجب المرسوم الرئاسي رقم 252/14مؤرخ في 13ذي القعدة 1435الموافق ل 8 سبتمبر2014،يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ج.ر.ر57،ووقع عليها كل من وزير الداخلية و الجماعات المحلية دحو ولد قابلية ووزير العدل الطيب بلعيز وفي هذا المضمار أدخلت الجزائر عدة تعديلات على المنظومة القانونية الجزائرية منها ، قانون العقوبات الذي تمم العنصر الثالث من الباب الثاني من الكتاب الثالث من الأمر 156/66 بقسم سابع مكـــــرر عنوانه " المساس بأنظمة المعالجة الآلية للمعطيات " و يشمل المواد من 394 مكرر إلى 394 مكرر 7 ".قانون رقم 15-03 مؤرخ في 11 ربيع الثاني عام 1436 الموافق أوّل فبراير سنة 2015 يتعلق بعصرنة العدالة و قانون رقم 15 - 04 مؤرخ في 11 ربيع الثاني عام 1436 الموافق أوّل فبراير سنة 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني، القانون رقم 09-04 الذي تضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، مؤرخ في 14 شعبان عام 1430، الموافق 05 /08 /2009،ج.ر.ر رقم 47.

[2]- المادة 32: المساعدة المتبادلة، على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الالكترونية في الجرائم...

المعلومات"[1]. وهو ما فسره المشرع الجزائري، في تجريمه للدخول غير المصرح به لموقع إلكتروني، والاستمرار في الاتصال به لمدة غير مصرح بها[2]،من الجرائم الشائعة سرقة معلومات البطاقات الإلكترونية واستخدامها للشراء عبر الإنترنت .

كما تطالب الاتفاقية بتجريم حيازة برامج أو تقنيات "بنيِّة ارتكاب أي جريمة من الجرائم المبينة"، وتجرم ما تراه اعتداءً على حقوق الملكية الفكرية، وحقوق المؤلف المحمية بموجب قوانين الحماية الفكرية كالأفلام والموسيقى والكتب[3]، التي قد تكون ممنوعة لأسباب سياسية أو غيرها في بعض الدول، وخاصة دول العالم العربي التي تشهد رقابة نشطة على المطبوعات والسينما والمحتوى الفني والإبداعي .مما جعل ملفات التورنت[4] ومثيلاتها من تقنيات تبادل الملفات؛ مدخلاً لدى أغلب مستخدمي الإنترنت العرب للوصول للمحتوى الفني والمعرفي الذي تمنعه عنهم سلطات بلادهم.

---

[1]- المادة 6: جريمة الدخول غير المشروع.....

3. الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.
4. تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:
   - محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين.

الحصول على معلومات حكومية سرية

[2]- المواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات الجزائري .

[3]- المادة 17: الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة: انتهاك حق المؤلف كما هو معرف حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي، وانتهاك الحقوق المجاورة لحق المؤلف ذات الصلة كما هي معرفة قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي.

[4]- ملفات التورنت هي ملفات برمجية خفيفة، تسمح لمستخدمي الإنترنت بتبادل الملفات الخاصة بالأفلام والكتب والموسيقى، من خلال خوادم تربط بين أجهزتهم على شبكة الإنترنت.

وبموجب القوانين الجديدة المنبثقة عن الاتفاقية، يعد استخدام هذه الملفات وحيازتها جريمة يعاقب عليها القانون، كما جرمت الاتفاقية "الاستخدام غير القانوني لأدوات الدفع الإلكتروني[1]"، والإباحية [2] والطائفية وغيرها[3].

كما تجرم الاتفاقية استيراد أو شراء أو حيازة البرمجيات التي يمكنها فتح كلمات السر، أو الولوج للمواقع غير المصرح بدخولها، وهو ما يتصل بالبرمجيات التي تختبر تأمين المواقع وكشف الثغرات الأمنية للأنظمة وشبكات الاتصالات والتقنيات، مما يضع التقنيون المختصون في تأمين الشبكات والأنظمة تحت طائلة القانون[4].

---

[1]- المادة18:الاستخدام غير المشروع لأدوات الدفع الالكترونية:

4. كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الالكترونية بأي وسيلة كانت.
5. كل من استولى على بيانات أي أداة من أدوات واستعملها أو قدمها للغير أو سهل للغير الحصول عليها.
6. كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.

كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك.

[2]- المادة 12:جريمة الإباحية:

3. إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات.
4. تشدد العقوبة على الجرائم المتعلقة بإباحية الأطفال والقصر.

يشمل التشديد الوارد في الفقرة (2) من هذه المادة , حيازة مواد إباحية الأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات و المادة 13:الجرائم الأخرى المرتبطة بالإباحية ،المقامرة والاستغلال الجنسي.

[3]- المادة 4/15 : نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

[4]- المادة 9: جريمة إساءة استخدام وسائل تقنية المعلومات:

1. إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير:
   - أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة.
   - كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأية من الجرائم المبينة في المادة السادسة الى المادة الثامنة، يرجى مراجعة ملحق الرسالة رقم 2.
2. حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه , بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة ، يرجى مراجعة ملحق الرسالة رقم 2.

الفرع الرابع: إتحاد الشركات والكيانات الإقتصادية في مجال حماية أمنها الإلكتروني

تعد الكيانات الاقتصادية من أهم الأهداف المحتملة لأي عمليات إجرامية تتم عبر الانترنت، وغالبا ما يكون الهدف من ارتكاب تلك الجرائم، هو البحث عن أموال تلك الشركات الضخمة، أو عما تخفيه من معلومات تريد الشركات الأخرى الحصول عليها في محاولة منها للتغلب على ما عداد الشركات الاقتصادية الكبرى، والمتقدمة اقتصاديا بما يعود عليها من فوائد اقتصادية ضخمة، وعليه فغالبا ما تكون الشركات الاقتصادية هي الهدف السمين الذي يلهث وراؤه مرتكبي جرائم الانترنت .[1]

يضاف إلى ذلك، قد يكون الهدف من الجرائم التي تتعرض لها تلك الشركات الاقتصادية الضخمة، هي الحصول على معلومات هامة عنها القيام بابتزازها و الحصول منها، على مبالغ مالية في مقابل عدم نشر ما تم الاستيلاء عليه من معلومات في الغالب يكون نشرها ضارا بالشركة ضررا بالغا .

بناءا على ذلك، صار لزاما على العديد من الكيانات الاقتصادية الهامة في العالم، أن تتحد مع بعضها البعض في محاولة منها للقيام ببناء الحائط ضد الاعتداء الكتروني مضاد لها قد تتعرض له من هجمات، ومحاولات اختراق و قرصنة من محترفي ارتكاب الجريمة الأنترنتية، و مكاسب تلك الكيانات الاقتصادية عظيمة من تعاونها مع بعضها البعض في هذا الأمر، منها :

ان التعاون الذي يتم بينها و بين الكيانات الاقتصادية الأخرى، يوفر لها قدرا كبيرا من الأموال فيها لو كانت ستقوم ببناء هذا الحائط المضاد بمفردها، فعندها كانت ستحمل بمفردها ما يتكلفه من أموال دون أي مساعدة من اي جهة خارجية .

إن هذا الإتحاد يكون ائتلافا قويا في مواجهة تلك الهجمات التتارية على تلك الكيانات، و بالتالي يجعلها أقوى عند مواجهة تلك الاختراقات وصدها و تعقب مرتكبيها .

[1]- جعفر حسن جاسم الطائي، المرجع السابق، ص 237.

إن تعاون الشركات و عدم تحمل أي تكاليف منها بمفرده يجعلها تستطيع القيام ببناء حائط قوي و منيع في مواجهة مرتكبي جرائم الانترنت، وبالتالي يصعب كثيرا من فرص اختراقه و النفاذ إلى تلك الشركات .

فعليه نجد تعاون الكيانات الاقتصادية الكبرى في مجال مكافحة جرائم الانترنت، يساعد أخيرا على حماية أمنها من مخاطر التعرض لتلك الجرائم، ويحافظ عليها من اي محاولات ابتزاز تتعرض لها إذا ما استطاع أي شخص النفاذ إلى معلوماتها والحصول عليها، فعندئذ سيكون عليها أن تدفع له الكثير من الأموال لمنعه من نشر معلوماتها السرية، والتي تستفيد منها أية شركة منافسة لها في الأسواق العالمية، أو التي قد تضر بالشركة ضرار بليغا إذا ما تم نشر تلك المعلومات.[1]

الفرع الرابع: اتفاقية الاتحاد الأفريقي فيما يتعلق بمجال الأمن السيبراني وحماية البيانات الشخصية.

في جوان من عام 2014 وافق رؤساء الاتحاد الأفريقي (AU) على اتفاقية تاريخية، تؤثر على كثير من مناحي الحياة الرقمية[2].

هذه الاتفاقية تغطي نطاق واسع جدا من الأنشطة على الإنترنت، مُتضمن التجارة الإلكترونية، وحماية البيانات، والجرائم الإلكترونية، مع تركيز خاص على العنصرية وكراهية الأجانب، واستغلال الأطفال في المواد الإباحية، والأمن السيبراني الوطني، إن نفذت هذه الاتفاقية، فإن العديد من الدول الإفريقية ستسن قوانين لحماية البيانات الشخصية لأول مرة، مُؤيَدة من قبل سلطات عامة جديدة ومستقلة. وهي تحركات من شأنها أن تُمثل هدية كبيرة لسيطرة المستخدم على البيانات الشخصية بالإضافة إلى أنه سيُطلب من كل دولة وضع إستراتيجية وطنية للأمن السيبراني، وتمرير قوانين الجرائم الإلكترونية، والتأكد من أن التجارة الإلكترونية ""تُمارس بحرية".

[1] – الشبكة القانونية العربية، فرع القانون، جرائم الكمبيوتر و الانترنت، منشور على الرابط التالي:
arab@wnetlawsubjects-26/05/2015.

[2] - La Convention de l'Union Africaine (UA) sur la Cybersécurité et la protection des données à caractère personnel a été finalement adoptée par la 23ème Session Ordinaire de la Conférence de l'Union qui s'est tenue le 27 juin à Malabo, République de la Guinée Equatorial

في قارة تُعرف أنها تَثِب من التكنولوجيا السلكية نحو الاتصال عبر الجوال، تمثل هذه الاتفاقية قفزة إلى الأمام في تنظيم الإنترنت، هذا التغيير لن يحدق عشية وضحاها وذلك لأن الاتفاقية يجب أن يُصدّق عليها من قبل 15 دولة لتدخل حيز التنفيذ، وحتى ذلك الحين فمن المرجح أن يكون هناك بضعة سنين قبل أن تمرر 54 حكومة إفريقية القوانين التي تُنفذ هذه الاتفاقية.

الخطوط العريضة للاتفاقية [1]:

- جزء كبير من الاتفاقية تعكس إطار حماية البيانات واللغة التي طُورت بواسطة الاتحاد الأوروبي، وبما أن الاتحاد الأوروبي راعى الإصلاح الشامل من خلال تنظيم حماية البيانات، فإنه ينبغي على المُشرعين اعتبار مثل هذه الاتفاقية كواحدة من أمثلة ''وضع المعايير'' التي تُجسد أغلب عملهم.
- في الاتفاقية، يُطلب من كل دولة عضو بالاتحاد الأفريقي أن يكون لها سلطة حماية البيانات الوطنية –مسؤول مُستقل لضمان أن البيانات الشخصية تُعالج وفقا لأحكام الاتفاقية– وأن يتم معالجة البيانات فقط في غرض مشروع، بينما لم يتم إعطاء تعريف للغرض المشروع.
- كما يُطلب أيضا من الدول الأعضاء، أن يكون معالجة وحفظ البيانات مُحدد بالوقت اللازم للغرض الذي تم جمعها أو معالجتها من أجله، مع وجود استثناءات لـــ ''المصلحة العامة، خاصة للأغراض التاريخية، أو الإحصائية أو العلمية.''
- حددت الوثيقة حق الفرد في الاعتراض على المعالجة التي تُضاف للبيانات، وهو ما يمكن أن يمثّل دعما المستخدمين، لكن ليس من الواضح ما هي ''الأغراض المشروعة'' التي يُمكن أن تُثير اعتراضات (المادة 18).
- كما أنه لأول مرة، أصحاب البيانات لهم الحق في إخبارهم، قبل أن يتم مشاركة البيانات الخاصة بهم مع أطراف ثالثة (المادة 18)[2].

---

1 -https://www.accessnow.org/african-union-adopts-framework-on-cyber-security-and-data-protection/

2 -Article 18: Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

- بموجب الاتفاقية، مطلوب من كل دولة من الدول الأعضاء، أن تضع إطارا قانونيا لحماية ‘‘البيانات المادية’’ ، بينما لم يتم تحديد ما هي "البيانات المادية" في أي مكان بالاتفاقية، وتُرك الاختلاف بشأن تحديد نطاق وجوهر المعايير القانونية التي يتعين طرحها من الدول.

الدول الأعضاء في الاتحاد الأفريقي، مُكلّفون باستحداث سلطات حماية البيانات، بينما على أطراف الاتفاقية من أعضاء الحكومة ورجال الأعمال، وحتى المساهمين في شركات تكنولوجيا المعلومات والاتصالات، المشاركين في سلطة حماية البيانات أن يعززوا استقلال هذه الهيئة، علاوة على بلورة المزيد من المبادئ التوجيهية في عملية اختيار الأعضاء، لضمان الشفافية والاستقلال بالكامل على حد سواء.

- الأمن السيبراني وحقوق الإنسان : أقسام الأمن السيبراني –على الأخص– في الاتفاقية تحمي حقوق الإنسان، يجب على الحكومات أن تكفل ‘‘الميثاق الأفريقي لحقوق الإنسان والشعوب وغيرها من الحقوق الأساسية الأخرى مثل حرية التعبير والحق في الخصوصية والحق في محاكمة عادلة في القوانين الجديدة، من بين أمور أخرى ‘‘(المادة 25 /3)[1].

-Elle a le droit, d’une part, d’être informée avant que des données la concernant ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et, d’autre part, de se voir expressément offrir le droit de s’opposer, gratuitement, à ladite communication ou utilisation. Instrument Juridique de l’Union Africaine.

[1] Article 25 - 3Droits des citoyens : En adoptant des mesures législatives et/ou réglementaires en matière de cyber sécurité ou en créant le cadre d'application de celle-ci, chaque État Partie veillera à ce que les mesures adoptées n'entravent pas les droits des citoyens garantis en vertu de la constitution nationale, droits internes et protégés par les conventions internationales, particulièrement la Charte africaine des droits de l'Homme et des Peuples, ainsi que les droits fondamentaux tels que le droit à la liberté d'expression, le droit au respect de la vie privée et le droit à une instruction équitable, entre autres. Instrument Juridique de l’Union Africaine.

علاوة على ذلك، تم تضمين المجتمع المدني صراحة، كجزء من أصحاب المصلحة، والشركات من القطاعين العام والخاص(المادة 26 /3)[1]، وثقافة الأمن السيبراني (المادة 26/ 1)[2].

قواعد الأمن السيبراني أيضا تدعم سيادة القانون: تَصر الاتفاقية على أن توقّع الحكومات اتفاقيات المساعدة القانونية المتبادلة، لوضع معايير التبادل الدولي للبيانات بطريقة فعالة (المادة 28 /2)[3].

الأهم من ذلك، يجب على الدول الأعضاء، تمرير القوانين التي تحمي أمن البيانات وإعلام المستخدمين عن المخاطر التي تتعرض لها ببياناتهم (المادة 29)[4] ونقلها لأطراف ثالثة (المادة18)، وهو البند الذي ينبغي أن يُطبق على خرق البيانات والتحويلات غير قانونية[5].

و مع تشجيع الشراكات العامة / الخاصة في مجال الأمن السيبراني.

---

[1] - Article 26/3 : Système national de la cyber sécurité, Partenariat Public-Privé

Chaque État Partie s'engage à développer un partenariat public-privé en tant que modèle afin d'engager l'industrie, la société civile et le monde universitaire dans la promotion et le renforcement d'une culture de la cyber sécurité. Instrument Juridique de l'Union Africaine

[2] -Article 26/1 : Système national de la cyber sécurité

Chaque État Partie s'engage à promouvoir la culture de la sécurité chez toutes les parties prenantes – gouvernements, entreprises et société civile
– qui développent, possèdent, gèrent, mettent en service et utilisent les systèmes et les réseaux d'information. La culture de la sécurité devra mettre l'accent sur la sécurité dans le développement des systèmes et des réseaux d'information et sur l'adoption de nouvelles façons de penser et de se comporter lors de l'utilisation des systèmes d'information et lors des communications ou des transactions à travers les réseaux... Instrument Juridique de l'Union Africaine

[3] -Article 282/ : Coopération internationale ,Entraide judiciaire

Les États Parties qui n'ont pas de conventions d'assistance mutuelle en matière de cybercriminalité s'engagent à encourager la signature des conventions d'entraide judiciaire en conformité avec le principe de la double incrimination tout en favorisant les échanges d'informations ainsi que le partage efficient des données entre les organisations des États membres sur une base bilatérale et multilatérale, Instrument Juridique de l'Union Africaine

[4] - Voir l'annexe n ° 3

[5] - http://www.moeltaher.net

تَحظر الاتفاقية استخدام الحاسوب في ''إهانة'' شخص ما لأسباب العرق أو اللون أو الأصل القومي/العرقي أو الدين أو الرأي السياسي. و لم تُعرّف الوثيقة ''الإهانة'' إطلاقا، وتُرك هذا الحكم الغير موضوعي لتجريم الخطاب بدلا من العمل الإجرامي. بالتزامن مع هذا الحكم الذي لا يرفض الموافقة عمدا أو نفيا أو تبريرا للأفعال'' التي تشكل جريمة الإبادة الجماعية أو الجرائم ضد الإنسانية'' هذه الأحكام غير مدروسة وضارة وستخدم فقط الحد من حرية التعبير وتثبط التعبير على الإنترنت.

وأخيرا، تمنح الاتفاقية صلاحيات واسعة للمحاكم للوصول إلى قواعد البيانات وإجراءات مراقبة الشبكات إذا كان ذلك ''مفيدا في كشف الحقيقة'' وهو ما يبدو غامضا، إذا كان شرط النية الحسنة مفتوح لسوء الاستخدام.

أجرى الاتحاد الأفريقي مسح شامل للأحكام ذات الصلة بقانون الاتصالات الحديث، واتُخذت في مشروع إصلاحي طموح بهذه الاتفاقية،لكن المعاهدة ستأخذ وقت طويل للتنفيذ.

فيجب على برلمانات 15 دولة من الدول الأعضاء(54 دولة) أن تُشير إلى الاتفاقية في أحكامها، ثم يجب أن تُمرر القوانين المنفذة للمعاهدة في كل دولة من الدول الأعضاء وتُنشر على الإنترنت.[1]

الفرع السادس: الصعوبات التي تواجه التعاون الدولي في مجال الحماية المعلوماتية.

التعاون الدولي بكافة صوره في مجال مكافحة ومواجهة الجرائم المتعلقة بشبكة الإنترنت[2]، وإن كان يعد مطلبا تسعى إلى تحقيقه أغلب الدول إن لم يكن كلها، إلا أنه ثمة صعوبات ومعوقات تقف دون تحقيقه أهمها :

---

[1] - Mouhamadou Lo, Président de la CDP au Sénégal ,La Convention de l'Union Africaine sur la cybersécurité et la protection des données, ouverte à la ratification,30/07/2014

:http://www.afapdp.org/archives/2701

[2] – حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، الإتحاد العربي للتحكيم الإلكتروني، 2007، ص 15 و ما بعدها، انظر كذلك، غانم مرضي الشمري، الجرائم المعلوماتية ماهيتها- خصائصها، كيفية التصدي لها، دار الثقافة للنشر و التوزيع، الأردن، 2016، ص 124و ما بعدها .

البند الأول: عدم وجود نموذج موحد للنشاط الإجرامي.

بنظرة متأنية للأنظمة القانونية القائمة، في الكثير من الدولة لمواجهة الجرائم المعلوماتية ومنها الجرائم المتعلقة بشبكة الإنترنت، يتضح لنا من خلالها عدم وجود اتفاق عام مشترك بين الدول، حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مباحا في أحد الأنظمة قد يكون مجرّما وغير مباح في نظام آخر، ويمكن إرجاع ذلك إلى عدة أسباب وعوامل كاختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لآخر، وبالتالي اختلاف السياسة التشريعية من مجتمع لآخر. [1]

البند الثاني: تنوع واختلاف النظم القانونية الإجرائية

بسبب تنوع واختلاف النظم القانونية الإجرائية، يتبين أن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما، قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها .

كما هو الحال بالنسبة للمراقبة الإلكترونية، والتسليم المراقب، والعمليات المستترة، وغيرها من الإجراءات الشبيهه، فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى، وبالتالي فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنقاذ القانون في الدولة الأخرى، على استخدام ما تعتبره هي أنه أداة فعّالة، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية، قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق تري هذه الدولة أنها طرق غير مشروعة، حتى وإن كان هذا الدليل تم الحصول عليه في اختصاص قضائي وبشكل مشروع.

البند الثالث :عدم وجود قنوات اتصال.

أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة والمجرمين، الحصول على المعلومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لزاما أن يكون هناك نظام اتصال، يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية، لجمع أدلة معينة أو معلومات مهمة، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العملية، التي

[1] – عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة،2002، ص102.

غالبا ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين، وبالتالي تنعدم الفائدة من هذا التعاون[1].

البند الرابع: مشكلة الاختصاص في الجرائم المتعلقة بالإنترنت.

الجرائم المتعلقة بالإنترنت، من أكبر الجرائم التي تثير مسألة الاختصاص على المستوى المحلى أو الدولي، ولا توجد أي مشكلة بالنسبة للاختصاص على المستوى الوطني أو المحلى حيث يتم الرجوع إلى المعايير المحددة قانونا لذلك.

ولكن المشكلة تثار بالنسبة للاختصاص على المستوى الدولي، حيث اختلاف التشريعات والنظم القانونية والتي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المتعلقة بالإنترنت، التي تتميز بكونها عابرة للحدود، فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استنادا إلى مبدأ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبيه، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى، فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية ،كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي، من إقليم دولة معينة وتم الإطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة.

البند الخامس: التجريم المزدوج

التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين، [2] فهو منصوص عليه في أغلب التشريعات الوطنية والصكوك الدولية المعنية بتسليم المجرمين، وبالرغم من أهميته تلك، نجده عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية سيما وأن معظم الدول لا تجرم هذه الجرائم، بالإضافة إلى أنه من الصعوبة أن نحدد فيما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم المتعلقة بشبكة الإنترنت

[1]- جميل عبد الباقي الصغير، المرجع السابق، ص 73.

[2]-غانم مرضي الشمري، المرجع السابق، ص 126 و ما بعدها .

أو لا، الأمر الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم المتعلقة بالإنترنت[1].

البند السادس: الصعوبات الخاصة بالمساعدات القضائية الدولية:

نعلم أن الأصل بالنسبة لطلبات الإنابة القضائية الدولية، والتي تعد من أهم صور المساعدات القضائية الدولية، في المجال الجنائي أن تسلم بالطرق الدبلوماسية وهذا بالطبع يجعلها تتسم بالبطء والتعقيد، والذي يتعارض مع طبيعة الإنترنت وما تتميز به من سرعة، وهو الأمر الذي انعكس على الجرائم المتعلقة بالإنترنت.

كذلك من الصعوبات الكبيرة في مجال المساعدات القضائية الدولية المتبادلة، التباطؤ في الرد، حيث أن الدولة متلقية الطلب غالبا ما تكون متباطئة في الرد على الطلب، سواء بسب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية، أو الفوارق في الإجراءات التي تعقد الاستجابة وغيرها من الأسباب، فكم هو محبط شطب قضية لعدم تلبية طلب بسيط في الوقت المناسب.

البند السابع: الصعوبات الخاصة بالتعاون الدولي في مجال التدريب

تتمثل في عدم رغبة بعض القيادات الإدارية في بعض الدول[2] في التدريب لاعتقادهم بدوره السلبي، في تطوير العمل من خلال تطبيق ما تعلمه المتدربون في الدورات التدريبية، وما اكتسبوه من خبرات، ومن الصعوبات أيضا والتي قد تهدد التعاون في مجال التدريب، ما يتعلق بالفوارق الفردية بين المتدربين وتأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة، و متكافئة لدي مختلف الأفراد المتدربين، سيما في مجال تكنولوجيا المعلومات وشبكات الاتصال حيث أنه يوجد بعض الأشخاص ممن لا يعي في هذا المجال شيء، وعلى النظير يوجد أناس على درجة كبيرة من المعرفة والثقافة في هذا المجال.

[1] – جميل عبد الباقي الصغير، المرجع السابق ، ص 91.

[2] – غانم مرضي الشمري، المرجع السابق ، ص 115و ص 127 .

بالإضافة إلى أن نظرة المتدرب إلى الدورة التدريبية، على أنها مرحلة تدريبية أو عبء لا طائل منه تهدد العملية التدريبية برمتها، وبالطبع نسف التعاون الدولي في هذا المجال .

أيضا من الصعوبات التي قد تؤثر على العملية التدريبية، وعلى التعاون الدولي فيها ما يتعلق بالملامح العامة المميزة للبيئة التدريبية، وعدم قدرتها على تمثيل الواقع العملي لبيئة العمل الطبيعية تمثيلا تاما ومتقنا، من حيث ما يدور بها من وقائع وملابسات وإجراءات، وما يتم فيها من نشاطات لا تبلغ حد التطابق مع طبيعة المهام التي سيؤديها المتدربون في بيئة العمل الطبيعية.

الفرع السابع : كيفية القضاء على الصعوبات التي تواجه التعاون الدولي

فيما يتعلق بالعقبة الأولى المتمثلة في عدم وجود نموذج موحد للنشاط الإجرامي، فإن الأمر يقتضي توحيد هذه النظم القانونية، ولاستحالة هذا الأمر فإنه لا مناص من البحث عن وسيلة أخرى، تساعد على إيجاد تعاون دولي يتفق مع طبيعة هذا النوع المستحدث من الجرائم، ويخفف من غلو الفوارق بين الأنظمة العقابية الداخلة، وتتمثل هذه الوسيلة في تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية، وإبرام اتفاقيات خاصة يراعي فيها هذا النوع من الجرائم[1]

وبالنسبة للمعوقة الثانية والخاصة بتنوع واختلاف النظم القانونية الإجرائية، نجد أن الصكوك الدولية الصادرة عن الأمم المتحدة، غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة، الشيء الذي يخفف من غلو واختلاف النظم القانونية والإجرائية، ويفتح المجال أمام تعاون دولي فعّال، فمثلا المادة 20 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، تشير في هذا الصدد إلى التسليم المراقب ، والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة[2]، والتي تعتبر من أهم التقنيات المستخدمة في التصدي للجماعات الإجرامية المنظمة المحنكة، بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها وتجميع المعلومات، وأدلة الإثبات لاستخدامها فيما بعد في

[1] – من الأمثلة على التشريعات المعنية بالجرائم المعلوماتية، حماية البيانات والخصوصية، القانون الجنائي، حماية الملكية الفكرية ، الحماية من المضمون الضار ،قانون الإجراءات الجزائية، التشفير والتوثيقات الرقمية، أنظر:

ULRICH SIEBER ,Legal Aspects of Computer, Related Crime in the Information Society, Com crime Study , 1/01/1998.

[2] – المادة 11 من اتفاقية 1988 بشأن التسليم المراقب، والمادة 50 من اتفاقية الأمم المتحدة لمكافحة الفساد.

الملاحقات القضائية المحلية، منها أو الدولية في دول أطراف في سياق نظم المساعدة القانونية المتبادلة[1].

وهذا ما أكدت عليه الاتفاقية الأوربية للإجرام المعلوماتي في موادها من 29 الى 34 المشار اليها انفا، للحد من ظاهرة عدم وجود قنوات اتصال بين جهات إنفاذ القانون، فنلاحظ أنه غالبا ما تشجع الصكوك الدولية الدول إلى التعاون فيما بينها وتدعوها إلى إنشاء قنوات اتصال بين سلطاتها المختصة، ووكالاتها ودوائرها المتخصصة، بغية التيسير في الحصول على هذه المعلومات وتبادلها [2].

ومن الأمثلة على هذه الصكوك الدولية:

- المادة 48 من اتفاقية الأمم المتحدة لمكافحة الفساد[3].

---

[1] – راجع في ذلك الأدلة التشريعية، لتنفيذ اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبرتوكولات الملحقة بها (منشورات الأمم المتحدة رقم المبيع (E.O.5.V2) الجزء الأول – الفقرة 384.

[2] – أنظر ما جاء بتوصية المجلس الأوربي رقم (R95)13 الصادرة في 1999/09/11م بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات.

[3] - Article 48 :Coopération entre les services de détection et de répression:

- Les États Parties coopèrent étroitement, conformément à leurs systèmes juridiques et administratifs respectifs, en vue de renforcer l'efficacité de la détec- tion et de la répression des infractions visées par la présente Convention. En particulier, les États Parties prennent des mesures efficaces pour:

a) Renforcer les voies de communication entre leurs autorités, organis mes et services compétents et, si nécessaire, en établir afin de faciliter l'échange sûr et rapide d'informations concernant tous les aspects des infractions visées par la présente Convention, y compris, si les États Parties concernés le jugent approprié, les liens avec d'autres activités criminelles

b) Coopérer avec d'autres États Parties, s'agissant des infractions visées par la présente Convention, dans la conduite d'enquêtes concernant les points suivants:

1- Identité et activités des personnes soupçonnées d'implication dans lesdites infractions, lieu où elles se trouvent ou lieu où se trouvent les autres personnes concernées;

2- Mouvement du produit du crime ou des biens provenant de la commission de ces infractions;

3- Mouvement des biens, des matériels ou d'autres instruments utilisés ou destinés à être utilisés dans la commission de ces infractions ,la Convention des Nations Unies contre la corruption, NATIONS UNIES , New York, November 2004.

- البند الثاني من المادة 27 من الاتفاقية الأوربية بشأن الإجرام المعلوماتى[1].

- المادة35 من ذات الاتفاقية الأوربية والتي أوجبت على الدول الأطراف فيها ضرورة تحديد نقطة اتصال تعمل لمدة 24 ساعة يومياً طوال أيام الأسبوع لكي تؤمن المساعدة المباشرة للتحقيقات المتعلقة بجرائم البيانات والشبكات، أو استقبال الأدلة ذات الشكل الإلكتروني[2].

- أما بالنسبة لمشكلة الاختصاص في الجرائم الإنترنتية فثمة حاجة ملحة إلى إبرام اتفاقيات دولية ثنائية كانت أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي خاصة بالنسبة للجرائم المتعلقة بالإنترنت[3]بالإضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرائية بما يتناسب والتطور الكبير التي تشهده تكنولوجيا المعلومات والاتصالات [4].

- وتطبيقاً للقواعد التي تحكم الاختصاص المكاني، فإن جرائم الإنترنت العابرة للحدود *Transnational Crimes* تخضع في كثير من الأحيان لأكثر من قانون، فإذا وقع السلوك في نطاق بلد معين والآثار الضارة تحققت في نطاق بلد آخر، فإن كلا البلدين يكون

---

[1] - Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables.
2. a. Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution;
b. les autorités centrales communiquent directement les unes avec les autres;
c. chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe;
d. le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.

[2] - Article 35 – Réseau 24/7
Chaque Partie désigne un point de contact joignable 24 heures sur 24, sept jours sur sept, afin d'assurer la fourniture d'une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et données informatiques ou pour recueillir les preuves ,Conseil de l'Europe - Convention sur la cybercriminalité (STE n° 185).

[3] – علي سبيل المثال 22 من الاتفاقية الأوربية بشأن الإجرام المعلوماتى.

[4] – R. Vouin et J. Léauté, droit pénal et procédure pénale, 2 me éd., Paris, 65, P 19 .

قانونه واجب التطبيق على الواقعة ، بمعنى أنه يتم تطبيق قانون كل دولة تحقق في نطاقها أحد عناصر الركن المادي للجريمة (السلوك أو النتيجة)، فيكفي ليكون قانون البلد واجب التطبيق،تلقي الضحية الرسالة الإلكترونية المجسدة لجريمة السبّ أو التهديد مثلاً في نطاقه ولو كان الفعل ذاته غير معاقب عليه في بلد المنشأ .

– وبتطبيق ذلك على جريمة نسخ المصنفات ينعقد الاختصاص للدولة،التي تم فعل النسخ على إقليمها، باعتبار أن النسخ عن بعد يعد أحد العناصر المكونة لجريمة التقليد.

– وثمة أمر آخر يزيد الأمر تعقيداً وصعوبة في تحديد الاختصاص في جرائم

الإنترنت عبر الوطنية بالذات ألا وهو تباين المعايير الوطنية،فيما يتعلق بتحديد الاختصاص، الأمر الذي يفضي عادة إلى حدوث تنازع في الاختصاص بشأن هذه الطائفة من الجرائم[1] .

– فعلى سبيل المثال، لو أن شخصاً ارتكب أياً من هذه الجرائم،على إقليم دولة لا يحمل جنسيتها، فقد يحدث التنازع بين قانون الدولة التي ارتُكِبت الجريمة على إقليمها وقانون الدولة التي ينتمي إليها.

– أي أن الفعل يتنازعه قانونان، قانون دولة الإقليم على أساس مبدأ الإقليمية، وفي

الوقت ذاته قد يخضع لقانون دولة الجاني عملاً بمبدأ الشخصية الإيجابية، ليس هذا فحسب، بل قد ينعقد الاختصاص لدولة ثالثة متى كانت الجريمة ماسّة بمصالحها الحيوية وفقاً لمبدأ العينية[2].

– وحتى على فرض إمكانية إيجاد حل لهذه المشكلة من الزاوية القانونية، فإنها تظل تصطدم بعقبات عملية بالنظر إلى الإجراءات المعقدة والطويلة،التي يلزم اتباعها لمحاكمة الجاني الذي ارتكب أياً من هذه الجرائم، وكانت إقامته خارج البلد الذي تتم فيها محاكمته، والأمر ينسحب أيضاً على تنفيذ الأحكام الصادرة بالخارج، ومن العوائق في ذلك مبدأ عدم جواز محاكمة الشخص عن الفعل الواحد مرتين، وكذلك عدم جواز تسليم الوطنيين .

---

[1]– موسى مسعودة أرحومة، الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية و القانون، أكاديمية الدراسات العليا،طرابلس،28-2009/10/29، ص 17 .

[2]– موسى مسعودة أرحومة، المرجع السابق، ص 18.

-وصفوة القول، إن جرائم الإنترنت عبر الوطنية، لا تحدّها حدود خلافاً للجرائم التقليدية المعروفة، الأمر الذي يجعلها في كثير من الأحيان تستعصي على الخضوع للقوالب القانونية،التي تحكم مسألة الاختصاص المكاني، ومن ثَم، فإن الطبيعة الخاصة لهذا الصنف من الجرائم المستحدثة،تتطلب تجاوز القوالب والمعايير التي طرحها الفقه للتغلب على مشكلة تنازع الاختصاص، والعمل على تبني حلول أكثر مرونة تأخذ في الحسبان النطاق الجغرافي لهذه الجرائم،وسهولة ارتكابها وآلية اقترافها والتخلص من آثارها وما إلى ذلك من اعتبارات يفرضها الطابع التقني المتطور لها .

وهذا بطبيعة الحال، ينبغي ألاّ يُترك لمحض اجتهادات الفقه والقضاء، وإنما يلزم تدخل المشرع لتحديد معايير الاختصاص التي يفترض عدم تضييق نطاقها[1].

ولأجل القضاء على مشكلة التجريم المزدوج، والذي يعد من أهم الشروط الخاصة بنظام تسليم المجرمين، ركزت الاتجاهات والتطورات التشريعية الخاصة بتسليم المجرمين، على تخفيف التطبيق الصارم لهذا الشرط، وذلك بإدراج أحكام عامة في المعاهدات والاتفاقيات المعنية بتسليم المجرمين، وذلك إما بسرد الأفعال والتي تتطلب أن تجرم كجرائم أو أفعال مخلة بمقتضي قوانين الدولتين معا أو بمجرد السماح بالتسليم لأي سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة.

وفيما يتعلق بالصعوبات الخاصة بالمساعدات القضائية الدولية، والتباطؤ في الرد فإنه الحاجة تزداد ملحة إلى إيجاد وسيلة أو طريقة، تتسم بالسرعة تسلم من خلالها طلبات الإنابة، كتعين سلطة مركزية مثلا أو السماح بالاتصال المباشر بين الجهات المختص، في نظر مثل هذه الطلبات لنقضي على مشكلة البطء والتعقيد في تسليم طلبات الإنابة، وهذا بالفعل ما أوصي به مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية والذي انعقد في بانكوك في الفترة

[1]- موسى مسعودة أرحومة ، المرجع السابق ،ص 20.

من 18-2005/4/25م[1]،حيث أكد على ضرورة تعزيز فعالية السلطات المركزية المعنية، في أعمال المساعدة القانونية المتبادلة وإقامة قنوات مباشرة للاتصال فيما بينها بغية ضمان تنفيذ الطلبات في الوقت المناسب، ونفس الشيء نجده في البند الثاني من المادة 27 من الاتفاقية الأوربية بشأن الإجرام المعلوماتي. والمادة35 من ذات الاتفاقية الأوربية، والتي أوجبت على الدول الأطراف فيها ضرورة تحديد نقطة اتصال تعمل لمدة 24 ساعة يومياً طوال أيام الأسبوع،لكي تؤمن المساعدة المباشرة للتحقيقات المتعلقة بجرائم البيانات والشبكات، أو الاستقبال الأدلة في الشكل الإلكتروني عن الجرائم .كما أوجبت ذات المادة على الدول الأطراف، ضرورة أن تتمكن نقطة الاتصال من الاتصال السريع بنقطة اتصال الطرف الآخر، وأن يعمل كل طرف على أن يتوافر لديه الأفراد المدربين القادرين على تسهيل عمل الشبكة.

أما بالنسبة للرد على طلبات التماس المساعدة، فإنه من الضرورة بمكان الاستجابة الفورية والسريعة على هذه الطلبات، لأجل ذلك تنص غالبية المعاهدات والاتفاقيات الخاصة بالمساعدات القضائية المتبادلة، على ضرورة الاستجابة الفورية والسريعة على طلبات التماس المساعدة، وهذا ما أكدت عليه الفقرة الثالثة من المادة 25 [2]من الاتفاقية الأوربية للإجرام المعلوماتي، حيث نصت على أنه " يمكن لكل طرف، في الحالات الطارئة أن يوجه طلباً للمعاونة أو للاتصالات المتعلقة بها عن طريق وسائل الاتصال السريعة مثل الفاكس أو البريد الإلكتروني، على أن تستوفي هذه الوسائل الشروط الكافية المتعلقة بالأمن وصحتها،(ويدخل ضمن ذلك الكتابة السرية إذا لزم

[1] - Onzième Congrès des nations Unies "synergies et réponses: alliances stratégiques pour la prévention du crime et la justice pénale" Bangkok (thaïlande)
18-25 avril 2005 ,Le onzième Congrès a adopté la Déclaration de Bangkok, document politique fondamental qui jette les bases de l'intensification de la coopération et de la concertation internationales et montre la voie à suivre pour prévenir la criminalité et la combattre.

[2] - Article 25 – Principes généraux relatifs à l'entraide
Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris le cryptage si nécessaire), avec confirmation officielle ultérieure si
l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

الأمر) مع تأكيد رسمي لاحق إذا اقتضت الدولة المطلوب منها المساعدة في ذلك، وتقوم الدولة بالموافقة على هذا الطلب والرد عليه عن طريق إحدى وسائل الاتصال السريعة.

أما فيما يتعلق بالصعوبات التي تواجه التعاون الدولي في مجال التدريب، فإنه يمكن التغلب عليها بإجراء المزيد من الحملات التوعوية، للتنبيه بمخاطر الجرائم المعلوماتية والأضرار التي تسببها وبأهمية تدريب رجال العدالة الجزائية على مواجهتها، كما أنه وبمزيد من التنسيق بن الأجهزة المعنية بتدريب رجال تنفيذ القانون، إيجاد برامج تدريبية مشتركة تناسب جميع الفئات، هذا بالإضافة إلى القيام ببعض العمليات المشتركة، والتي من شأنها صقل مهارات القائمين على مكافحة تلك الجرائم وتقريب وجهات النظر بشأنها.

الفرع الثامن: بعض الهيئات المساعدة لمتابعة جرائم الانترنت

نظرا لنوع و خصوصية جرائم الانترنت، فقد أوجدت بعض الدول أجهزة مختصة تتولى تطبيق قوانين مكافحة الجريمة المعلوماتية، وتتبع الجناة و من أهمها :

البند الأول : مركز الشكاوى الخاصة بجرائم الانترنت

قد طوّرت وكالات تطبيق القوانين أساليب جديدة وعلاقات جديدة للقبض على المجرمين في الفضاء السيبراني، أو الانترنت [1]،فظهر كنتيجة لذلك مركز الشكاوى الخاصة بجرائم الانترنت2 (IC3)هو كناية عن نظام تبليغ وإحالة لشكاوى الناس في الولايات المتحدة والعالم أجمع ضد جرائم الأنترنت، ويخدم المركز، بواسطة استمارة للشكاوى مرسلة على الإنترنت وبواسطة فريق من الموظفين والمحللين، الجمهور ووكالات فرض تطبيق القوانين الأميركية والدولية التي تحقق في جرائم الانترنت .

[1] -IC3 Mission Statement The mission of the Internet Crime Complaint Center is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.- http://www.ic3.gov/default.aspx

[2] - http://www.ic3.gov/default.aspx.

نشأ مركز الشكاوى الخاصة بجرائم الانترنت كمفهوم سنة 1998 بعد ادراك بأن الجريمة، بدأت تدخل الانترنت لأن الأعمال التجارية والمالية كانت قد بدأت تتم عبر الانترنت، ولأن مكتب التحقيقات الفدرالي أراد أن يكون قادراً على تعقب هذه النشاطات وعلى تطوير تقنيات تحقيق خاصة بجرائم الانترنت .

و لم يكن آنذاك أي مكان واحد معين يمكن للناس التبليغ فيه عن جرائم الإنترنت، وأراد مكتب التحقيقات الفدرالي التمييز بين جرائم الانترنت، والنشاطات الإجرامية الأخرى التي تُبلّغ عنها عادةً الشرطة المحلية، ومكتب التحقيقات الفدرالي والوكالات الأخرى التي تطبق القوانين الفدرالية وهيئة التجارة الفدرالية (*FTC*) و المكتب الأميركي للتفتيش البريدي(*USPIS*) ، وهو الشعبة التي تطبق القوانين المتعلقة بمصلحة البريد الأميركية، وغيرها من الوكالات .

وقد تم تأسيس أول مكتب للمركز سنة 1999 في مورغانتاون بولاية وست فرجينيا، وسمّي مركز شكاوى الاحتيال على الانترنت، وكان المكتب عبارة عن شراكة بين مكتب التحقيقات الفدرالي والمركز القومي لجرائم موظفي المكاتب، وهذا الأخير مؤسسة لا تبغي الربح متعاقدة مع وزارة العدل الأميركية مهمتها الأساسية تحسين قدرات موظفي أجهزة تطبيق القانون، على صعيد الولاية والصعيد المحلي، على اكتشاف جرائم الانترنت أو الجرائم الاقتصادية ومعالجة أمرها [1].

وفي عام 2002، وبغية توضيح نطاق جرائم الانترنت التي يجري تحليلها، بدءاً من الاحتيال البسيط إلى تشكيلة من النشاطات الإجرامية، التي أخذت تظهر على الانترنت، أعيدت تسمية المركز وأطلق عليه اسم مركز الشكاوى الخاصة بجرائم الانترنت، ودعا مكتب التحقيقات الفدرالي وكالات فدرالية أخرى، مثل مكتب التفتيش البريدي وهيئة التجارة الفدرالية والشرطة السرية وغيرها، للمساعدة في تزويد المركز بالموظفين وللمساهمة في العمل ضد جرائم الانترنت .

وقد أصبح هناك اليوم في مركز الشكاوى القائم بفيرمونت، بولاية وست فرجينيا، ستة موظفين فدراليين وحوالى أربعين محللاً من القطاع الأكاديمي، وقطاع صناعة الكمبيوتر وخدمات الانترنت، يتلقون الشكاوى المتعلقة بجرائم الإنترنت من الجمهور، ثم يقومون بالبحث في

[1] -https://elhanem.wordpress.com.

الشكاوى وتوضيب ملفها وإحالتها إلى وكالات تطبيق القانون الفدرالية والمحلية والتابعة للولايات وإلى أجهزة تطبيق القانون الدولية أو الوكالات التنظيمية وفرق العمل التي تشارك فيها عدة وكالات، للقيام بالتحقيق فيها .

وبإمكان الناس من كافة أنحاء العالم تقديم شكاوى بواسطة موقع مركز الشكاوى الخاصة بالجرائم الواقعة على الانترنت(*http://www.ic3.gov*) ، ويطلب الموقع اسم الشخص وعنوانه البريدي ورقم هاتفه؛ إضافة إلى اسم وعنوان ورقم هاتف والعنوان الإلكتروني، إذا كانت متوفرة، للشخص، أو المنظمة، المشتبه بقيامه بنشاط إجرامي؛ علاوة على تفاصيل تتعلق بكيفية وقوع الجريمة حسب اعتقاد مقدم الشكوى ووقت وقوعها وسبب اعتقاده بوقوعها؛ بالإضافة إلى أي معلومات أخرى تدعم الشكوى .

يعمل مركز الشكاوى الخاصة بجرائم الانترنت ووكالات أميركية أخرى مع المنظمات الدولية، مثل لجنة الجرائم الاقتصادية والمالية في نيجيريا *(EFCC)* ومع المسؤولين عن تطبيق القانون في بلدان أخرى لمحاربة الاحتيال على الانترنت، وإعداد ملفات القضايا وإحالتها على المركز، هدف عمليات المركز الرئيسي هو أخذ شكوى المواطن الفرد التي قد تتعلق بجريمة تنجم عنها أضرار بحدود 100 دولار مثلاً، وضمها إلى المعلومات المبلّغ عنها من جانب 100 أو 1000ضحية أخرى من مختلف أنحاء العالم، فقدت أموالاً نتيجة نفس السيناريو، وثم إعداد ملف قضية مهمة بأسرع وقت ممكن و إحالتها على الجهات المختصة بالمتابعة.

والحقيقة هي أنه لا يسمح لمعظم الوكالات فرض تطبيق القانون، معالجة أمر القضايا التي تمثل مبالغ ضئيلة نسبياً، ومبلغ مئة دولار أقل على الأرجح من المبلغ المسموح بالتحقيق في أمره، غير أن معظم المجرمين يعملون على الانترنت لكي يوسعوا نطاق فرصهم في إيذاء الضحايا وكسب المال؛ وجرائم الانترنت لا تقتصر أبداً على ضحية واحدة، وهكذا، إذا تمكن محققو مكتب الشكاوى من ربط عدة شكاوى ببعضها البعض، وحولوها إلى قضية واحدة قيمتها عشرة آلاف أو مئة ألف دولار، أضرت بمائة أو ألف ضحية، تصبح الجريمة عندئذ قضية مهمة، ويصبح بإمكان وكالات تطبيق القانون التحقيق فيها .

ويساعد مركز الشكاوى الخاصة بجرائم الانترنت أحياناً وكالات تطبيق القانون من خلال إجراء الأبحاث وإعداد ملف القضية الأولى، وقد وجد محققو المركز، خلال السنتين

والنصف الأوليين من عمر المشروع، وعلى الرغم من جهود إعداد القضايا وإحالتها بسرعة إلى وكالات تطبيق القوانين، أن فرق العمل الخاصة بمكافحة جرائم الانترنت لم تكن جميعاً مجهزة لمتابعة هذه الجرائم أو التحقيق فيها بسرعة، وقد لا تملك بعض فرق العمل هذه القدرة على القيام بعمليات سرية، أو قد لا تملك التجهيزات اللازمة لاقتفاء الآثار الرقمية للأدلة الجرمية التي يحولها إليها مركز الشكاوى، لذلك، أصبح من المهم جداً بالنسبة لمركز الشكاوى أن يطور ويتعقب آثار الجرائم ثم يتوصل إلى إعداد ملف القضية الأولي مثلاً، قد يتعرف مركز الشكاوى الخاصة بجرائم الانترنت على هوية 100 ضحية[1]، ويقرر أنه يبدو أن النشاط الإجرامي صادر عن جهاز مقدم خدمات كمبيوتر في كندا، مثلاً، لكن ذلك الجهاز قد يكون مجرد كمبيوتر تم التسلل إليه، وقد يكون ما حدث هو أن المجرمين يستخدمون هذه الآلة "كنقطة انطلاق وهمية" لإخفاء مكان تواجدهم الحقيقي، لذا فإنه من المفيد بالنسبة لمحللي مركز الشكاوى أن يعرفوا المزيد عن "نقطة الانطلاق الوهمية"؛ فقد تكون هناك مجموعة في تكساس، أو أفريقيا الغربية، أو رومانيا، تستخدم جهاز مقدم خدمات الانترنت في كندا لجمع المعلومات عن الضحايا المحتملين [2].

البند الثاني : الوكالة الوطنية لأمن النظم المعلوماتية[3] (ANSSI)

الوكالة الوطنية لأمن النظم المعلوماتية، هي السلطة الوطنية في مجال أمن النظم المعلوماتية والدفاع عنها، وتتمثل المهمات الرئيسية للوكالة في تحقيق أمن النظم المعلوماتية للدولة ومراقبة نظم المعلوماتية للوكالات التنفيذية الوطنية ذات الأهمية الحيوية، وتنسيق أنشطة الدفاع عن نظم المعلومات، وتصميم الشبكات المحصنة التي تلبي احتياجات أرفع السلطات في الدولة واحتياجات

---

[1]- اظهر التحليل الشامل للشكاوى التي قدمت للمركز، إن عدد الشكاوى التي تلقاها المركز منذ بدأ أعماله في 2000 وحتى شهر تشرين ثاني من نفس العام (أي خلال ستة أشهر فقط) قد بلغت 6087 شكوى، من ضمنها 5273 حالة تتعلق باختراق الكمبيوتر عبر الإنترنت و814 تتعلق بوسائل الدخول والاقتحام الأخرى كالدخول عبر الهاتف أو الدخول المباشر إلى النظام بشكل مادي، مع الإشارة إلى ان هذه الحالات هي فقط التي تم الإبلاغ عنها ولا تمثل الأرقام الحقيقية لعدد حالات الاحتيال الفعلي ، وهي تتعلق فقط بجريمة الاحتيال عبر الإنترنت التي هي واحدة من العديد من أنماط جرائم الكمبيوتر والإنترنت. وقد بلغت الخسائر المتصلة بهذه الشكاوى ما يقارب 4.6 مليون دولار وهي تقارب 33% من حجم الخسائر الناشئة عن كافة جرائم الاحتيال التقليدية المرتكبة في نفس الفترة . وان 22% من هذه الخسائر نجمت عن شراء منتجات عبر الإنترنت دون ان يتم تسليم البضاعة فعليا للمشترين، وان 5% منها نشأت عن احتيال بطاقات الائتمان : http://www.dralmarri.com/show.asp?field=res_a&id=197

2 -https://elhanem.wordpress.com

3 -ANSSI : Agence Nationale Sécurité des systèmé information

الوزارات ومد هذه الشبكات، وتوفير الشروط الكفيلة بإرساء جو الثقة والأمن الموات لتطوير مجتمع المعلومات في فرنسا وأوروبا[1].

أنشئت الوكالة في عام 2009[2]،وألحقت بالأمانة العامة للدفاع والأمن القومي (SGDSN)، وهي السلطة المكلفة بمساعدة رئيس الوزراء في ممارسة مهامه في مجال الدفاع والأمن القومي[3].

البند الثالث : وحدة مبادرات جرائم الانترنت

نظراً لتوصل مركز الشكاوى الخاصة بجرائم الانترنت، IC3 إلى أنه من الأفضل في بعض القضايا التقنية المعقدة، تعقب أثر التحقيقات المبكرة، قام بإنشاء مكتب فرعي لهذا الغرض في بيترسبرغ، بولاية بنسلفينيا، أطلق عليه اسم "وحدة مبادرات جرائم الانترنت ودمج مواردها، ويقوم محللو هذه الوحدة بإلغاء مسارات التحقيق الخاطئة ويغربلون أدلة القضية وينقحونها قبل إحالتها إلى وكالات تطبيق القوانين أو فرق العمل الخاصة المحلية أو الدولية .

تحظى وحدة مبادرات جرائم الإنترنت، بالدعم من بعض أكبر الشركات التي يستهدفها مجرمو الفضاء السبراني، أي المنظمات والتجار الذين يعملون في مجال الانترنت مثل

---

[1] -le Premier ministre, Manuel Valls. de la Stratégie nationale pour la sécurité du numérique.

-La Stratégie nationale pour la sécurité du numérique, dévoilée ce 16 octobre 2015 par Monsieur le Premier ministre ,Manuel Valls, est destinée à accompagner la transition numérique de la société française.

Cette stratégie a fait l'objet de travaux interministériels coordonnés par l'ANSSI. Ses objectifs ont été consolidés par la secrétaire d'Etat chargée du numérique et le secrétaire général de la défense et de la sécurité nationale. Elle répond aux nouveaux enjeux nés des évolutions des usages numériques et des menaces qui y sont liées avec cinq objectifs : garantir la souveraineté nationale ; apporter une réponse forte contre les actes de cybermalveillance ; informer le grand public ; faire de la sécurité numérique un avantage concurrentiel pour les entreprises françaises et renforcer la voix de la France à l'international.Avec la Stratégie nationale pour la sécurité du numérique, l'Etat s'engage au bénéfice de la sécurité des systèmes d'information pour aller, par une réponse collective, vers la confiance numérique propice à la stabilité de l'État, au développement économique et à la protection des citoyens. http://www.ssi.gouv.fr

[2] -Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »

[3]- للمزيد من المعلومات عن الوكالة الوطنية لأمن النظم المعلوماتية،راجع http://www.ssi.gouv.fr/

مايكروسوفت، وإي باي/ باي بال، وأميركا أونلاين، وجمعيات هذه الصناعة التجارية مثل اتحاد برامج كمبيوتر الأعمال، وجمعية التسويق المباشر، ومجلس مخاطر التجار،وصناعة الخدمات المالية، وغيرها ،وقد انضم محققون ومحللون من هذه المنظمات،يعمل الكثير منهم على قضايا جرائم الانترنت، إلى وحدة المبادرات المذكورة لتحديد اتجاهات وتكنولوجيات جرائم الانترنت، ولجمع المعلومات لإعداد ملفات قضايا قانونية ذات شأن، ولمساعدة وكالات تطبيق القانون في جميع أنحاء العالم على اكتشاف جرائم الإنترنت ومحاربتها .

ويتعاون في وحدة المبادرات موظفون فدراليون ومحللون من القطاع الأكاديمي وقطاع صناعة الانترنت سوية للتوصل إلى معرفة المصدر الذي تنبثق عنه الجريمة، ومن يقف وراءها، وطريقة محاربتها، وعندما تسمع وحدة المبادرات من مجموعة صناعية عن اتجاه أو مشكلة معينة، تُشكّل الوحدة مبادرة لاستهداف بعض كبار المجرمين وإلقاء القبض عليهم، ولا تكتفي بمقاضاتهم بل تسعى لمعرفة المزيد عن كيفية قيامهم بعملياتهم، وعقب ذلك، يُبلّغ مكتب الشكاوى الجمهور عن هذه الاتجاهات وعن العمليات الاحتيالية، وذلك من خلال إصدار بيان خدمة عامة ينبه الشعب وينشر على موقع مكتب الشكاوى، أو يوزع بطرق أخرى [1].

واستناداً إلى معطيات شكاوى المستهلكين أو قطاع صناعة الإنترنت، يرصد المحققون الاتجاهات والمشاكل، ويضعون بالتعاون مع شركاء في صناعة الانترنت مبادرات لفترة تمتد ما بين ستة أشهر وسنة لاستهداف النشاطات الإجرامية، بما في ذلك ما يلي:

1. إعادة الشحن: عملية يتم من خلالها توظيف متآمرين أو شركاء، لا علم لهم بالموضوع، في الولايات المتحدة، لاستلام طرود تحتوي على بضائع إلكترونية، أو سلع أخرى، كان قد تم

[1] -Since 2000, the IC3 has received complaints crossing the spectrum of cyber crime matters, to include online fraud in its many forms including Intellectual Property Rights (IPR) matters, Computer Intrusions (hacking), Economic Espionage (Theft of Trade Secrets), Online Extortion, International Money Laundering, Identity Theft, and a growing list of Internet facilitated crimes. It has become increasingly evident that, regardless of the label placed on a cyber crime matter, the potential for it to overlap with another referred matter is substantial. Therefore, the IC3, formerly known as the Internet Fraud Complaint Center (Internet Fraud Complaint Center), was renamed in October 2003 to better reflect the broad character of such matters having an Internet, or cyber, nexus referred to the IC3, and to minimize the need for one to distinguish "Internet Fraud" from other potentially overlapping cyber crimes. http://www.ic3.gov/about/default.aspx

شراؤها بواسطة بطاقات ائتمان مزورة أو مسروقة، فيعاد توضيبها وشحنها، عادةً إلى خارج البلاد، وعندما يكتشف التاجر أن بطاقة الائتمان كانت مزورة، تكون البضاعة قد أصبحت في بلد آخر .

البريد الإغراقي (سبام) الإجرامي: وهو عبارة عن رسائل إلكترونية ترسل بالجملة دون أن تكون قد طلبت وتُستعمل للاحتيال على المؤسسات المالية، وتزوير بطاقات الائتمان، وسرقة الهوية، وجرائم الأخرى، ويمكن أن يُستعمل البريد الإغراقي أيضاً كوسيلة للدخول إلى الكمبيوترات الخاصة وأجهزة شركات تقديم خدمات الإنترنت دون إذن، أو لإيصال الفيروسات وبرمجيات الكمبيوتر الإجتياحية إلى كمبيوترات أخرى[1].

2. اصطياد كلمات المرور: وهو محاولات لسرقة كلمات السر الإلكترونية والمعلومات المالية، عن طريق تظاهر المجرم بأنه شخص جدير بالثقة أو مؤسسة أعمال عبر اتصال إلكتروني يبدو وكأنه رسمي، كرسالة إلكترونية أو موقع إلكتروني .

3. سرقة الهوية: هي نتيجة عمل يقوم به المجرم مستخدماً معلومات شخصية مسروقة لشخص ما، من أجل اقتراف عملية احتيال أو جرائم أخرى، وكل ما يحتاجه المجرم لسرقة هوية هو القليل من المعلومات الشخصية .

يعمل مركز الشكاوى الخاصة بجرائم الإنترنت أيضاً مع منظمات دولية مثل هيئة الجرائم الاقتصادية والمالية في نيجيريا، حيث توجد مستويات عالية من الجرائم الاقتصادية والمالية كتبييض الأموال والاحتيال بقبض أموال مسبقة لمشاريع وهمية، أو ما يسمى احتيال 419، مما كانت له عواقب سلبية شديدة على ذلك البلد [2].

---

[1] - Daniel Larkin, Fighting Online Crime,IC3 investigates the growing number, of complaints about activity online. Read more:
http://iipdigital.usembassy.gov.

[2] -Criminal code act, 1st day of June 1916,Chapter 38: Obtaining Property by false pretences; Cheating Article 419. Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.

- If the thing is of the value of one thousand naira or upwards, he is liable to imprisonment for seven years.

وتجمع جريمة احتيال 419، التي أطلق عليها اسمها لخرقها الفقرة 419 من مدونة القوانين الجنائية النيجيرية[1]، ما بين جرم انتحال الشخصية وتشكيلة متنوعة من مؤامرات قبض الأموال مسبقاً لمشاريع وهمية، فالضحية المحتملة تتلقى رسالة، أو رسالة إلكترونية، أو فاكس، من أشخاص يدعون أنهم موظفون حكوميون نيجيريون أو أجانب، يطلبون فيها المساعدة في إيداع مبالغ طائلة من المال في حسابات في مصارف خارجية، عارضين حصة من الأموال مقابل ذلك، ويعتمد المخطط على إقناع الضحية الراغبة في التعاون بإرسال مبلغ من المال إلى كاتب الرسالة على دفعات لأسباب متنوعة .

- It is immaterial that the thing is obtained or its delivery is induced through the medium of a contract induced by the false pretence.

- The offender cannot be arrested without warrant unless found committing the offence.

[1] - 419A. Any person who by any false pretence or by means of any other fraud obtains credit for himself or any other person-

(a) in incurring any debt or liability; or

(b) by means of an entry in a debtor and creditor account between the person giving and the person receiving credit, is guilty of a felony and is liable to imprisonment for three years.

-The offender cannot be arrested without warrant unless found committing the offence.

419B. Where in any proceedings for an -offence under section 419 or 419A it is proved that the accused-

(a) obtained or induced the delivery of anything capable of being stolen; or

(b) obtained credit for himself or any other person, by means of a cheque that, when presented for payment within a reasonable time, was dishonoured on the ground that no funds or insufficient funds were standing to the credit of the drawer of the cheque in the bank on which the cheque was drawn, the thing or its delivery shall be deemed to have been obtained or induced, or the credit shall he deemed to have been obtained, by a false pretence unless the court is satisfied by evidence that when the accused issued the cheque he had reasonable grounds for believing, and did in fact believe, that it would be honoured if presented for payment within a reasonable time after its issue by him.

وهناك مجموعة متنامية من الوكالات الدولية المنخرطة في محاربة جرائم الانترنت، ويعمل مركز الشكاوى الخاصة بجرائم الانترنت، مع المسؤولين عن تطبيق القانون في بلدان عديدة، بينها أستراليا والمملكة المتحدة، كما يحضر ممثلو مركز الشكاوى أيضاً اجتماعات دورية للمجموعة الفرعية حول جرائم التكنولوجيا المتقدمة التابعة لمجموعة الثماني (كندا، فرنسا، ألمانيا، إيطاليا، اليابان، روسيا والمملكة المتحدة والولايات المتحدة)، ويعمل قسم من

هذه المجموعة الفرعية على محاربة جرائم الانترنت وتعزيز التحقيقات بشأنها. [1]

ومشروعا مركز الشكاوى الخاصة بجرائم الإنترنت(IC3 ، ووحدة مبادرات جرائم الإنترنت ودمج مواردها)، هما بمثابة عمل متطور ومتقدم باستمرار، وأثناء هذا التقدم، يراجع موظفو ومحللو مركز الشكاوى ما أثبت نجاحه وما ثبت فشله من إجراءات، ويسعون باستمرار لتأمين مساعدة الخبراء والمصادر، التي تزودهم بمعلومات استخباراتية ليصبحوا أكثر فطنة بخصوص جرائم الإنترنت، ولكي يتعلموا كيف يمكنهم محاربتها بصورة أكثر فعالية، فهذه هي مهمة مركز الشكاوى الدائمة التي لا تتغير.[2]

الفرع التاسع : أمثلة عن التعاون الدولي :

يمكن ذكر العديد من الأمثلة التي تُوِّجت بالنجاح، نذكر بذلك مكافحة استغلال الأطفال في إنتاج المواد الإباحية على الإنترنت، حيث قامت الشرطة، في السنوات الأخيرة، بعمليات عديدة نُفِّذت بالتنسيق بين دول مختلفة انتهت بتوقيف الجناة:

✓ عملية فالكون *FALCON* في إبريل 2005، والتي تمت بين كل من الشرطة الفيدرالية الأمريكية FBIوالإنتربول والشرطة الفرنسية والتي سمحت بتفكيك شبكة تنشط في العديد من الدول الأوروبية.

---

[1] -Daniel Larkin, Fighting Online Crime,IC3 investigates the growing number of complaints, about activity online,Read more: http://iipdigital.usembassy.gov

[2]- طرق التحقيق في الجرائم الالكترونية، جريدة حقوقية جزائرية الكترونية، منشور بتاريخ07 أبريل2015.

https://www.seoudi-law.com/?p=21788.

✓ عملية محطم الجليد *Icebreaker* (قامت بها يوروبول) *Europol* في 14 يونيو 2005، تم خلالها مداهمة وتفتيش أماكن في ثلاث عشرة دولة أوروبية هي(النمسا، بلجيكا، فرنسا، ألمانيا، المجر، أيسلندا، إيطاليا، هولندا، بولونيا، البرتغال، سلوفاكيا، السويد، وبريطانيا العظمى)كما تم توقيف أفراد في كل من فرنسا، بلجيكا، المجر، وأيسلندا والسويد.

✓ عملية أوديسيوس *Odysseus* التي تمت في 26 فبراير/شباط 2004 بمبادرة من يوروبول، وقامت قوات الشرطة خلالها بعمليات شملت 10 دول هي(أستراليا، بلجيكا، كندا، ألمانيا، هولندا، النرويج، بيرو، أسبانيا، السويد وبريطانيا[1].

[1]- جان فرنسوا هنروت، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي، مداخلة في الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر،16-20 يونيو 2007 بالمملكة المغربية ص 108.

المبحث الثاني الجزائر بين جرائم الواقع الإفتراضي والمستجدات القانونية والإجرائية

حطمت الجريمة العنكبوتية[1] كل القيم والمفاهيم التي تربى عليها الجزائريون، وعجّلت بتآكل أساسات المجتمع بعدما أباحت المحظورات وكسرت الحواجز الأخلاقية، وفتحت النار على بقايا شخصية لطالما اعتبرت النخوة والشرف سر وجودها، وفشلت الأجهزة الردعية في ترجمة قوانين هشة لا تتوافق والرؤية العالمية لمفهوم الإجرام على الشبكة العنكبوتية، في وقت يتفاخر قراصنة النّت بتوقيع الأذية على الآخرين ويتباهون بإمساكهم لناصية العالم الافتراضي[2] وتحكمهم بخبايا السياسات الدولية بمجرد الضغط على زر المفاتيح.

فتحت الجزائر الأبواب على مصراعيها لتلقي واستهلاك محتوى الأنترنت، وسمحت لمن عرّج عليها الغوص في شبكتها، دون ترهيبه من نتائج ارتكاب المحظور الممثل خاصة في التهديد والابتزاز والتشهير بالآخرين في مواقع الأنترنت وإنشاء وارتياد المواقع الإرهابية والتزوير والسطو على المعطيات المحمية، ومنها أسرار الدول الخطيرة التي تصبح متاحة بمجرد حركة ضغط واحدة على لوح المفاتيح .

واكتشفت بعدها أن الوقت كان لا يزال مبكرا على استهلاك هذا الكم الهائل من المعلومات، وأن تشعب فضاءات الأنترنت أصعب من أن تتمكّن بسياستها التقليدية، من السيطرة على مرتاديه في ظل عدم إنشاء منظومة ردعية، ترافق هذه التقنية المتطورة والتي منحت المفتاح المفقود للمجرمين، فالمتورطون في جرائم الشرف الإلكترونية[3] ومعهم محتالوها الذين يخدعون

---

[1] – أظهرت الإحصائيات الأمنية لسنة 2015 ،تنامي الجريمة الالكترونية بشكل كبير، إذ عالجت مصالح الدرك الوطني خلال السنة المنصرمة أكثر من 500 جريمة الكترونية، حسب ما صرح به رئيس مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية والحماية منها ومكافحتها، التابعة للدرك الوطني، العقيد بن رجم لـــ''الخبر''، أن أكثر من 300 جريمة رقمية كان مسرحها موقع التواصل الاجتماعي ''الفايسبوك''، بينما عالجت المديرية العامة للأمن الوطني 547قضية تعلقت بالجرائم الالكترونية الممارسة في الفضاء الافتراضي.

الجزائر: حسام حريشان ، سطيف،عبد الرزاق ضيفي / قسنطينة، وردة /سيدي بلعباس: م.ميلود، الفايسبوك تحوّل إلى وسيلة انتقام وخراب بيوت الجزائريين، تم الاطلاع عليه ، 27 – 14:46 في يناير 2016

http://www.elkhabar.com/press

[2] -Jacques TISSEAU,Réalité Virtuelle, Habilitation à Diriger des Recherches ,Université de Rennes 1.Spécialité , Informatique,Document de Synthèse, 6 décembre 2001.p16

[3] – 75بالمائة من الجرائم الإلكترونية المرتكبة في الجزائر متعلقة بالشرف.

المغفلين، وغيرهم لسرقة أموالهم بسهولة والأخطر منهم أولئك الذين يشيدون بالإرهاب ويستهلكون الرسائل المميتة القادمة، من مشايخ مزيفين يدعون إلى الفتنة الكبرى، كل هؤلاء لا يتم اقتيادهم إلى السجون، وفي أحسن الأحوال يتم إيقافهم وإطلاق سراحهم لعدم إثبات التهم الموجهة إليهم، في حين يضطر القضاة إلى تبرئتهم وربما إخضاع المعنيين لعقوبات لا تتجاوز خمس سنوات سجنا فقط[1].

المطلب الأول : الشقّ القانوني لمكافحة الجريمة الإلكترونية

إسهاما في توفير الاستخدام الآمن لتقنية المعلومات، التي تشهد انتشاراً واسعاً في القطاعين العام و الخاص [2]، فقد قام المشرع الجزائري بإصدار ترسانة من القوانين[3] منها قانون العقوبات 04 /15[4]،و قانون04/09المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال[5]،

أكد محافظ الشرطة القضائية المتخصص في الجرائم الإلكترونية، مصطفاوي عبد القادر، أن مصالح الأمن التابعة لولاية الجزائر قامت بإحصاء 28 قضية خاصة بالجرائم الإلكترونية خلال سنة 2010، أما في السنة الجارية فقد تم تسجيل 25 قضية خلال السداسي الأول منها، فيما تبقى الحالات المسكوت عنها أكبر من ذلك إذا عرفنا أن 75 بالمائة من هذه الجرائم متعلقة بالشرف.. الأمر الذي يحول دون الإبلاغ .

[1]- المواد 394 مكرر وما يليها من القانون 15-04المؤرخ في 2004/11/10 المعدل و المتمم لقانون العقوبات، الذي ينص على الحماية الجزائية للأنظمة المعلوماتية، من خلال تجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، التي تقضي بمعاقبة مقترفي الجرائم المتعلقة بتكنولوجيا الاتصال بما يصل إلى خمس سنوات سجنا، وغرامات مالية تصل إلى 200 مليون سنتيم قابلة للمضاعفة في حالات التشديد.

[2]- يوسف قجاج ،المرجع السابق : http://www.marocdroit.com

[3]- تطور التشريع الجزائري في مجال محاربة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال

- القانون رقم 04-15 الصادر في 10-11-2004 المعدل و المتمم لقانون العقوبات
- القانون رقم 04-14الصادر في 10-11-2004 المعدل و المتمم لقانون الاجراءات الجزائية
- القانون رقم 06-22 الصادر في 20-12-2006 المعدل والمتمم لقانون الإجراءات الجزائية
- القانون رقم 09-04 الصادر في05-08-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال،
- القانون 2000-03المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية و اللاسلكية ومكافحتها.

[4]- قانون العقوبات رقم 04-15 المؤرخ في 10 نوفمبر 2004.

[5]- القانون رقم 09-04 الذي تضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، مؤرخ في 14 شعبان عام 1430، الموافق 05 /08 /2009،ج.ر.ر رقم 47.

وقانون رقم15-03المتعلق بعصرنة العدالة وكذا قانون رقم15- 04 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني.[1]

الفرع الأول: أمن المعلومات و المعاملات الالكترونية بمقتضى قانون العقوبات 15/04

تدارك المشرع الجزائري مؤخرا – ولو نسبيا- الفراغ القانوني في مجال الإجرام ألمعلوماتي و ذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية [2]،بموجب القانون رقم 15/04 المتضمن تعديل قانون العقوبات، لكن تجدر الإشارة إلى أن المشرع الجزائري قد ركز على الاعتداءات الماسة بالأنظمة المعلوماتية.

البند الأول : الاعتداءات الماسة بالأنظمة المعلوماتية

على المستوى الوطني،فقد استدرك المشرع الجزائري الفراغ القانوني من خلال التعديل الأخير لقانون العقوبات،الذي تم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم156/66 بقسم سابع مكرر عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات" ويشمل المواد من 394 مكرر إلى 394 مكرر 7.

الجرائم الماسة بالأنظمة المعلوماتية وان كانت تختلف في أركانها و عقوباتها إلا أن ما يجمعها أنهما تحقق حماية جزائية تنظم المعالجة الآلية للمعطيات،أي أن القاسم المشترك بينهما هو نظام المعالجة الآلية،ولذلك فان دراسة تلك الجرائم تقتضي منا أولا توضيح وبيان مفهوم نظام المعالجة الآلية للمعطيات.

[1]– قانون رقم 15-03 مؤرخ في 11 ربيع الثاني عام 1436 الموافق أوّل فبراير سنة 2015 يتعلق بعصرنة العدالة و قانون رقم 15 - 04 مؤرخ في 11 ربيع الثاني عام 1436 الموافق أوّل فبراير سنة 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني.

[2]– قانون العقوبات الذي تمم العنصر الثالث من الباب الثاني من الكتاب الثالث من الأمر 156/66 بقسم سابع مكـــــرر عنوانه " المساس بأنظمة المعالجة الآلية للمعطيات " و يشمل المواد من 394 مكرر إلى 394 مكرر 7 ".

أ- مفهوم نظام المعالجة الآلية للمعطيات

يقصد بالمعالجة الآليّة للبيانات، مجموعة العمليّات المحقّقة بواسطة الوسائل الأوتوماتيكيّة والتّي لها علاقة بجمع وتسجيل وتعديل وحفظ وتحطيم وبثّ المعطيات، واستغلالها بوجه عام، أي جميع العمليّات التّي يمكن أن يقوم بها الحاسوب، انطلاقا من إدخال المعطيات وجمعها، فتغييرها وتعديلاها، وإن شئنا حفظها أو إلغاءها، إلى غاية إخراجها من الحاسوب في اتّجاه الربط بوسائل إلكترونيّة أخرى.[1]

ويعتمد الحاسوب لغة خاصّة في المعالجة، وهي لغة البتّة ***code binaire*** أي أن تتحوّل جميع البيانات إلى أرقام متكوّنة من الصّفر والواحد، وهو ما يعرف بالرّقمنة ***numérisation***، حيث تتحوّل الكتابة العاديّة إلى أرقام يفهمها الحاسوب[2] .

- إن نظام المعالجة الآلية للمعطيات، تعبير فني وتقني، يصعب على الباحث إدراك حقيقته وفحواه، بسهولة، فضلا على كونه مدلول متطور يخضع للتطورات السريعة المتلاحقة في مجال فن الحسابات الآلية، والمشرع المغربي لم يعرف نظام المعالجة الآلية للمعطيات، بل ترك الأمر للفقه والقضاء .

- وفي الفقه الفرنسي، فقد تم تعريفه بأنه" كل مركب يتكون من وحدة او مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات، التي عن طريقها تتحقق نتيجة معينة، على أن يكون هذا المركب خاضع لنظام الحماية الفنية ."

- ومهما يكن من أمر، وبالرجوع إلى القانون الجنائي الجزائري، نجدان المشرع خص عقوبات صارمة على دخول أنظمة المعالجة الآلية للمعطيات، وقد أفردت نصوص القانون المذكور عقوبات صارمة في هذا الشأن، كما يلي:

---

[1]- فالكلمة الواحدة، على سبيل المثال، يوافقها ثماني بتّات bitsأي أكتي واحد .un octetوتنسحب هذه اللّغة الرقميّة على جميع التّعابير الثّقافيّة بما في ذلك الصّوت والصّورة والنّصوص. وهو الأساس في تخزين المعلومة بالبرامجيّات المستقلّة ومنها الأقراص المكتنزة CDRom التّي بإمكانها أن تحمل عددا ضخما من البيانات على مساحة صغيرة، والمثل ينطبق على جميع المعدّات المعلوماتيّة. وقد ارتبط تقدّم المعلوماتيّة بمستوى الرّقمنة، وانتشر استعمالها، فأبقت عدّة تأثيرات على مستوى التّطبيقات، والمهمّ أن نعلم الآن أن الرّقمنة هي أساس المعالجة الإلكترونيّة

[2]- علي كحلون، المسؤولية المعلوماتية، مركز النشر الجامعي، ص 10 .وما بعد.

ب- نظام المعلومات *information system*

يمكن أن نعرف نظام المعلومات ***information system*** بأنه مجموعة من العناصر المتداخلة والمتفاعلة مع بعضها ***set of interrelated component*** والتي تعمل على جمع البيانات والمعلومات، ومعالجتها، وتخزينها، وبثها وتوزيعها، بغرض دعم صناعة القرارات، والتنسيق وتأمين السيطرة على المنظمة، إضافة إلى تحليل المشكلات، وتأمين المنظور المطلوب للموضوعات المعقدة، ويشتمل نظام المعلومات على بيانات عن الأشخاص الأساسيين، والأماكن، والنشاطات والأمور الأخرى التي تخص المنظمة، والبيئة المحيطة بها.

ج- نظام المعلومات المحوسبة *computerize information system*

أما استخدام مصطلح نظام المعلومات المحوسبة ***computerize information system***،والذي كثيراً ما يصطلح على تسميته نظام المعلومات المعتمدة على الحاسوب ***Computer-based information systems***، ويرمز له اختصاراً ***(CBIS)***، فهو النظام الذي يعتمد على المكونات المادية أو الأجهزة ***Hardware***،والمكونات البرمجية Software للحاسوب، في معالجة البيانات، من ثم وبث واسترجاع المعلومات. ***Information processing and disseminating*** وعموماً، فإن نظام المعلومات هو عبارة عن آلية وإجراءات منظمة، تسمح بتجميع، وتصنيف، وفرز البيانات data ومعالجتها، ومن ثم تحويلها إلى معلومات ***information*** يسترجعها الإنسان عند الحاجة، ليتمكن من إنجاز عمل أو اتخاذ قرار أو القيام بأية وظيفة تفيد حركة المجتمع، عن طريق المعرفة التي سيحصل عليها من المعلومات المسترجعة من النظام. وقد يتم استرجاع المعلومات، في نظام المعلومات يدوياً، أو ميكانيكياً، أو إلكترونياً وهو، أي هذا الأخير هو الغالب في نظم المعلومات المعاصرة.

ويمكن الذهاب إلى اتجاه أكثر تحديداً فنعرف نظام المعلومات بأنه "مجموعة من العناصر البشرية والآلية، التي تعمل معاً على تجميع البيانات ومعالجتها وتحليلها وتبويبها، طبقاً لقواعد

وإجراءات مقننة لأغراض محدد، بغرض إتاحتها للباحثين وصانعي القرارات والمستفيدين الآخرين، على شكل معلومات مناسبة ومفيدة"[1].

يمثل نظام المعالجة الآلية للمعطيات،المسالة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان أية جريمة من جرائم الاعتداء على هذا النظام،فان ثبت تخلف هذا الشرط الأولي،لا يكون هناك مجال لهذا البحث, ويؤدي توافر هذا الشرط إلى الانتقال إلى المرحلة التالية وهي بحث توافر أركان أية جريمة من الجرائم السابقة،إذ أن هذا الشرط يعتبر عنصر لازما لكل منها،ولذلك يكون من الضروري تحديد مفهوم نظام الآلية للمعطيات .

نظام المعالجة الآلية للمعطيات تعبير فني تقني،يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلا عن انه تعبير متطور يخضع للتطورات السريعة و المتلاحقة في مجال فن الحاسبات الآلية[2].

ولذلك فالمشرع الجزائري على غرار التشريع الفرنسي لم يعرف نظام المعالجة الآلية للمعطيات فأوكل بذلك مهمة تعريفه كل من الفقه و القضاء.

الاتفاقية الدولية للإجرام ألمعلوماتي [3]قدمت تعريف للنظام ألمعلوماتي في مادتها الثانية على النحو التالي:

Système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnecté ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement ou tonatisé des données.

بناء على التعريفات السابقة، تخلص إلى أن تعريف نظام المعالجة الآلية للمعطيات يعتمد على عنصرين:

1- عامر قنديلجي، علاء الدين الجنابي، نظام المعلومات المحوسب، المنشاوي للدراسات و البحوث، المقال متوفر على الموقع التالي : http://www.minshawi.com

[2] – علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي ،كلية الحقوق، مصر،1999، ص ص 119-120.

[3]- المادة 01 من الاتفاقية الدولية للإجرام ألمعلوماتي.- ملحق الرسالة رقم 1.

للاطلاع على النص الكامل لاتفاقية الإجرام السيبيري و لمعرفة مزيد من التفاصيل حول تطبيق هذه الاتفاقية ، يرجى مراجعة الموقع الالكتروني الخاص بالمجلس الأوروبي .

http///www.coe.int/t/e/legal-affairs/legal-co-operation.

http://www.conventions.coe.int/treaty/EN/treaties/html/185.htm

1. العنصر الأول: مركب يتكون من عناصر مادة ومعنوية،مختلفة ترتبط بينهما نتيجة علاقات توحدهما نحو تحقيق هدف محدد.

2. العنصر الثاني: ضرورة خضوع النظام لحماية فنية.

د- مكونات نظام المعالجة الآلية للمعطيات :

العناصر المادية والمعنوية التي يتكون منها المركب ومثال ذلك: الذاكرة، البرامج، المعطيات, أجهزة الربط... الخ، هذه العناصر واردة على سبيل المثال لا الحصر.

وهذا يفتح المجال أمام إضافة عناصر جديدة أو حذف بعضها حسب ما يفرزه التطور التقني في هذا المجال،وعلى ذلك لا يتوافر نظام المعالجة الآلية للمعطيات، ولا تقع بالتالي أي جريمة من جرائم الاعتداء عليه المنصوص عليها إذا وقع الاعتداء على برامج معروضة للبيع،أو على جهاز حاسب لم يدخل الخدمة أو على عنصر مودع بالمخازن، أو على قطع الغيار، أو على الأجهزة التي مازالت في حالة التجربة، أو حتى الأنظمة التي خرجت من الخدمة تماما و لكن على العكس من ذلك، تقع الجريمة إذا وقع الاعتداء على النظام خارج ساعات تشغيله العادية، أو إذا كانت أحد عناصره في حالة عطل أو حتى لو كان النظام كله في حالة عطل تام، و كان يمكن إصلاحه.

و تقع الجريمة أيضا إذا وقع الاعتداء على عنصر يشكل جزءا من أنظمة متعددة، فإذا تصورنا عدة أنظمة ترتبط فيما بينها بأجهزة اتصال،و وقع اعتداء على جهاز حاسب آلي في نظام من تلك الأنظمة المرتبطة، فإن الجريمة تقع في هذه الحالة، و إذا كان الدخول إلى هذا الجهاز مشروع ،فإن البحث في توافر الجريمة يتوقف على ما إذا كانت توجد علاقة سببية بين هذا الدخول المشروع و الاعتداء المفروض على الأنظمة ككل، ومدى حسن أو سوء نية المتدخل كما تقع الجريمة،إذا وقع الاعتداء على شبكة الاتصال التي تربط بين أكثر من نظام، لأن تلك الشبكة تعتبر عنصر في كل نظام من الأنظمة التي تربط بينهما [1].

ه- ضرورة خضوع النظام لحماية فنية

[1] – علي عبد القادر القهوجي، المرجع السابق، ص 121.

يسعى المتخصصون بأمن المعلومات،للحفاظ على خصوصية البيانات المتناقلة عبر الشبكات،وبالأخص حاليا شبكة الانترانت فهم يسعون لتامين سرية الرسائل الالكترونية وسرية البيانات المتناقلة،وخاصة بالأعمال التجارية الرقمية، ويمثل التشفير أفضل وسيلة للحفاظ على سرية البيانات المتناقلة، ويرى الخبراء ضرورة استخدام أسلوب التشفير لمنع الآخرين من الاطلاع على الرسائل الالكترونية [1]:

و تنقسم الأنظمة إلى ثلاثة أنواع :

1. أنظمة مفتوحة للجمهور.
2. أنظمة قاصرة على أصحاب الحق فيها ولكن بدون حماية فنية.
3. أنظمة قاصرة على أصحاب الحق فيها و تتمتع بحماية فنية.[2]

و مقتضى تطبيق هذا العنصر أن النوع الثالث فقط من تلك الأنظمة هو الذي يتمتع بالحماية الجنائية أما النوع الأول و الثاني فلا يتمتعان بتلك الحماية، و هناك من يصرون عليه لأن الحماية الجزائية في نظرهم يجب أن تقتصر على الأنظمة المحمية، فنيا لأنه من الطبيعي في نظرهم، أن ما يقوم بالاستغلال يضع الوسائل الفنية اللازمة لمنع الغش و أن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم، و ليس من يهمل منهم في توفير الحد الأدنى لحماية أمواله، و يكون دور القانون الجنائي في هذه الحالة دور وقائي و هذا أيضا هو ما يتفق و سياسة المشرع الجنائي و ما نلاحظه من المفهوم العام للحماية الجزائية للملكية.

بالرجوع إلى النصوص المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات،لا تتضمن شرط الحماية الفنية و خرجت تلك النصوص الخالية منه تماما.

و من المبادئ العامة المستقرة في تفسير القانون الجنائي،أنه لا يجوز تقييد النص المطلق، أو تخصيص النص العام، إلا إذا وجد نص يجيز ذلك،و لا يوجد في حالتنا نص خاص يقيد إطلاق النص أو يخصص عمومه، و لذلك فإن عدم ذكر المشرع لشرط الحماية الفنية يعني أن المشرع

[1] – أمال قارة، المرجع السابق، ص 103.

[2] – مزياني عبد الغني ،الجرائم الماسة بأنظمة المعالجة الآلية للمعلومات،مجلس قضاء المسيلة ،وزارة العدل ، ص11 .

أراد استبعاده، هذا بالإضافة إلى أن الحماية الجزائية يجب أن تمتد لتغطي كل أنظمة المعالجة الآلية للمعطيات،سواء كانت تتمتع بحماية فنية أم لا.

و تطبيقا لذلك، فإنه لا يشترط لوجود الجريمة أن يكون الدخول إلى النظام مقيدا بوجود حماية فنية،و لكن إذا نظرنا للوقائع، نلاحظ أن غالبية أنظمة المعالجة الآلية للمعطيات تتمتع بنظام حماية فنية، بالإضافة إلى أن وجود مثل تلك الحماية يساعد على إثبات أركان الجريمة و بصفة خاصة الركن المعنوي[1].

أما عن الأركان الأساسية : فتتمثل فيما يلي :

- الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات.
- الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات.
- الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام.

هذه الاعتداءات تتطلب وجود نظام المعالجة الآلية للمعطيات،كشرط مسبق بخلاف الاعتداءات على منتوجات النظام و سنتعرض إليها بالتفصيل فيما يلي:

البند الثاني: الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات

Unauthorized Access [2] تعد أنشطة الدخول أو التوصل غير المصرح به أو غير المخول به بين جرائم الكمبيوتر والانترنت . *most windespread* ، الانشطة الجرمية الأكثر انتشارا[3]

الركن المادي :

ويقوم التوصل غير المصرح به بالأساس، على الدخول إلى نظام الحاسوب أو شبكة المعلومات، عادة من خلال استخدام وسيلة اتصال عن بعد كالموديم *modem* أو من خلال التوصل عبر نقاط الاتصال والموجهات، الموجودة على الشبكة للدخول إلى نظام كمبيوتر معين بغرض التوصل مع البيانات أو البرامج المخزنة في النظام، ويتطلب هذا النشاط غالبا تجاوز أو كسر

[1]– علي عبد القادر القهوجي، المرجع السابق، ص 123.

[2] – فشار عطاءالله ، المرجع السابق، ص 26.

[3]– هو التوصل أو الولوج دون تصيح إلى نظام أو مجموعة نظم عن طريق انتهاكات إجراءات الأمن، لمزيد من التفاصيل انظر، عبد الفتاح مراد، شرح النصوص العربي لاتفاقيات الجات و منظمة التجارة العالمية،الباب الثاني، مقررات و توصيات المؤتمر 15 للجمعية الدولية لقانون العقوبات، 4 –9،نوفمبر 1994، البرازيل ري ودي جانيرو، بشان جرائم الكمبيوتر ط 2، ص 45 .

إجراءات الحماية التقنية للنظام *Security system*، كتجاوز كلمة السر *password* وإجراءات التعريف والجدران النارية، وغيرها أو التوصل لنقطة ضعف في نظام حماية البرامج والنفاذ منها.

ومعظم الذين يرتكبون هذه الأنشطة بآلياتها التقنية المتعددة، تكون أنشطتهم مجردة عن أغراض لاحقة، ولا يكون هدفهم – في الغالب – الأضرار بالبيانات والملفات أو تدميرها *destroying data or files*، وفي الغالب يسعى مقترفو هذه الأنشطة إلى الاطلاع على المعلومات المحمية، غير أن حماية المعلومات من أخطار هذه الأنشطة، واحتمال تطور هذه الأنشطة من مجرد هدف الاطلاع إلى أهداف أكثر خطورة، كالتلاعب بالمعطيات أو إتلافها أو ارتكاب غير ذلك من جرائم الحاسوب، أو استخدام الدخول لارتكاب جرائم أخرى بواسطة الكمبيوتر، دفعت غالبية دول العالم إلى تجريم هذه الأنشطة، كما هو الشأن في قوانين كل الدول الأوروبية وأمريكا واليابان.

أما المشرع الجنائي الجزائري نص على هذه الحالة في المادة 394 مكرر قانون العقوبات: "يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"،تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 إلى 150000 دج".

كما نصت عليه المادة 02 من الاتفاقية الدولية للإجرام ألمعلوماتي[1].

[1] -Article 2 - Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique, Convention sur la cybercriminalité, Budapest, 23.*11*.2001.

الصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع، فيما الصورة المشددة، تتحقق بتوافر الظرف المشدد لها، ويكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.

الركن المعنوي :

جريمة الدخول أو البقاء داخل النظام،جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم و الإرادة.

فيلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء، و أن يعلم الجاني بأنه ليس له الحق في الدخول إلى النظام و البقاء فيه، و عليه لا يتوافر الركن المعنوي،إذا كان دخول الجاني أو بقاؤه داخل النظام مسموح به أي مشروع، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع،سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، كأن يجهل بوجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول، فإذا توافر القصد الجنائي بعنصريه العلم و الإرادة،فإنه لا يتأثر بالباعث على الدخول أو البقاء فيظل القصد قائما حتى و لو كان الباعث هو الفضول أو إثبات القدرة على المهارة و الانتصار على النظام [1] .

موقف القوانين المقارنة بشأن جريمة التوصل غير المصرح به مع نظام الكمبيوتر إن القوانين المقارنة التي وضعت لمواجهة جرائم الحاسوب، جرمت في غالبيتها، جريمة التوصل غير المصرح به مع نظام الحاسوب، لكنها تتفاوت في تحديد المراد بهذه الجريمة ، ففي القانون الفرنسي (1988 المعدل لعام 1994) يجرم المشرع مجرد التوصل مع نظام الحاسوب او البقاء فيه ، وكذلك ينهج ذات القانون البريطاني (1990) مع تباين في نطاق الأفعال المكونة للجريمة بين القانونيين[2] ، في حين نجد القانون الأمريكي (1984 والتشريعات اللاحقة عليه (يقرن فعل الاتصال بدون تصريح مع تحقيق نتائج محددة ، كالحصول على المعلومات أو استخدام النظام أو إتلاف المعطيات، وتتردد بقية القوانين محل الدراسة بين هذه الاتجاهات، فنجد قوانين معظم الولايات الأمريكية سلكت مسلك القانون البريطاني في تجريم مجرد التوصل مع نظام الحاسوب،

[1] – علي عبد القادر القهوجي، المرجع السابق، ص 136-137.

[2] -BENSOUSSAN Alain, Op. Cit , p. 198 ,Martin WASIK, Op. Cit, p. 632.

فنص قانون كاليفورنيا لعام 1985 على انه يعتبر مرتكبا لجنحة كل من دخل عمدا إلى منظومة أو شبكة حواسيب أو إلى برنامج أو بيانات عالما بحظر ذلك من قبل مالكها أو مستأجرها، ولعل مسلك القوانين الخاصة بالولايات الأمريكية، يستند إلى منهج مشروع القانون الفدرالي لحماية نظم الحاسوب لسنة 1984، الذي جرم في المادة الثانية الاتصال عمدا بغير تصريح لحاسوب أو بنظام حاسوب أو بشبكة تتضمن حاسوبا، ونجد مثلا : القانون السويسري ينتهج منهج القانون الأمريكي (قانون غش وإساءة استخدام الحاسوب لسنة 1984)، وعلى هدي مسلك القانونين الفرنسي والانجليزي سلكت معظم القوانين الأوروبية[1].

البند الثالث: الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات:

نصت عليه المادتين 05[2]و08[3]من الاتفاقية الدولية للإجرام المعلوماتي، لم يورد المشرع الجزائري نصا خاصا بالاعتداء ألعمدي على سير النظام،و اكتفى بالنص على الاعتداء ألعمدي على المعطيات الموجودة بداخل النظام،و ربما يجد ذلك تفسيره في أن الاعتداء على المعطيات،قد يؤثر على صلاحية النظام للقيام بوظائفه، وقد وضع الفقه معيارا للتفرقة بين الاعتداء على المعطيات و الاعتداء على النظام،على أساس ما إذا كان الاعتداء وسيلة أم غاية.

---

[1]- يونس عرب، تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، 8 ديسمبر, 2014، متوفر على الموقع التالي : http://www.assakina.com

[2] -Article 5 - Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération et la suppression de données informatiques, Convention sur la cybercriminalité, Budapest, 23.11.2001.

[3] -Article 8 - Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui par:
a. l'introduction, l'altération, l'effacement ou la suppression de données informatiques,
b. toute forme d'atteinte au fonctionnement d'un système informatique,
dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui, Convention sur la cybercriminalité, Budapest, 23.11.2001.

فإذا كان الاعتداء الذي وقع على المعطيات مجرد وسيلة، فإن الفعل يشكل جريمة الاعتداء ألعمدي على النظام، أما إذا كان الاعتداء الذي وقع على المعطيات غاية فإن الفعل يشكل جريمة الاعتداء ألعمدي على المعطيات.

سبق و أن ذكرنا أن الاعتداء على سير النظام الناجم عن الدخول أو البقاء غير المشروع لا يشترط أن يكون مقصودا، لكن الإشكال المطروح أن أفعال الاعتداء على سير النظام الناجمة عن الدخول المشروع للنظام تفلت من العقاب خاصة مع عدم وجود نص خاص بالاعتداء ألعمدي على سير النظام.

✓ الركن المادي :

يتمثل هذا السلوك المادي في فعل توقيف نظام المعالجة الآلية للمعطيات،من أداء نشاطه العادي و المنتظر منه القيام به، وإما في فعل إفساد نشاط أو وظائف هذا النظام، ولا يشترط أن يقع فعل التعطيل أو فعل الإفساد على كل عناصر النظام جملة، بل يكفي أن يؤثر على أحد هذه العناصر فقط سواء المادية جهاز الحاسب الآلي نفسه، شبكات الاتصال، أجهزة النقل ...الخ، أما المعنوية مثل البرامج و المعطيات.

✓ الركن المعنوي :

إن هذه الجريمة جريمة عمدية، إذ أن من المفترض أن أفعال العرقلة والتعطيل لا تكون إلا عمدية، وهذا ما يميزه عن الاعتداء غير ألعمدي لسير النظام الذي يشكل ظرفا مشددا لجريمة الدخول والبقاء الغير مشروع داخل النظام،وعليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة[1].

البند الرابع: الاعتداءات العمدية على المعطيات

تنقسم جرائم الدخول غير المشروع على أجهزة الكمبيوتر إلى صنفين من الجرائم[2]، جرائم الدخول غير المشروع في حد ذاته، والدخول غير المشروع بقصد ارتكاب جريمة أخرى.

[1] – علي عبد القادر القهوجي، المرجع السابق، ص142.

[2]- فشار عطاء الله ، المرجع السابق ، ص 29.

ويشمل هذا الجزء جرائم القرصنة « *hacking*» والاختراق« *cracking* » الشهيرة حيث يقوم شخص غير مرخص له بالدخول على نظام كمبيوتر معين، ويشمل ذلك أيضا اعتراض البيانات بشكل غير مصرح به.

ولكن هل يشكل الشروع الخائب جُرما؟ وهل مجرد الدخول على جهاز كمبيوتر بشكل غير مشروع يدخل ضمن هذا الجزء من جرائم الإنترنت؟ وينبغي الحذر من تجريم الدخول غير المشروط بدون استثناء؛ فثمة حالات كثيرة يكون فيها هذا الدخول مشروعا مثل النظر غير المتعمد في محتويات أجهزة محمولة[1].

نصت عليها المواد 03 [2]04[3]، من الاتفاقية الدولية للإجرام ألمعلوماتي.

[1]– إيهاب ماهر السنباطي،الجرائم الإلكترونية، قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد، مداخلة في الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر،16-20 يونيو 2007 بالمملكة المغربية ص 24.

[2] –Article 3 - Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique, Convention sur la cybercriminalité , Budapest, 23.11.2001.

[3] –Article 4 - Atteinte à l'intégrité des données

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux, Convention sur la cybercriminalité , Budapest, 23.11.2001.

و المادة 08[1]، من الاتفاقية الدولية للإجرام ألمعلوماتي.

كما نص المشرع الجزائري عليها في المادة 394 مكرر2 في قانون العقوبات «يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة من 500000 دج إلى 2000000 دج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريقة الغش المعطيات التي تتضمنها».

✓ **الركن المادي :**

– الصورة الأولى: الاعتداءات العمدية على المعطيات الموجودة داخل النظام،النشاط الإجرامي في جريمة الاعتداء ألعمدي على المعطيات،يتجسد في إحدى الصور الثلاث التالية[2]:

1. الإدخال *L'intrusion*[3].

---

[1] –Article 8 - Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui par:

a. l'introduction, l'altération, l'effacement ou la suppression de données informatiques,

b. toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, Convention sur la cybercriminalité , Budapest, 23.11.2001.

[2] – أمال قارة، المرجع السابق، ص 120.

[3] – الإدخال L'intrusion:

يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية، أم كان يوجد عليها معطيات من قبل، و يتحقق هذا الفعل في الغرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة، هاته الأخيرة ليسحب بمقتضاها النقود من أجهزة السحب الآلي، و ذلك حين يستخدم رقمه الخاص و السري للدخول لكي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه، و كذلك الحامل الشرعي لبطاقة الائتمان و التي يسدد عن طريقها مبلغ أكثر من المبلغ المحدد له و بصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو الفقد أو التزوير، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب« فيروس...الخ» يضيف معطيات جديدة .

2. المحـــــو *L'effacement*[1].

3. التعديل *Modification*[2].

لا يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقـــط لكي يتوافر الركـــن المـــادي، وأفعال الإدخال و المحو و التعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات،سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل و هذا يعني أن النشاط الإجرامي، في هذه الجريمة إنما يرد على محل أو موضوع محدد،و هو المعطيات أو المعلومات التي تمت معالجتها آليا،و التي أصبحت مجرد إشارات أو رموزا تمثل تلك المعلومات، و ليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة، كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام، أي التي يحتويها النظام و تشكل جزءا منه.

لا تقع الجريمة على مجرد المعلومات التي لم يتم إدخالها بعد إلى النظام،أو تلك التي دخلت، و لم يتخذ حيالها إجراءات المعالجة الآلية، أما تلك التي في طريقها إلى المعالجة حتى و لو لم تكن المعالجة قد بدأت بالفعل تتمتع بالحماية الجنائية، و يكون هناك مجال للقول بتوافر الجريمة التامة أو الشروع على حسب الأحوال.

---

[1]- المحـــــو L'effacement :

يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة و الموجودة داخل النظام أو تحطيم تلك الدعامة، أو نقل و تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.

[2]- التعديل Modification:

يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام و استبدالها بمعطيات أخرى، و يتحقق فعل المحو و التعديل عن طريق برامج غريبة بتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها و ذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات و برنامج الممحاة Gomme d'effacement أو برنامج الفيروسات بصفة عامة، و هذه الأفعال المتمثلة في الإدخال و المحو و التعديل وردت على سبيل الحصر فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى و لو تضمن الاعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات فلا يخضع لتلك الجريمة فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب فيما بينهما، لأن كل تلك الأفعال لا تنطوي لا على إدخال و لا على تعديل بالمعنى السابق.

– ومن بين الأمور التي ينبغي أن توضع في الاعتبار ما إذا كان التعديل غير المشروع ،لا يؤثر على محتوى نظام الكمبيوتر، أو ما إذا كان هذا التعديل قد أدى بالفعل إلى تحسين نظام الكمبيوتر ،وقد يؤثر التعديل غير المشروع أيضا على حقوق الطبع والنشر، مثلما يحدث عندما تضبط شركات البرمجيات برامجها بحيث لا تعمل بشكل ملائم إذا لم يدفع العميل في الوقت المحدد، إيهاب ماهر السنباطي، الجرائم الإلكترونية ، مرجع سابق، ص 26.

تجدر الإشارة إلى أن الحماية الجنائية،تشمل المعطيات طالما أنها تدخل في نظام المعالجة الآلية، أي طالما كان يحتويها ذلك النظام و كانت تكون وحدة واحدة مع عناصره و يترتب على ذلك أن الجريمة،لا تتحقق إذا وقع النشاط الإجرامي على المعطيات خارج النظام سواء قبل دخولها أم بعد خروجها،و حتى ولو لفترة قصيرة، كما لو كانت مفرغة على قرص أو شريط ممغنط خارج النظام، فالحماية الجنائية تقتصر على المعطيات التي توجد داخل النظام أو تلك التي في طريقها إلى الدخول إليه، أو تلك التي دخلت بعد خروجها، و لا يشترط أن تقع أفعال الإدخال و المحو و تعديل المعطيات بطريق مباشر بل يمكن أن يتحقق ذلك بطريق غير مباشر سواء عن بعد أم بواسطة شخص ثالث .

– الصورة الثانية: المساس ألعمدي بالمعطيات خارج النظام

وفر المشرع الجزائري الحماية الجزائية للمعطيات في حد ذاتها من خلال تجريمه السلوكات التالية:

1- نص المادة 394 مكرر2 يستهدف حماية المعطيات في حد ذاتها،لأنه لم يشترط أن تكون داخل نظام المعالجة الآلية للمعطيات أو أن يكون قد تم معالجتها آليا، فمحل الجريمة هو المعطيات سواء كانت مخزنة كأن تكون مخزنة على أشرطة أو أقراص،أو تلك المعالجة آليا،أو تلك المرسلة عن طريق منظومة معلوماتية، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

2- نص المادة 394 مكرر 2/2 يجرم أفعال الحيازة، الإفشاء، النشر، الاستعمال، أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها،من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات بأهداف المنافسة غير المشروعة، الجوسسة، الإرهاب، التحريض على الفسق ...الخ.

✓ الركن المعنوي [1]:

جريمة الاعتداء ألعمدي على المعطيات، جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، كما يجب أن يعلم الجاني بان نشاطه الجرمي يترتب عليه التلاعب في المعطيات، ويعلم

[1] – فشار عطاءالله ، المرجع السابق، ص 32-33

أيضا أن ليس له الحق في القيام بذلك وانه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته [1] .

كما يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش [2]،لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير، بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل، مع العلم بذلك واتجاه الإرادة إليه [3]، وان كان الضرر قد يتحقق في الواقع نتيجة النشاط الإجرامي إلا انه ليس عنصرا في الجريمة .

الفرع الثاني: القانون04/09المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال

كان لا بد وأن تصاحب الثورة المعلوماتية، تدخلاً تشريعياً لتوفير البيئة الملائمة للتداول والاستخدام المشروع للتقنية المعلوماتية، وما يمكن إستشافه حول القانون09 -04 [4]

---

[1] علي عبد القادر القهوجي، المرجع السابق، ص145.

[2]- بالنسبة للمشرع الفرنسي تنص المادة 323-3 على معاقبة كل من يقوم بـــ"إدخال بيانات بطريق الغش في نظام المعالجة الآلية للبيانات أو محوها أو التعديل بطريق الغش للبيانات التي يحتوي عليها بالحبس لمدة خمس سنوات وبغرامة مقدارها 75 ألف يورو من القانون 88-19 الفرنسي المتعلق بالاحتيال و الغش المعلوماتي .

[3]- المادة 323 من هذا القانون لهذا الغرض، حيث تم تعديل الصياغة وتشديد العقاب، لتنص في فقرتها 2 المعدلة على " يعاقب كل من يقوم بـــ"تعطيل أو إفساد تشغيل نظام المعالجة الآلية للبيانات بالحبس لمدة خمس سنوات وغرامة مقدارها 75 ألف يورو".من القانون الفرنسي 88-19 .

[4]- القانون رقم 09-04 الذي تضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، مؤرخ في 14 شعبان عام 1430، الموافق 05 /08 /2009،ج.ر.ر رقم 47،صادق المجلس الشعبي الوطني الجزائري في الأربعاء 8 يوليو 2009 م بالإجماع على مشروع القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، إلا أن تطبيق النصوص القانون فعلي ، بعدما أهملت الجوانب الكفيلة بتصنيف هذه الجرائم و تحديد العقوبات المناسبة، و اقتصرت في اغلب الأحيان على الغرامة المالية .

و يتضمن القانون (19) مادة موزعة على (6) فصول، أعده نخبة من رجال القانون بمشاركة خبراء و مهنيين مختصين في مجال الإعلام الالكتروني من كافة القطاعات المعنية، و يتضمن القانون أحكاما خاصة بالمراقبة الالكترونية التي لا يجوز إجراؤها ، إلا بإذن من السلطة القضائية المختصة و في حالات تم تحديدها، و هي الأفعال الموصوفة بجرائم الإرهاب و التخريب و الجرائم الماسة بأمن الدولة، أو حالة توفر معلومات عن اعتداء محتمل يهدد منظومة من المنظومات لمؤسسات الدولة أو الدفاع الوطني أو النظام العام، و ينص القانون أيضا على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيا الإعلام و الاتصال و مكافحته، تتولى تنشيط و تنسيق عمليات الوقاية من الجرائم المعلوماتية ، و مساعدة السلطات القضائية و مصالح الشرطة في التحريات التي تجريها بشان هذه الجرائم، و تتكفل اللجنة أيضا بتبادل المعلومات مع الخارج ،طارق إبراهيم الدسوقي عطيه ، مرجع سبق ذكره ، ص 278.

انه يحاكي ويتواءم مع أحكام كل من الاتفاقية العربية لمكافحة الجرائم المعلوماتية، التي صادقت عليها الجزائر سنة2014، و اتفاقية الجرائم المعلوماتية *"Cyber Crime Convention"* " الخاصة بمجلس أوروبا "*Council of Europe*" الموقعة في بودابست في 23 نوفمبر 2001.[1]

أرسى القانون04 -09 قواعد إجرائية جديدة تستطيع معها أجهزة إنفاذ القانون، ممارسة إجراءات خاصة تتوافق و طبيعة الجرائم الإلكترونية، إذ تضمن الفصل الثالث من هذا القانون القواعد الإجرائية الخاصة بالتفتيش و الحجز في مجال الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال، وذلك وفقا للمعايير العالمية المعمول بها في هذا الشأن، إذ خول هذا القانون لأجهزة إنفاذ القانون الدخول و التفتيش، ولو عن بعد إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة، من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي(المادة الخامسة)، كما سمح القانون المذكور باستنساخ المعطيات محل البحث، في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها (المادة السادسة)، بالإضافة إلى الإلتزامات التي ألقاها هذا القانون على مقدمي الخدمات، وذلك بمساعدة السلطات العمومية في مواجهة هذه الجرائم و الكشف عن مرتكبيها و ذلك من خلال الفصل الرابع من نفس القانون[2]، حيث فرض المشرع

---

[1]– وقد انضمت إليها (26) دولة منها فرنسا والدنمارك وألمانيا وإيطاليا وهولندا والنرويج والولايات المتحدة الأمريكية، كما تم التوقيع عليها من قبل عشرين دولة أخرى.

La Convention du Conseil de l'Europe sur la cybercriminalité est le premier texte international ,à se pencher sur ce nouvau fléau.

- La Convention traite en particulier des infractions portant atteinte aux droits d'auteur, de la fraude liée à l'informatique, de la pornographie enfantine, ainsi que des infractions liées à la sécurité des réseaux. Elle contient également une série de compétences procédurales, tels que la perquisition de réseaux informatiques et l'interception...

http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm(3of30) [23/11/2001 17:43:11
Vous pouvez consulter la convention elle-même, et son guide explicatif.
http://www.droit-technologie.org/legislation-82/convention-internationale-sur-la-cybercriminalite.html.

[2]– يوسف صغير، الجريمة المرتكبة عبر الانترنيت، مذكرة ماجستير في القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، الجزائر، سنة 2013، ص114.

الجزائري من خلال المادتين 10و 11من قانون 04/09المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها، على مقدمي الخدمات حفظ المعطيات، بشكل يسمح بالتعرف على الأشخاص المساهمين في إنشاء المحتويات على الانترنيت، وذلك من أجل التبليغات المحتملة للسلطات القضائية، أو في حال طلب هذه الأخيرة لأجل التحريات أو المعاينات أو المتابعات القضائية للجرائم المرتكبة[1] ، و القيام بحفظ المعطيات المتعلقة بحركة السير، منها المعطيات التي تسمح بالتعرف على مستعملي الخدمة وكذا الخصائص التقنية و تاريخ ووقت و مدة الإتصال .

كما عالج هذا القانون مسألة الإختصاص من خلال مقتضيات المادة 15حيث نصت هذه المادة " على أنه زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا و تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني ".

علاوة على هذه الآليات الإجرائية التي تضمنها القانون 04/09، فقد تضمن قانون الإجراءات الجزائي الجزائري، مجموعة من الآليات الخاصة بالتحريات و التحقيقات في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال مثل الآلية المتعلقة باعتراض المراسلات (المواد من 65 مكرر 5إلى المادة 65مكرر 10من قانون الإجراءات الجزائري[2]) ، كما سمح بامتداد

---

[1]- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام و الاتصال في ضوء القانون رقم 04/09، مذكرة ماجستير في القانون الجنائي، جامعة قاصدي مرباح ورقلة، الجزائر، سنة 2013، ص100 .

[2]- أمر رقم 02/15مؤرخ في 7 شوال 1436، الموافق ل 23جويلية2015، العدد 40 ، يعدل و يتمم الأمر رقم 155/66المؤرخ في 18صفر 1386الموافق ل 8جوان1966، و المتضمن قانون الاجراءات الجزائية.

المادة 65مكرر 5: اذا اقتضت ضرورات التحري في الجريمة المتلبس بها او التحقيق الابتدائي في جرائم المخدرات او الجريمة المنظمة العابرة للحدود الوطنية او الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات او جرائم تبييض الاموال او الارهاب او الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص ان يأذن بما يأتي:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.
- وضع الترتيبات التقنية، دون موافقة المعنيين، من اجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة او سرية من طرف شخص او عدة اشخاص في اماكن خاصة او عمومية او التقاط صور لشخص او عدة اشخاص يتواجدون في مكان خاص.

المادة 65 مكرر 6 : تتم العمليات المحددة في المادة 65 مكرر 5، دون المساس بالسر المهني المنصوص عليه في المادة 45 من هذا القانون. اذا اكتشفت جرائم اخرى غير تلك التي ورد ذكرها في اذن القاضي، فان ذلك لا يكون سببا لبطلان الاجراءات العارضة.

اختصاص الأجهزة المكلفة بالبحث و التحري، إلى كامل الإقليم الوطني إذا تعلق الأمر بجريمة إلكترونية من خلال المادة 16من قانون الإجراءات الجزائري، على امتداد اختصاص ضباط الشرطة القضائية، إلى كامل الإقليم الوطني إذا تعلق الأمر ببحث و معاينة لجرائم ماسة بأنظمة المعالجة الآلية للمعطيات، و كذا من خلال ما نصت عليه المادة 37على جواز امتداد الاختصاص المحلي للنيابة العامة إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[1]

فضلا على إنشاء هيئة وطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال سنة 2007 التي أعلن عنها المرسوم الرئاسي الصادر في شهر أكتوبر 2015 ،والتي تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل، وتتضمن أعضاء من الحكومة، مسؤولي مصالح الأمن وقاضيين اثنين من المحكمة العليا، يعينهما المجلس الأعلى للقضاء.

المادة 65 مكرر 7 : يجب ان يتضمن الاذن المذكور في المادة 65 مكرر 5 أعلاه، كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والاماكن المقصودة سكنية او غيرها والجريمة التي تبرر اللجوء الى هذه التدابير ومدتها. يسلم الاذن مكتوبا لمدة اقصاها اربعة (4) اشهر قابلة للتجديد حسب مقتضيات التحري او التحقيق ضمن نفس الشروط الشكلية والزمنية.

المادة 65 مكرر 8 : يجوز لوكيل الجمهورية او ضابط الشرطة القضائية الذي اذن له، ولقاضي التحقيق او ضابط الشرطة القضائية الذي ينيبه ان يسخر كل عون مؤهل لدى مصلحة او وحدة او هيئة عمومية او خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 65 مكرر 5 .

المادة 65 مكرر 9 : يحرر ضابط الشرطة القضائية المأذون له او المناب من طرف القاضي المختص، محضرا عن كل عملية اعتراض وتسجيل المراسلات، وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي او السمعي البصري، يذكر بالمحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها.

المادة 65 مكرر 10 : يصف او ينسخ ضابط الشرطة القضائية المأذون له، أو المناب المراسلات او الصور او المحادثات المسجلة والمفيدة في اظهار الحقيقة في محضر يودع بالملف، تنسخ وتترجم المكالمات التي تتم باللغات الاجنبية، عند الاقتضاء، بمساعدة مترجم يسخر لهذا الغرض.

أضيفت هذه المواد بموجب المادة 14 من القانون رقم 06-22مؤرخ في 20 ديسمبر 2006،ج.ر.عدد84 قانون الإجراءات الجزائية.

[1]- المادة 16من قانون الإجراءات الجزائري، غير أنه فيما يتعلق ببحث و معاينة جرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية، و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، و جرائم تبييض الأموال و الإرهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف، يمتد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني.

الفرع الثالث: أمن المعلومات بمقتضى قانون التصديق والتوقيع الالكترونيين الجزائري الجديد 2015.

القانون الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، [1] يضمن تأمين البيانات الشخصية وتسهيل المبادلات عبر الأنترنت.

كما ان القانون يهدف إلى إرساء جو من الثقة وحماية و تأمين البيانات الشخصية، وكذا تسهيل المبادلات والتبادلات عبر الانترنت" وتحسين الحياة اليومية للمواطنين والمؤسسات، وكل الفاعلين الاجتماعيين والاقتصاديين، عن طريق تجسيد التعاملات عن بعد، في كل الميادين كالتجارة الإلكترونية وسحب الوثائق الإدارية عن بعد و تعميم استعمال الدفع الإلكتروني عن طريق الانترنت"، وهو ما يستوجب استكماله بنصوص متعلقة بحماية البيانات الشخصية المنشورة عبر الانترنيت سيما من القرصنة".

ويتضمن القانون أحكاما تتعلق بتحديد الموضوع والتعريفات الخاصة بالمصطلحات المستعملة والمبادئ العامة، التي تسير نشاط التوقيع والتصديق الإلكترونيين، ويلتزم بموجب أحكام هذا الباب كل المتدخلين بضرورة تخزين المعطيات المتعلقة بالتصديق الالكتروني داخل التراب الوطني.

كما وخصص الباب الثاني من القانون إلى التوقيع الإلكتروني، الذي يضمن سلامة المعطيات وهوية الأطراف ووظيفته ومعايير تطابقه مع الإمضاء الخطي، كما يتضمن كذلك المتطلبات التي يجب توفرها في أجهزة الإنشاء والتحقق من التوقيع الإلكتروني لضمان أمن هذه الأخيرة.

أما الباب الثالث من القانون فقد خصص للتصديق الالكتروني الذي يبدأ بتحديد المتطلبات الواجب توفرها في المصادقة الالكترونية، ويصف التنظيم المعتمد المتمثل في إحداث سلطة وطنية للتصديق الإلكتروني.

---

[1]- قانون رقم 15-03 يتعلق بعصرنة العدالة و قانون رقم 15 - 04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني. صدر كلا القانونين في 20 ربيع الثاني 1436، الموافق ل 10فبراير 2015، العدد 06.

ويحدد الباب الرابع من مشروع القانون العقوبات المالية والإدارية التي تطبق في حالة إخلال المؤدي بالتزاماته، وكذا العقوبات الجزائية في حالة الإخلال بأحكام هذا النص، في حين يتضمن الباب الخامس أحكاما انتقالية ضرورية للتكفل بالكيانات العاملة حاليا في هذا المجال، ودمجها تدريجيا في النظام الجديد كالضمان الاجتماعي و البنوك[1].

المطلب الثاني : الشق الإجرائي و الأكاديمي لإستتباب الأمن الرقمي في الجزائر

الجرائم الرقمية في الجزائر تندرج ضمن قسمين؛ الأول خاص بالجرائم المتصلة بتكنولوجيا الإعلام و الاتصال[2]، أي أن أي جريمة مهما كانت إذا تمت بواسطة الانترنت أو الهاتف النقال، وكأمثلة عن ذلك المساس بحرمة الأشخاص أو الهيئات العامة، كنشر صور أشخاص أو تهديدهم بفعل ذلك، التحريض على الإخلال بالنظام العام، ونشر صور مخلة بالحياء خاصة إذا تعلقت بالأطفال، أما القسم الثاني متعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، أو ما يعرف بالقرصنة التي تستهدف الأنظمة المعلوماتية من خلال الدخول غير الشرعي في النظام المعلوماتي، لشخص أو جهة معينة والعمل على إزالة، تعطيل، أو إضافة معلومات جديدة بغرض سرقتها أو التجارة بها.

الفرع الأول : المستحدات الإجرائية في القانون الجزائري [3]

1. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال
2. الهيئات القضائية المتخصصة
3. أساليب التحري الخاصة

---

[1] - http://www.aps.dz.

[2] - القانون رقم 09-04 المؤرخ في 2009/08/05 الذي تضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، محاولا بذلك وضع إطار قانوني يتلاءم مع خصوصية الجريمة الافتراضية، و يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية، التي تسمح بالرصد المبكر للاعتداءات المحتملة و التدخل السريع لتحديد مصدرها و التعرف على مرتكبيها.

[3] -Bensalem Abderezak, Investigating Judge at the Tribunal of Sidi M'Hamed, THE Algerian legal system to fight against cyber criminality .

البند الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال

أنشئت بموجب القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

يقصد بالجرائم المتصلة بتكنولوجيات الإعلام و الاتصال جرائم المساس بأنظمة المعالجة الآلية للمعطيات،و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال:

1. إدارة وتنسيق عمليات الوقاية.
2. المساعدة التقنية للجهات القضائية والأمنية،مع إمكانية تكليفها بالقيام بخبرات قضائية.
3. تفعيل التعاون القضائي و الأمني الدولي .

الحالات التي تسمح بمراقبة الاتصالات الإلكترونية لأغراض وقائية:

1. الوقاية من جرائم الإرهاب والجرائم الماسة بأمن الدولة،بإذن من النائب العام لدى مجلس قضاء الجزائر لمدة ستة أشهر قابلة للتجديد.
2. الوقاية من اعتداءات على منظومات معلوماتية،على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني،بإذن من السلطة القضائية المختصة [1]

البند الثاني: الهيئات القضائية المتخصصة

أنشئت بموجب القانون 14/04 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية والتي تختص ب:

[1] - Meriem ALI MARINA ,Centre de prévention et de lutte contre la criminalité informatique et la cybercriminalité, N° 98 – Août2016,Disponible: www.eldjazaircom.dz/index.php?id_rubrique=314&id_article=4567

1. الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (المواد37[1] و المادة 40 [2]من قانون الإجراءات الجزائية) .

2. اختصاص إقليمي موسع ،المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05

3. إمكانية قيام اختصاص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني (المادة15 من القانون رقم 09/04)[3] .

4. توسيع صلاحيات الضبطية القضائية عند معاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

5. تمديد الاختصاص المحلي إلى كامل الإقليم الوطني[4] .

---

[1]- المادة 37 يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، وبمحل إقامة احد الأشخاص المشتبه في مساهمتهم فيها، او بالمكان الذي تم في دائرته القبض على احد هؤلاء الأشخاص، حتى ولو حصل هذا القبض لسبب اخر.
-يجوز تمديد الاختصاص المحلي لوكيل الجمهورية الى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الاموال والارهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، أضيفت بموجب المادة الثالثة من قانون رقم 04-14 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 الذي يعدل ويتمم قانون الإجراءات الجزائية.

[2]- المادة 40: يتحدد اختصاص قاضي التحقيق محليا ،بمكان وقوع الجريمة أو محل إقامة احد الأشخاص المشتبه، في مساهمتهم في اقترافها أو بمحل القبض على احد هؤلاء الأشخاص، حتى ولو كان هذا القبض قد حصل لسبب آخر.يجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، أضيفت بموجب المادة الثالثة من قانون رقم 04-14.

[3]- المادة 15 من قانون 09/04 ، الفصل السادس تحت عنوان التعاون و المساعدة القضائية الدولية – الاختصاص القضائي – زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر الى الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال المرتكبة خارج الإقليم الوطني ، عندما يكون مرتكبها أجنبيا و تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني .

[4]- المادة 16من قانون الإجراءات الجزائية"...غير انه فيما يتعلق ببحث و معاينة جرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ...يمتد اختصاص ضباط الشرطة القضائية إلى كامل التراب الإقليم الوطني ..."

6. إمكانية تفتيش المحلات السكنية و غير السكنية في كل ساعة من ساعات الليل و النهار بإذن من وكيل الجمهورية [1] وإمكانية تفتيش المساكن دون حضور المشتبه فيه أو صاحب المسكن ,و دون شهود (المادة45 من قانون الإجراءات الجزائية)

7. إمكانية تمديد فترة التوقيف للنظر مرة واحدة في حالة التلبس (المادة 51 من قاون الإجراءات الجزائية)

البند الثالث: أساليب التحري الخاصة

1. اعتراض المراسلات الإلكترونية (المادة 65 مكرر 5من قانون الإجراءات الجزائية المدرجة بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006) .[2]

2. التسرب(المادة 65 مكرر 11من قانون الإجراءات الجزائية المدرجة بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006)[3] .

3. تفتيش المنظومة المعلوماتية (المادة 5 القانون رقم 04/09)[4] .

4. إمكانية تمديد التفتيش إلى منظومة أخرى يمكن الدخول إليها انطلاقا من المنظومة الأولى .

---

[1]- المادة 47 من قانون الإجراءات الجزائية"...و عندما يتعلق الأمر ب جرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات...فانه يجوز إجراء التفتيش و المعاينة و الحجز، في كل محل سكني أو غير سكني،في كل ساعة من ساعات النهار أو الليل،و ذلك بناءا على إذن مسبق من وكيل الجمهورية المختص..".

[2]-المادة 65 مكرر 5 من الفصل الرابع في اعتراض المراسلات و تسجيل الأصوات و التقاط الصور "إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ... يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي ك

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية.

- وضع الترتيبات التقنية ،دون موافقة المعنيين من أجل التقاط و تثبيت و بث و تسجيل الكلام المتفوه بها بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط لشخص أو عدة أشخاص يتواجدون في مكان خاص .

[3]- المادة 65 مكرر 11 " عندما تقضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 أعلاه ، يجوز لوكيل الجمهورية أو لقاضي التحقيق ، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ..."

[4]- يجوز للجهات القضائية وضباط الشرطة القضائية الدخول، بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي، ويسمح القانون للمحققين باستنساخ المعطيات محل البحث، في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أو مرتكبيها.

5. حجز المعطيات المعلوماتية (المادة 6 القانون رقم 04/09).
6. نسخ المعطيات على دعامة تخزين إلكترونية.
7. إمكانية منع الوصول إلى معطيات تحتويها المنظومة .
8. منع الإطلاع على المعطيات التي يشكل محتواها جريمة.

الفرع الثاني : تشكيل أمني جزائري مختص للردع والوقاية من الجرائم العنكبوتية .

استجابت مصالح الأمن الجزائرية لمطلب الأمن المعلوماتي، ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية، من خلال إنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية.

أن المصلحة " كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترّونية على مستوى المديرية العامة للأمن الوطني، والتي أنشأت سنة 2011 ،ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي2015.

وفي المرحلة الثانية من تشكيل المصلحة المركزية لمكافحة الجريمة الإلكترونية ،" تم توسيع التشكيل الأمني بتكوين فصائل على مستوى أمن الولايات 48،حيث تم القيام بعملية انتقاء لـــ 100 عنصر شرطة ممن تتوفر فيهم شروط الميول، الكفاءة، الإطلاع الدائم على التكنولوجيات الحديثة ،الأنترنيت وشبكات التواصل الاجتماعي، أسفرت عن استحداث 48 فصيلة تابعة للمصالح الولائية للشرطة القضائية لأمن الولايات" [1].

[1]- تم تسجيل 129 قضية خاصة بالجرائم الإلكترونية تمكنت المصالح المختصة لجهاز الشرطة من معالجة 89 قضية منها تورط فيها 120 شخصا، يُذكر أن سنة 2014 قد شهدت 68 قضية خاصة بالجرائم الالكترونية عولجت منها 48 سمحت بتوقيف 53 شخصا متورطا وفق ما أشار إليه العرض المقدم بهذه المناسبة، وحسب نفس المسؤول فإن قضايا الجرائم الالكترونية، التي تم تسجيلها ومعالجتها تراوحت ما بين النصب والغش في مجال المعاملات التجارية عبر الأنترنت والتقليد وانتحال الهوية عبر الأنترنت، وكذا التشهير والمساس بالحياة الشخصية وكذا التزوير الإلكتروني للبيانات، وكذا تزوير البطاقات المغناطيسية، وأضاف وهراني أنه من بين قضايا الجرائم الإلكترونية التي تم معالجتها خلال 2015 يوجد 8 قضايا نوعية مرتبطة أيضا بمجال الشرطة الاقتصادية والمالية، كما ثمن المفتش الجهوي لشرطة الغرب المجهودات المبذولة في مجال مكافحة الجرائم التي تطال المال العام والاقتصاد الوطني منوها بارتفاع نسبة معالجة هذا النوع من القضايا على مستوى الولايات ال12، التي تدخل ضمن نطاق تخصص هيئته الجهوية والتي فاقت 82 بالمائة أي 1375 قضية معالجة من أصل 1665 مسجلة، المفتش الجهوي لشرطة الغرب مراقب شرطة محمد وهراني، ندوة صحفية لعرض الحصيلة السنوية لنشاطات مصالح الأمن الوطني بغرب البلاد لسنة .2015 ، http://elayem.com/2016/01/20

الفرع الثالث: تنسيق دولي بروتوكولي بين الجزائر و مكتب التحقيقات الفيدرالي

بخصوص أول قضية عالجتها المصلحة المركزية للجريمة الإلكترونية في الجزائر، كانت قضية ذات بعد دولي وقعت في نهاية سنة 2009 على إثر بلاغ من مكتب التحقيقات الفدرالية أف. بي. أي ،وتنقل ممثلين عنهم لتقديم بلاغ إلى السلطات الجزائرية بسبب تعرّض شركة أمريكية إلى عملية قرصنة بخصوص بيانات بنكية، وتبيّن من التحقيق أنها منظمة إجرامية تنشط في مجال الإختراق والقرصنة ولها شريك في الجزائر ،وبعد وصول البلاغ الأجنبي تم توجيه الملف إلى مصالح مديرية الشرطة القضائية فتشكل فوج للتحقيق متكون من ثلاثة عناصر، حيث أسفرت التحريات المكثفة عن تحديد مكان وهوية الشخص الذي اتضح أنه يقطن بإحدى ولايات الشرق الجزائري، حيث تمكنت المصلحة من إثبات كفاءة الشرطة الجزائرية بتحديد هويته وتقديمه للعدالة".

كما و التعاون القضائي بين الجزائر والولايات المتحدة الأمريكية تدعّم أكثر بعد إمضاء اتفاقية التعاون في المجال الجزائي بين البلدين خلال زيارة وزير العدل الأمريكي إيريك هولدر إلى الجزائر في أفريل 2010، والتي هدفت إلى تحسين التعاون في مجال مكافحة الجرائم والتبادل الجيد للأدلة التي بإمكان المسؤولين في كلا البلدين استعمالها في سياق التحقيق ومقاضاة النشاط الإجرامي[1].

الفرع الرابع: اتفاقية حول التعاون الأكاديمي لحماية أمن الشبكات الإلكترونية بين الجزائر وفنلندا

أبرمت الجزائر وفنلندا -بالجزائر العاصمة- اتفاقية-إطار تتعلق بالتعاون الأكاديمي حول أمن الشبكات الإلكترونية .و هذه الاتفاقية الموقعة بين وزارة البريد و تكنولوجيات الإعلام و الاتصال و شركة "ستونسوفت" الفنلندية على هامش استقبال وزير القطاع موسى بن حمادي للوزير الفنلندي للشؤون الأوروبية و التجارة الخارجية ألكسندر ستوب، و ترمي الاتفاقية إلى "توسيع نطاق التعاون حول سبل مكافحة الجرائم الإلكترونية"، و كذا "تفعيل بروز كفاءات

[1] - http://www.algeriachannel.net

جزائرية في مجال أمن الشبكات، من خلال دمج التدريب في هذا التخصص ضمن مناهج الجامعات والمدارس الجزائرية"، و في هذا الصدد تقرر عقد شراكة بين "ستونسوفت" و ثلاث جامعات أو مدارس وطنية كبرى مع "ترك الباب مفتوحا أمام اقتراحات جديدة للتعاون في هذا المجال".

- و مما يزيد من أهمية هذه الاتفاقية تشجيع الجزائر لقطاعها البنكي، من أجل التوجه نحو التعاملات المالية في إطار مشروع البنك الإلكتروني (التجارة الإلكترونية).

- كما أنها تندرج ضمن استراتيجية قطاع تكنولوجيات الإعلام والاتصال الهادفة إلى ضمان أمن المعلومات، عن طريق تجسيد الإطار المناسب الذي يسمح بتوفير الوسائل الأمنية الكفيلة، بحماية المواقع والخدمات على جميع المستويات.

- إن مكافحة الجريمة الإلكترونية يستوجب تعاون دولي لإرساء نظام دفاع دون ثغرات، كما شدد من جهة أخرى على ضرورة إرساء تعاون حقيقي مع الشركات الأجنبية عموما يقوم على الاستقرار بالجزائر وفق السياسة الاقتصادية الجديدة، التي تبنتها الجزائر و القاضية باشتراط فتح الشركات المستثمرة في الجزائر فروعا لها[1].

الفرع الخامس : برنامج تعاون بين الجزائر و إيران ضدّ الإجرام الرقمي.

شرع وفد من خبراء الشرطة الإيرانية، في دورة تكوينية لفائدة إطارات متخصصة، من الشرطة الجزائرية، حول الوقاية ومكافحة الجريمة السيبرانية و تم ذلك على مدار 5 أيام بتاريخ 2015-08-08.

وكان الهدف الأسمى من هذه الدورة هو الرفع من مستوى البوليس الجزائري حتى يعود قادرا على التعاطي بنجاعة اكبر مع الجرائم الرقمية المنتشرة عبر العالم، والتي يقف وراءها أفراد كما الجماعات المنظمة، حيث يركز برنامج التأطير على أمن الشبكات وحماية البيانات وضبط الأدلة الإلكترونية وتأمين التعاملات الإدارية والمالية[2].

[1] -www.press solidarity.dz le29 janvier 2013- et voir aussi: www.elkhabar.com

[2] - http://www.hespress.com/international/273166.html

كما هذا عن طريق تبادل الخبرات عن التشريعات الدولية، وأفضل الممارسات والمساعدة التقنية والتعاون الدولي، بغية تعزيز سبل مكافحة هذا النوع من الجرائم الحديثة.

كما جاء في بيان للمديرية العامة للأمن الوطني، أنه في إطار تجسيد مساعي اللواء عبد الغني هامل المدير العام للأمن الوطني في مجال الوقاية ومكافحة الجرائم السيبرانية، أتت هذه الدورة التكوينية عالية المستوى لمواجهة ارتفاع مستويات الجرائم السيبرانية، التي تعرفها دول العالم دون أي قيد جغرافي، حيث يستغل الأفراد والجماعات الإجرامية المنظمة، الفرص الجديدة المتاحة لارتكاب الجرائم بغية تحقيق الأرباح والمكاسب الشخصية، إذ ناقشت أمن الشبكات، وحماية البيانات الفردية، والتطرق إلى كيفيات ضبط الأدلة الإلكترونية الضرورية كمادة إثباتية، وتأمين التعاملات الإدارية والمالية عبر الشبكات.

كما تأتي أهمية هذه الدورة التكوينية، في مسايرة فرق المحققين من الشرطة الجزائرية لأحدث التكنولوجيات والتحكم فيها، والاطلاع على الأساليب المعتمدة دوليا في الوقاية والمكافحة من الجريمة السيبرانية، إذ يبذل الأمن الوطني جهودا معتبرة في الوقاية والتحسيس من هذه الجرائم الناجمة عن سوء استعمال الشبكة العنكبوتية، خاصة من طرف الشباب والأطفال.[21]

وما يمكن قوله و التأكيد عليه،في هذه الرسالة إن "أي دولة مهما بلغت من التطور لا يمكنها أن تكافح لوحدها أشكال الجرائم المتطورة، التي يستخدم مقترفوها وسائل تكنولوجية حديثة ومتطورة"[3].

فتعد المساعدة القانونية المتبادلة في المسائل الجنائية من الآليات الفعالة لمواجهة الجريمة[4].

---

[1]– وفي ظل وجود أزيد من 80 بالمائة من الأطفال في الجزائر يرون بأنه من الضروري حماية باقي الأطفال من أخطار الانترنت، والجرائم الالكترونية نتيجة مضاعفاتها الخطيرة،كمثال كشفت دراسة استطلاعية،قامت بها الهيئة الوطنية لترقية الصحة وتطوير البحث العلمي، أن 55.33 بالمائة من الأطفال تعرضوا لصدمة بسبب صور شاهدوها عبر النت

mostafa khiyati,Cybercriminalité et enfance en algerie, edition, FOREM 2007.p 58

[2] - http://www.echoroukonline.com/ara/articles/251604.html

[3] - For more: about the international solution see Yaman Akdaniz, Clive Walker and David Wall (eds.),The I n ternet, Law and Society, Longman Pearson Education, 2000, P. 12.

[4] -DENIS Flory ,Union Europeenne ,programme d' action criminlitc organisee , Rev inter d dr P , Vol 68. Tri 1.2 , 1997 .PP 338 -339.

الخاتمة

الخاتمة.

إن أي رحلة في المسالك المتشعبة لشبكة الإنترنت الأخطبوطية، يتلمس للجوانب المعرفية التي تفرزها هذه الشبكة، وبالتالي طبيعة الانتهاكات القانونية التي يمكن أن تباشر من خلال فضائها الحاسوبي الكوني، الذي لم يعد يعير اهتماما لمفاهيم الزمان والمكان التقليديين، ويرسى مفاهيم وأطرا معرفية جديدة، تلفت الانتباه إلى ضرورة مباشرة عملية معالجة قانونية محكمة لمسألة الانتهاكات السائدة في الفضاء الافتراضي الحاسوبي بشبكة الإنترنت .[1]

فعادة عندما يأتي لنا العلم بجديد، سرعان ما تتعالى الصيحات بضرورة إصدار تشريعات خاصة لمواجهة المستجدات لتفادي الفراغ القانوني، الذي يترتب على ظهور المستجدات.

-من العرض السابق يتضح لنا أن القواعد العامة في خطوطها العريضة تواجد بكفاءة

المشكلات القانونية التي تنشأ عن الإنترنت، ولكن الأمر يحتاج إلى إتقان كامل لأصول قانون خاص لتطويعها، فهي تحتوي على المرونة الملائمة والتي تستمد من تجريد القاعدة القانونية، فالأمر يحتاج إلى رياضة ذهنية قانونية متقدمة، مع أنه لا بد من معرفة جيدة للأصول الفنية والتقنية التي تحكم المستجدات.

فمعرفة كيفية عمل الإنترنت، تلعب دوراً رئيسياً في التوصل إلى الحلول القانونية الملائمة،

ولا يرى اتخاذ الطريق السهل وهو التشريع الخاص لأن ذلك يهدد بخطرين، الخطر الأول احتمال التضارب وعدم التناسق بين التشريعات ولا يخفى تدني مستوى الصياغة التشريعية عن ذي قبل، والخطر الثاني وهو لا ينقطع الصلة بالأول وهو الإخلال بالاستقرار القانوني، فالتعديل قد لا يكون كافياً ويستتبع سلسلة من التعديلات التي تهدد الاستقرار... وانتظار التعديل التشريعي، يضعف قوة الصنع ويؤدي إلى التقاعس عن قدح الذهن لتطويع النصوص.

[1] - جابر إبراهيم الراوي ، الحدود الدولية، الطبعة1، مطبعة دار السلام، بغداد، 1975 ، ص8.

-كما اكتشفنا في إطار البحث عن المسائل المتعلقة بالأمن المعلوماتي أن :

المعلومة في هذا العصر تُعد كنز عظيم وهام لاسيما في ظل وجود تكنولوجيا المعلومات، التي ساهمت بشكل فعّال في معالجة، تخزين، وبث المعلومات؛ وبالتالي امتلاكها يُشكل قوة لصاحبها، لكن نجد أن إمكانية العدوان والتخريب والتجسس على هذه المعلومات يفرض علينا توفير قدر من الحماية يتناسب مع مستوى أهمية المعلومات، ونتيجة لتنامي ظاهرة العدوان على البيئة المعلوماتية، وتعدد اتجاهاته ليطال البرامج، الأجهزة، والاتصالات، إضافةً إلى المعلومات برز أمن المعلومات ليشكّل مجموعة الوسائل والطرق المعتمدة للسيطرة على كافة أنواع المعلومات وحمايتها، من أوجه العدوان المختلفة مع الحرص على عدم المبالغة التي قد تؤثر على عنصر الأداء وكذلك عدم التساهل في الإجراءات الأمنية، بشكل لا يكفل الحماية الواجبة، وقد ظهرت تقنيات متعددة في هذا المجال من الضروري توافرها لحماية المعلومات، وتجدر الإشارة إلى أهمية العنصر البشري ودوره الفعّال في حماية المعلومة، وذلك بالتزامه بالسلوك الصحيح وابتعاده عن الإهمال والأخطاء، وفي كل الأحوال يتعين عدم الاعتماد على التقنيات الأجنبية الخاصة بأمن المعلومات، وخصوصاً على الشبكات الرسمية التابعة للدولة، فالتجسس الذي يعد أحد ظواهر العلاقات الدولية تعدى النطاق العسكري والسياسي ليشمل الجانب الاقتصادي، فالحل الأمثل لأمن المعلومات هو تطوير الحلول الوطنية، أو على الأقل وضع الحلول الأجنبية تحت اختبارات مكثفة ودراسات معمّقة.

- ينبغي على العالم العربي أن يستشف مركزا متوازنا في تلك المنظومة الكونية

الراهنة، فالأمن الالكترونية أصبح يمثل مطلبا جذريا، في تحقيق التكامل المعلوماتي لمجتمع المعلومات العالمي، الذي أصبحت تمثل فيه الحياة الافتراضية جوهر التعاملات الالكترونية.

-بيد أن الحياة التخيلية في مفكرة بعض التيارات، تبشر بأفول العصر الورقي وبزوغ

مفهوم جديد من المجتمعات، وهو "المجتمع اللاورقي" وهو المجتمع الذي يفترض فيه أن تكون فيه الإدارة والتعاملات الحياتية بدون ورق أي إدارة حياة اليكترونية.

فقد أصبح العالم يعيش ثورة هائلة في مجال المعلومات والاتصالات، التي أتاحت للبشر قدراً هائلاً من المعرفة، لم يكن متاحاً من قبل، كما وفَّرت هذه التقنية الجديدة فرصاً للمؤسسات والشركات والمصارف والحكومات، لتقديم خدماتها بشكل غير مسبوق، وإذا كان ذلك هو الوجه المضيء لهذه التقنية، فإن الوجه الآخر تمثل في إمكانية العدوان والاختراق وممارسة الإتلاف والتخريب والتجسس، الأمر الذي فرض ضرورة توفير قدر من الحماية يتناسب مع مستوى أهمية المعلومات.

- كما ينبغي أن تنهض الجهات الوطنية المسؤولة عن صياغة القوانين، بأعباء إصدار وتنفيذ القوانين والضوابط، التي تضمن سلامة البيئة الإلكترونية من التجاوزات غير المشروعة، مع كف جرائم الفضاء المعلوماتي، والحد من تأثيرها على كلٍّ من المستثمر والزبائن، وتشمل هذه الأمور مسائلَ مثل: حقوق الملكية الفكرية، واحترام ضوابط وقواعد حقوق الطباعة، وضمان حماية المستخدم من التهديدات السائدة في الفضاء المعلوماتي، يضاف إلى ذلك ضرورة تكيُّف التقنين مع التقنينات الدولية السائدة، بحيث يتوفر مناخ آمن للتعامل مع الغير في الصفقات التجارية المبرمة مع الدول العربية، أو دول أخرى، مع ضمان التقدم صوب محو الأمية المعلوماتية، التي تقف عائقًا أمام الكثير من أنشطة التجارة الإلكترونية.

- و أملنا في الختام أن تسعى بلادنا الجزائر مع بقية الدول العربية إلى إنشاء منظمة عربية، تهتم بالتنسيق في مجال مكافحة الجرائم المعلوماتية عبر الانترنت؛ مع تشجيع قيام اتحادات عربية، تهتم بالتصدي لجرائم الانترنت وتفعيل دور المنظمات والإدارات والحكومات العربية، في مواجهة هذه الجرائم عن طريق نظام الأمن الوقائي، ويا حبذا لو تم إنشاء شرطة عربية تهتم بمكافحة الجرائم المعلوماتية، لأن الأمن المعلوماتي مسؤولية مشتركة تقع على عاتق الجميع، وفي حاجة الآن إلى

مبادرة دولية عاجلة فاعلة لتقوية وزيادة التعاون والتنسيق الدولي، واتخاذ الخطوات اللازمة لمنع ومواجهة التهديدات الأمنية التي تتعرض لها، واعتبار أن أي هجوم وتهديد على شبكات الإنترنت في أي دولة، بمثابة هجوم على شبكات الدول كلها، وتهديد لها، وبخاصة فيما يتعلق بقوانين وتشريعات مكافحة التهديدات الإلكترونية، فلا يمكن التصدي للتحديات الناشئة في هذا المجال إلاّ من خلال معالجة فعّالة عن طريق التعاون والتضافر بين الحكومات، وأوساط الصناعة والمنظمات الدولية والمجتمع المدني وغيرها من أصحاب المصلحة ذوي الصلة، ويشكل إذكاء الوعي الأساسي بالتحديات والفرص، وبناء القدرات المحلية، ووضع التشريعات التي يمكن تنفيذها، وتنفيذ مشاريع تُقدم حلولاً مؤمَّنة وذات موثوقية عالية، ووضع سياسات ملائمة بعض المجالات الرئيسية التي ينبغي أن يعمل الشركاء، فيها متضافرين من أجل تحقيق الهدف المُتفق عليه بوجه عام المتمثل في إقامة مجتمع معلومات شامل ومؤمَّن ومكفول للجميع.

الملاحق

فهـرس الملاحـق

English

Convention sur la cybercriminalité

Budapest, 23.XI.2001

Rapport explicatif

Préambule

Les Etats membres du Conseil de l'Europe et les autres Etats signataires,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres;

Reconnaissant l'intérêt d'intensifier la coopération avec les autres Etats parties à la Convention;

Convaincus de la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyber-espace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale;

Conscients des profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques;

Préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux;

Reconnaissant la nécessité d'une coopération entre les États et l'industrie privée dans la lutte contre la cybercriminalité et le besoin de protéger les intérêts légitimes liés au développement des technologies de l'information ;

Estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération

internationale en matière pénale accrue, rapide et efficace;

Convaincus que la présente Convention est nécessaire pour prévenir les actes portant atteinte à la confidentialité, l'intégrité et la disponibilité des systèmes informatiques, des réseaux et des données ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable ;

Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de droits de l'homme, qui réaffirment le droit de ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée;

Conscients également de la protection des données personnelles, telle que la confère, par exemple, la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Considérant la Convention des Nations Unies relative aux droits de l'enfant et la Convention de l'Organisation Internationale du Travail sur les pires formes de travail des enfants (1999) ;

Tenant compte des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, ainsi que d'autres traités similaires conclus entre les Etats membres du Conseil de l'Europe et d'autres Etats, et soulignant que la présente Convention a pour but de les compléter en vue de rendre plus efficaces les enquêtes et procédures pénales portant sur des infractions pénales en relation avec des systèmes et données informatiques, ainsi que de permettre la collecte des preuves électroniques d'une infraction pénale ;

Se félicitant des récentes initiatives destinées à améliorer la compréhension et la coopération internationales aux fins de la lutte contre la criminalité dans le cyber-espace, et notamment des actions menées par les Nations Unies, l'OCDE, l'Union européenne et le G8;

Rappelant la Recommandation N°(85) 10 concernant l'application pratique de la Convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications, la Recommandation N° R (88) 2 sur des mesures visant à combattre la piraterie dans le domaine du droit d'auteur et des droits voisins, la Recommandation

N° R(87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, la Recommandation N° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques et la Recommandation n° R (89) 9 sur la criminalité en relation avec l'ordinateur, qui indique aux législateurs nationaux des principes directeurs pour définir certaines infractions informatiques, ainsi que la Recommandation n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information;

Eu égard à la Résolution n° 1, adoptée par les Ministres européens de la Justice à leur 21e Conférence (Prague, juin 1997) qui recommande au Comité des Ministres de soutenir les activités menées par le Comité européen pour les problèmes criminels (CDPC) concernant la cybercriminalité afin de rapprocher les législations pénales nationales et de permettre l'utilisation de moyens d'investigation efficaces en matière d'infractions informatiques, ainsi qu'à la Résolution N°3, adoptée lors de la 23e Conférence des Ministres européens de la Justice (Londres, juin 2000), qui encourage les parties aux négociations à poursuivre leurs efforts afin de trouver des solutions adaptées permettant au plus grand nombre d'Etats d'être parties à la Convention et reconnaît la nécessité de disposer d'un mécanisme rapide et efficace de coopération internationale qui tienne dûment compte des exigences spécifiques de la lutte contre la cybercriminalité;

Prenant également en compte le Plan d'action adopté par les Chefs d'Etat et de gouvernement du Conseil de l'Europe à l'occasion de leur Deuxième Sommet (Strasbourg, 10 - 11 octobre 1997) afin de chercher des réponses communes au développement des nouvelles technologies de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe;

Sont convenus de ce qui suit:

Chapitre I - Terminologie

Article 1 – Définitions

Aux fins de la présente Convention, l'expression:

a. «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;

b. «données informatiques» désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;

c. «fournisseur de service» désigne :

i. toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ;

ii. toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs ;

d. «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent.

Chapitre II - Mesures à prendre au niveau national

Section 1 - Droit pénal matériel

Titre 1 - Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Article 2 - Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 - Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 4 - Atteinte à l'intégrité des données

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Article 5 - Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération et la suppression de données informatiques.

Article 6 – Abus de dispositifs

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:

a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition

i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 – 5 ci-dessus ;

ii. d'un mot de passe, d'un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique

dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 – 5 ; et

b. la possession d'un élément visé aux paragraphes (a) (1) ou (2) ci-dessus dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 – 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2. Le présent article ne saurait être interpréter comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'a pas pour but de commettre une infraction établie conformément à l'Article 2 à 5 de la présente Convention, comme en cas d'essais autorisés ou de protection d'un système informatique.

3. Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1 (a)(2).

Titre 2 - Infractions informatiques

Article 7 - Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger en droit interne une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8 - Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui par:

a. l'introduction, l'altération, l'effacement ou la suppression de données informatiques,

b. toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Titre 3 - Infractions se rapportant au contenu

Article 9 – Infractions se rapportant à la pornographie enfantine

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:

a. la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique ;

b. l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système

informatique;

c. la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique;

d. le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique;

e. la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

2. Aux fins du paragraphe 1 ci-dessus, la «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle :

a. un mineur se livrant à un comportement sexuellement explicite;

b. une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;

c. des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

3. Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.

4. Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1 (d) et 1 (e) et 2 (b) et 2 (c).

Titre 4 - Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Article 10 - Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle définie par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de la Convention universelle sur le droit d'auteur révisée à Paris le 24 juillet 1971, de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces Conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système

informatique.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de la Convention internationale sur la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion faite à Rome (Convention de Rome), de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations, exécutions et phonogrammes, à l'exception de tout droit moral conféré par ces Conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

3. Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.

Titre 5 – Autres formes de responsabilité et de sanctions

Article 11 - Tentative et complicité

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des Articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des Articles 3 à 5, 7, 8, 9 (1)a et 9(1)c de la présente Convention.

3. Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent Article.

Article 12 – Responsabilité des personnes morales

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour faire en sorte que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, sur les bases suivantes:

a. un pouvoir de représentation de la personne morale;

b. une autorité pour prendre des décisions au nom de la personne morale;

c. une autorité pour exercer un contrôle au sein de la personne morale.

2. Outre les cas déjà prévus au paragraphe 1, chaque Partie adopte les mesures nécessaires pour s'assurer qu'une personne morale puisse être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions visées au paragraphe 1 pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

3. Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.

4. Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

Article 13 – Sanctions et mesures

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour faire en sorte que les infractions pénales établies en application des articles 2 - 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

2. Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.

Section 2 – Droit procédural

Titre 1 – Dispositions communes

Article 14 – Portée d'application des mesures du droit de procédure

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2. Sauf disposition contraire figurant à l'Article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 :

a. aux infractions pénales établies conformément aux articles 2-11 de la présente Convention ;

b. à toutes autres infractions pénales commises au moyen d'un système informatique ; et

c. à la collecte des preuves électroniques de toute infraction pénale.

3. a. Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'Article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'Article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.

b. Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services qui

i. est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et

ii. n'emploi pas les réseaux publics de télécommunications et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé,

cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

Article 15 – Conditions et sauvegardes

1. Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966) ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

2. Lorsque cela est approprié eu égard à la nature du pouvoir ou de la procédure concerné, ces

conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3. Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette Section sur les droits, responsabilités et intérêts légitimes des tiers.

Titre 2 – Conservation rapide de données informatiques stockées

Article 16 – Conservation rapide de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et protéger l'intégrité desdits données pendant une durée aussi longue que nécessaire, jusqu'à maximum 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 17 – Conservation et divulgation rapides de données relatives au trafic

1. Afin d'assurer la conservation des données relatives au trafic en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour:

a. veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de service aient participé à la transmission de cette communication; et

b. assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne

désignée par cette autorité, d'une quantité de données relatives au trafic suffisante pour permettre l'identification des fournisseurs de service et de la voie par laquelle la communication a été transmise.

2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Titre 3 – Injonction de produire

Article 18 – Injonction de produire

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

a. à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en la possession où sous le contrôle de cette personne, et stockées dans un système informatique ou un support de stockage informatique; et

b. à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services;

2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

3. Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service ;

c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service.

Titre 4 – Perquisition et saisie de données informatiques stockées

Article 19 – Perquisition et saisie de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

a. à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et

b. à un support du stockage informatique permettant de stocker des données informatiques

sur son territoire.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1 (a), et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou un d'un accès d'une façon similaire à l'autre système.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes :

a. saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci ou un support de stockage informatique ;

b. réaliser et conserver une copie de ces données informatiques ;

c. préserver l'intégrité des données informatiques stockées pertinentes ; et

d. rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.

5. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

Titre 5 – Collecte en temps réel de données informatiques

Article 20 – Collecte en temps réel des données relatives au trafic

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à :

a. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire ;

b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i. collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii. prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1(a), elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 21 – Interception de données relatives au contenu

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter

ses autorités compétentes relativement à un éventail d'infractions graves à définir en droit interne, à :

a. collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire ; et

b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à :

i. collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire , ou

ii. prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1(a), elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et15.

Section 3 – Compétence

Article 22 – Compétence

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux Articles 2 – 11 de la présente Convention, lorsque l'infraction est commise:

a. sur son territoire ;

b. à bord d'un navire battant pavillon de cette Partie ;

c. à bord d'un aéronef immatriculé dans cette Partie ;

d. par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.

2. Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou conditions spécifiques, les règles de compétence définies aux paragraphes 1b – 1d du présent article ou dans une partie quelconque de ces paragraphes.

3. Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1 de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.

4. La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

5. Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de décider quelle est celle qui est la mieux à même d'exercer les poursuites.

Chapitre III – Coopération internationale

Section 1 – Principes généraux

Titre 1 – Principes généraux relatifs à la coopération internationale

Article 23 – Principes généraux relatifs à la coopération internationale

Les Parties coopèrent conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible les unes avec les autres, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et données informatiques ou pour recueillir les preuves sous forme électronique d'une infraction pénale.

Titre 2 – Principes relatifs à l'extradition

Article 24 – Extradition

1. a. Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.

b. Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, c'est la peine minimum prévue par ce traité ou cet arrangement qui s'applique.

2. Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.

3. Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article.

4. Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition.

5. L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.

6. Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétente pour cette infraction, la Partie requise soumet l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte en temps utile de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable conformément à la législation de cette Partie.

7. a. Chaque Partie communique au Secrétaire général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.

b. Le Secrétaire général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre.

Titre 3 – Principes généraux relatifs à l'entraide

Article 25 – Principes généraux relatifs à l'entraide

1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

2. Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.

3. Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris le cryptage si nécessaire), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

4. Sauf disposition contraire expressément prévue dans les articles du présent Chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.

5. Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, en relation avec laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

Article 26 – Information spontanée

1. Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente

Convention, ou lorsque ces informations pourraient aboutir à une demande formulée par cette Partie au titre du présent chapitre.

2. Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou ne soient utilisées que sous certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

Titre 4 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

1. En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.

2. a. Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution;

b. les autorités centrales communiquent directement les unes avec les autres;

c. chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe;

d. le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.

3. Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise.

4. Outre les conditions ou motifs de refus prévus à l'Article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise :

a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b. si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

5. La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités.

6. Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement ou sous réserve des conditions qu'elle juge nécessaires.

7. La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative.

8. La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre restent confidentiels, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.

9. a. En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans de tels cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante

b. Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol).

c. Lorsqu'une demande a été formulée en application de l'alinéa (a) du présent article et que l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité nationale compétente et en informe directement la Partie requérante.

d. Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise.

e. Chaque Partie peut informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou

d'adhésion, que, pour des raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.

Article 28 – Confidentialité et restriction d'utilisation

1. En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article.

2. La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande à la condition :

a. que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition; ou

b. qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande.

3. Si la Partie requérante ne peut satisfaire à l'une des conditions énoncées au paragraphe 2, elle en informe rapidement la Partie requise, qui détermine alors si l'information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci.

4. Toute Partie qui fournit des informations ou du matériel soumis à l'une des conditions énoncées au paragraphe 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel.

Section 2– Dispositions spécifiques

Titre 1 – Entraide en matière de mesures provisoires

Article 29 – Conservation rapide de données informatiques stockées

1. Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.

2. Une demande de conservation faite en application du paragraphe 1 doit préciser :

a. l'autorité qui demande la conservation ;

b. l'infraction faisant l'objet de l'enquête et un bref exposé des faits qui s'y rattachent ;

c. les données informatiques stockées à conserver et la nature de leur lien avec l'infraction ;

d. toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique ;

e. la nécessité de la mesure de conservation ; et

f. le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

3. Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.

4. Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données peut, pour des infractions autres que celles établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser qu'au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.

5. En outre, une demande de conservation peut être refusée uniquement :

a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

a. si la Partie requise estime que le fait d'accéder de la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.

6. Lorsque la Partie requise estime que la conservation simple ne suffira pas pour garantir la disponibilité future des données, compromettra la confidentialité de l'enquête de la Partie requérante ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande.

7. Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins 60 jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.

Article 30 – Divulgation rapide de données conservées

1. Lorsqu'en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de service et la voie par laquelle la communication a été transmise.

2. La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement :

a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b. si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

***Titre 2* – Entraide concernant les pouvoirs d'investigation**

Article 31 – Entraide concernant l'accès aux données stockées

1. Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, et de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.

2. La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations évoqués à l'article 23 et en se conformant aux dispositions pertinentes du présent chapitre.

3. La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:

a. il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification ; ou

b. les instruments, arrangements et législations évoqués au paragraphe 2 prévoient une coopération rapide.

Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie, :

a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou

b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic

1. Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et procédures prévues en droit interne.

2. Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

Article 34 – Entraide en matière d'interception de données relatives au contenu

Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

Titre 3 – Réseau 24/7

Article 35 – Réseau 24/7

1. Chaque Partie désigne un point de contact joignable 24 heures sur 24, sept jours sur sept, afin d'assurer la fourniture d'une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et données informatiques ou pour recueillir les preuves

sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes :

a. apport de conseils techniques;

b. conservation des données conformément aux articles 29 et 30 ; et

c. recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

2. a. Le point de contact d'une Partie pourra correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.

b. Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités selon une procédure accélérée.

3. Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

Chapitre IV – Clauses finales

Article 36 – Signature et entrée en vigueur

1. La présente Convention est ouverte à la signature des Etats membres du Conseil de l'Europe et des Etats non membres qui ont participé à son élaboration.

2. La présente Convention est soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation sont déposés auprès du Secrétaire Général du Conseil de l'Europe.

3. La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats, incluant au moins trois Etats membres du Conseil de l'Europe, auront exprimé leur consentement à être liés par la Convention, conformément aux dispositions des paragraphes 1 et 2.

4. Pour tout Etat signataire qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de l'expression de son consentement à être lié par la Convention conformément aux dispositions des paragraphes 1 et 2.

Article 37 – Adhésion à la Convention

1. Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe peut, après avoir consulté les Etats contractants à la Convention et en avoir obtenu l'assentiment unanime, inviter tout Etat non membre du Conseil et n'ayant pas participé à son élaboration à adhérer à la présente Convention. La décision est prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des Etats contractants ayant le droit de siéger au Comité des Ministres.

2. Pour tout Etat adhérent à la Convention conformément au paragraphe 1 ci-dessus, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.

Article 38 – Application territoriale

1. Tout Etat peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires sur lesquels s'appliquera la présente Convention.

2. Tout Etat peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.

3. Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

Article 39 – Effets de la Convention

1. L'objet de la présente Convention est de compléter les traités ou accords multilatéraux ou bilatéraux applicables existant entre les Parties, y compris les dispositions:

- de la Convention européenne d'extradition ouverte à la signature le 13 décembre 1957 à Paris [STE n°24];

- de la Convention européenne d'entraide judiciaire en matière pénale ouverte à la signature le 20 avril 1959 à Strasbourg [STE n°30];

- du Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale ouvert à la signature le 17 mars 1978 à Strasbourg [STE n°99].

2. Si deux ou plusieurs Parties ont déjà conclu un accord ou un traité relatif aux matières traitées par la présente Convention ou si elles ont autrement établi leurs relations sur ces sujets, ou si elles le feront à l'avenir, elles ont aussi la faculté d'appliquer ledit accord ou traité ou d'établir leurs relations en conséquence, au lieu de la présente Convention. Toutefois, lorsque les Parties établiront leurs relations concernant les matières faisant l'objet de la présente Convention d'une manière différente de celle y prévue, elles le feront d'une manière qui ne soit pas incompatible avec les objectifs et principes de la Convention.

3. Rien dans la présente Convention n'affecte d'autres droits, restrictions, obligations et responsabilités d'une Partie.

Article 40 – Déclarations

Par déclaration écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la faculté d'exiger, le cas échéant, un ou plusieurs éléments supplémentaires tels que prévus aux Articles 2, 3, 6, paragraphe 1(b), 7, 9, paragraphe 3 et 27, paragraphe 9(e).

Article 41 – Clause fédérale

1. Un État fédéral peut se réserver le droit d'honorer les obligations aux termes du Chapitre II de la présente Convention dans la mesure où celles-ci sont compatibles avec les principes fondamentaux qui gouvernent les relations entre son gouvernement central et les États constituants ou autres entités territoriales analogues, à condition qu'il soit en mesure de coopérer sur la base du Chapitre III.

2. Lorsqu'il fait une réserve prévue au paragraphe 1, un Etat fédéral ne saurait faire usage des termes d'une telle réserve pour exclure ou diminuer de manière substantielle ses obligations en vertu du chapitre II. En tout état de cause, il se dote de moyens étendus et effectifs permettant la mise en oeuvre des mesures prévues par ledit chapitre.

3. En ce qui concerne les dispositions de cette Convention dont l'application relève de la compétence législative de chacun des Etats constituants ou autres entités territoriales analogues, qui ne sont pas, en vertu du système constitutionnel de la fédération, tenus de prendre des mesures législatives, le gouvernement fédéral porte, avec son avis favorable, lesdites dispositions à la connaissance des autorités compétentes des Etats constituants, en les encourageant à adopter les mesures appropriées pour les mettre en oeuvre.

Article 42 – Réserves

Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou les réserves prévues aux Article 4, paragraphe 2, Article 6, paragraphe 3, Article 9, paragraphe 4, Article 10, paragraphe 3, Article 11, paragraphe 3, Article 14, paragraphe 3, Article 22, paragraphe 2, Article 29, paragraphe 4, et à l'article 41, paragraphe 1. Aucune autre réserve ne peut être faite.

Article 43 – Statut et retrait des réserves

1. Une Partie qui a fait une réserve conformément à l'Article 42 peut la retirer en totalité ou en partie par notification adressée au Secrétaire Général. Ce retrait prend effet à la date de réception de ladite notification par le Secrétaire Général. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.

2. Une Partie qui a fait une réserve comme celles mentionnées à l'Article 42 retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent.

3. Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves comme celles mentionnées à l'Article 42 des informations, sur les perspectives de leur retrait.

Article 44 – Amendements

1. Des amendements à la présente Convention peuvent être proposés par chaque Partie, et sont communiqués par le Secrétaire Général du Conseil de l'Europe aux États membres du Conseil de l'Europe, aux États non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout État y ayant adhéré ou ayant été invité à y adhérer conformément aux dispositions de l'article 37.

2. Tout amendement proposé par une Partie est communiqué au Comité européen pour les problèmes criminels (CDPC), qui soumet au Comité des Ministres son avis sur ledit amendement.

3. Le Comité des Ministres examine l'amendement proposé et l'avis soumis par le Comité européen pour les problèmes criminels (CDPC) et, après consultation avec les Etats non membres parties à la présente Convention, peut adopter l'amendement.

4. Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 du présent article est communiqué aux Parties pour acceptation.

5. Tout amendement adopté conformément au paragraphe 3 du présent article entre en vigueur le trentième jour après que toutes les Parties ont informé le Secrétaire Général de leur acceptation.

Article 45 – Règlement des différends

1. Le Comité européen pour les problèmes criminels du Conseil de l'Europe est tenu informé de l'interprétation et de l'application de la présente Convention.

2. En cas de différend entre les Parties sur l'interprétation ou l'application de la présente Convention, les Parties s'efforceront de parvenir à un règlement du différend par la négociation ou par tout autre moyen pacifique de leur choix, y compris la soumission du différend au Comité européen pour les problèmes criminels, à un tribunal arbitral qui prendra des décisions qui lieront les Parties au différend, ou à la Cour internationale de justice, selon un accord commun entre les Parties concernées.

Article 46 – Concertation des Parties

1. Les Parties se concertent périodiquement, au besoin, afin de faciliter :

a. l'usage et la mise en œuvre effectifs de la présente Convention, y compris l'identification de tout problème en la matière, ainsi que les effets de toute déclaration ou réserve faite conformément à la présente Convention;

b. l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique ;

c. l'examen de l'éventualité de compléter ou d'amender la Convention.

2. Le Comité européen pour les problèmes criminels (CDPC) est tenu périodiquement au courant du résultat des concertations mentionnées au paragraphe 1.

3. Le Comité européen pour les problèmes criminels (CDPC) facilite, au besoin, les concertations mentionnées au paragraphe 1 et adopte les mesures nécessaires pour aider les Parties dans leurs efforts visant à compléter ou amender la Convention. Au plus tard à l'issue d'un délai de trois ans à compter de l'entrée en vigueur de la présente Convention, le Comité européen pour les problèmes criminels (CDPC) procèdera, en coopération avec les Parties, à un réexamen de l'ensemble des dispositions de la Convention et proposera, le cas échéant, les aménagement appropriés.

4. Sauf lorsque le Conseil de l'Europe les prend en charge, les frais occasionnés par l'application

des dispositions du paragraphe 1 sont supportés par les Parties de la manière qu'elles déterminent.

5. Les Parties sont assistées par le Secrétariat du Conseil de l'Europe dans l'exercice de leurs fonctions découlant du présent article.

Article 47 – Dénonciation

1 Toute Partie peut, à tout moment, dénoncer la présente Convention par notification au Secrétaire Général du Conseil de l'Europe.

2 La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

Article 48 – Notification

Le Secrétaire Général du Conseil de l'Europe notifie aux États membres du Conseil de l'Europe, aux États non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout État y ayant adhéré ou ayant été invité à y adhérer :

a. toute signature;

b. le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion;

c. toute date d'entrée en vigueur de la présente Convention conformément à ses articles 36 et 37 ;

d. toute déclaration faite en application des Articles 40 et 41 ou toute réserve faite en application de l'article 42 ;

e. tout autre acte, notification ou communication ayant trait à la présente Convention.

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé la présente Convention.

Fait à Budapest, le 23 novembre 2001, en français et en anglais, les deux textes faisant également foi, et en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe, aux Etats non membres qui ont participé à l'élaboration de la Convention et à tout Etat invité à y adhérer.

الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية

ديبـاجة

إن الدول العربية الموقعة،

التزاما منها بالمبادئ الأخلاقية والدينية السامية ، ولاسيما أحكام الشريعة الإسلامية السمحة ، وبأهداف ومبادئ ميثاق جامعة الدول العربية وميثاق الأمم المتحدة والاتفاقيات والمعاهدات العربية والدولية في مجال التعاون القضائي والأمني لمنع ومكافحة الجريمة والتي تكون الدول المتعاقدة طرفا فيها، ولا سيما منها اتفاقية الرياض للتعاون القضائي، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية،

وإدراكا منها لأهمية التصدي للجريمة المنظمة عبر الحدود الوطنية ، لما تمثله هذه الجريمة من تهديد لأمن الأمة العربية واستقرارها وعرقلة للتنمية الاقتصادية والاجتماعية للبلدان العربية،

وحرصا منها على تعزيز التعاون العربي في مجال منع ومكافحة الجريمة المنظمة عبر الحدود الوطنية في المجالين القضائي والأمني وتجريم الأفعال المكونة لهذه الجريمة، واتخاذ تدابير وإجراءات منعها ومكافحتها وملاحقة ومعاقبة مرتكبيها وشركائهم وفق أحكام الشريعة الإسلامية السمحة أو القوانين الوطنية مع مراعاة النظام العام لكل دولة وتسليمهم إلى الدول الطالبة.

وأخذا في الاعتبار عدم تعارض أحكام الاتفاقية مع دساتير الدول الأطراف أو أنظمتها الأساسية،

قد اتفقت على مايلي :

الفصل الأول: أحكام عامة

المادة (1)
الهدف من الاتفاقية

تهدف هذه الاتفاقية إلى تعزيز التعاون العربي لمنع ومكافحة الجريمة المنظمة عبر الحدود الوطنية.

المادة (2)
المصطلحات

يكون للمصطلحات التالية أينما وردت في هذه الاتفاقية المعاني المبينة إزاءها :

1 - الدولة الطرف :

كل دولة عضو في جامعة الدول العربية صادقت على هذه الاتفاقية أو انضمت إليها وأودعت وثائق تصديقها أو انضمامها لدى الأمانة العامة لجامعة الدول العربية.

2- الجريمة المنظمة عبر الحدود الوطنية:

هي كل جريمة ذات طابع عابر للحدود الوطنية وتضطلع بتنفيذها أو الاشتراك فيها أو التخطيط لها أو تمويلها أو الشروع فيها جماعة إجرامية منظمة على النحو الموصوف في الفقرة (3) من هذه المادة.

3- الجماعة الإجرامية المنظمة:

هي كل جماعة ذات بنية محددة مكونة لفترة من الزمن من ثلاثة أشخاص أو أكثر اتفق أفرادها على ارتكاب احدى الجرائم المشمولة بهذه الاتفاقية من أجل الحصول على منفعة مادية مباشرة أو غير مباشرة.

4- جماعة ذات بنية محددة :

ويقصد بها جماعة غير مشكلة عشوائياً لغرض الإرتكاب الفوري لجرم ما، ولا يلزم أن يكون لأعضائها أدوار محددة رسمياً، أو أن تستمر عضويتهم فيها أو أن تكون لها بنية متطورة.

5 - متحصلات الجريمة :

أي ممتلكات أو أشياء أو أموال تم التحصل عليها بطريق مباشر أو غير مباشر من ارتكاب جريمة مشمولة بهذه الاتفاقية.

6 – التحفظ أو التجميد :

هو الحجز المؤقت على الممتلكات أو الأشياء أو الأموال ذات الصلة بالجريمة بمقتضى أمر صادر عن سلطة قضائية أو سلطة مختصة أخرى، وفقاً لما تنص عليه القوانين الداخلية لكل دولة.

7 – المصادرة :

تجريد الشخص من الممتلكات أو الأشياء أو الأموال ذات الصلة بالجريمة بمقتضى حكم غير قابل لأي طريق من طرق الطعن صادر عن سلطة قضائية مختصة، وفقاً لما تنص عليه القوانين الداخلية لكل دولة.

8- الممتلكات:

ويقصد بها الموجودات أياً كان نوعها، سواء أكانت مادية أم غير مادية، منقولة أم غير منقولة، ملموسة أم غير ملموسة، والمستندات أو الصكوك القانونية التي تثبت ملكية تلك الموجودات أو وجود مصلحة فيها.

9- الأموال:

ويقصد بها العملات الوطنية العربية والعملات الأجنبية والأوراق المالية والأوراق التجارية وكل ذي قيمة من عقار أو منقول مادي أو معنوي، وجميع الحقوق المتعلقة بها، والصكوك والمحررات المثبتة لهذه الأموال.

10- الجرم الأصلي:

أي جرم تأتت منه عائدات يمكن أن تصبح موضوع جريمة.

المادة (3)

نطاق تطبيق الاتفاقية

1- تطبق هذه الاتفاقية على ما يأتي:

أ- الأفعال المجرّمة بمقتضى هذه الاتفاقية.

ب- أية جريمة أخرى منظمة عبر الحدود الوطنية معاقب عليها بعقوبة سالبة للحرية لمدة لا تقل عن ثلاث سنوات، وفقاً للقوانين الوطنية لكل دولة.

2- لأغراض الفقرة 1 من هذه المادة، تكون الجريمة عابرة للحدود الوطنية إذا أرتكبت:

أ – في أكثر من دولة واحدة.

ب- في دولة واحدة، وكان الإعداد أو التخطيط لها أو توجيهها أو تمويلها أو الإشراف عليها في دولة أو دول أخرى.

ج- في دولة واحدة، من جماعة إجرامية منظمة تمارس أنشطة إجرامية في أكثر من دولة واحدة.

د- في دولة واحدة، وترتبت عليها آثار شديدة في دولة أو دول أخرى.

المادة (4)

صون السيـادة

1- تتعهد الدول الأطراف بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة والسلامة الإقليمية للدول ومبدأ عدم التدخل في الشؤون الداخلية للدول الأخرى.

2- ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة طرف أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصراً بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي.

المادة (5)

مسؤولية الهيئات الاعتبارية

1- تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى، بما يتفق مع مبادئها القانونية، لإقرار مسؤولية الهيئات الاعتبارية عن المشاركة في الجرائم الخطيرة، التي تكون ضالعة فيها جماعة إجرامية منظمة، والأفعال المجرمة بمقتضى هذه الاتفاقية .

2- عملاً بالمبادئ القانونية للدولة الطرف، يجوز أن تكون مسؤولية الهيئات الاعتبارية جنائية أو مدنية أو إدارية.

3- لا تخل المسؤولية المنصوص عليها في الفقرة (1) من هذه المادة بالمسؤولية الجنائية للأشخاص الطبيعيين الذين ارتكبوا الجرائم.

4- تكفل كل دولة طرف، على وجه الخصوص، إخضاع الأشخاص الاعتباريين الذين تلقى عليهم المسؤولية وفقاً لهذه المادة، لعقوبات جزائية أو غير جزائية فعالة ومتناسبة ورادعة بما في ذلك الجزاءات النقدية.

الفصل الثاني: الأحكام الجزائية

المادة (6)

غسل الأموال

1- تتعهد كل دولة طرف أن تتخذ ما يلزم في إطار قانونها الداخلي، لتجريم أي من الأفعال التالية إذا ارتكبت قصداً أو عمداً بالنسبة للأموال المتحصلة من أية جريمة أصلية من الجرائم المشمولة بهذه الاتفاقية :

أ – تحويل الأموال أو نقلها مع العلم بكونها متحصلات إجرامية بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات.

ب – إخفاء أو تمويه الطبيعة الحقيقية للأموال أو مصدرها أو مكانها أو كيفية التصرف فيها أو ملكيتها أو الحقوق المتعلقة بها مع العلم بكونها متحصلات إجرامية.

ج – اكتساب الأموال أو حيازتها أو استعمالها مع العلم وقت تلقيها بكونها متحصلات إجرامية.

2- يشمل مفهوم الجريمة الأصلية الجرائم التي تشملها هذه الاتفاقية والتي تحصلت عنها الأموال، وكافة الجرائم التي ارتكبت داخل أو خارج إقليم الدولة الطرف المعنية. ولكن يشترط في حال وقوع تلك الجريمة خارج إقليم الدولة الطرف أن تمثل فعلا إجراميا بمقتضى قانون الدولة التي ارتكبت فيها وقانون الدولة الطرف المعنية بتطبيق أحكام هذه المادة.

3- تعمل كل دولة طرف في هذه الاتفاقية على وضع تدابير للإشراف والرقابة بغرض منع ومكافحة غسل الأموال.

المادة (7)

الفساد الإداري

1- تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير تشريعية وتدابير أخرى لتجريم ارتكاب أو المشاركة في ارتكاب الأفعال التالية في إطار قانونها الداخلي في حال ارتكاب هذه الأفعال عمدا من جماعة إجرامية منظمة:

أ - طلب موظف عمومي أو من في حكمه أو قبوله بشكل مباشر أو غير مباشر سواء لصالح الموظف نفسه أو لصالح غيره مزية أو منفعة غير مستحقة أو وعداً بها ، لكي يقوم بعمل أو يمتنع عن القيام بعمل من الأعمال الداخلة ضمن نطاق وظيفته الرسمية.

ب- وعد موظف عمومي أو من في حكمه بمزية أو بمنفعة غير مستحقة أو عرضها عليه أو منحه إياها بشكل مباشر أو غير مباشر سواء لصالح الموظف نفسه أو لصالح غيره لكي يقوم بعمل أو يمتنع عن القيام بعمل من الأعمال الداخلة ضمن نطاق وظيفته الرسمية.

ج - تسرى أحكام الفقرتين (أ) و (ب) من هذه المادة على كل موظف عمومي أجنبي أو موظف مدني دولي ارتكب فعلا من الأفعال المجرمة في هاتين الفقرتين.

د- كل موظف عمومي أو من في حكمه حصل لنفسه أو لغيره على مزية أو منفعة غير مشروعة بسبب استغلال السلطة أو الصفة أو نتيجة لسلوك مجرّم قانوناً.

2 - تتعهد كل دولة طرف أن تتخذ بما يتناسب مع نظامها القانوني التدابير التشريعية والإدارية بهدف تعزيز نزاهة الموظفين العموميين ومنع فسادهم وكشفهم ومعاقبتهم.

3- تتعهد كل دولة طرف أن تنظر في تجريم الأشكال الأخرى للفساد الإداري الواقع على الوظيفة العامة.

المادة (8)

جرائم القطاع الخاص

تتخذ كل دولة طرف وفقاً لنظامها الأساسي أو لمبادئها الدستورية وفي إطار قانونها الداخلي، تدابير لمنع ضلوع القطاع الخاص في الجريمة المنظمة، وتعزيز معايير المحاسبة ومراجعة الحسابات في القطاع الخاص وتفرض عقوبات مدنية أو إدارية أو جنائية تكون فعالة ومناسبة على عدم الامتثال لهذه التدابير.

المادة (9)

الاحتيال على المؤسسات المالية والمصرفية

تتعهد كل دولة بأن تتخذ ما يلزم من تدابير في إطار قانونها الداخلي، لتجريم الاحتيال على المؤسسات المالية و المصرفية، عندما تقع من جماعة إجرامية منظمة أو أحد أعضائها.

المادة (10)

تزوير وتزييف العملة وترويجها

تتعهد كل دولة طرف بالاتفاقية أن تتخذ مايلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في حال ارتكابها عمداً من جماعة إجرامية منظمة:

1- تزوير أو تزييف عملة ورقية أو معدنية متداولة قانوناً أو مأذون بإصدارها قانوناً في دولة طرف بالاتفاقية.

2- حيازة وإخراج أو إدخال أي من العملات المزورة أو المزيفة لحدود دولة طرف بالاتفاقية.

3- ترويج العملات المزورة أو المزيفة أو التعامل بها في أي دولة طرف بالاتفاقية.

المادة (11)

الاتجار بالأشخاص وبخاصة النساء والأطفال

تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير في إطار قانونها الداخلي، لتجريم ارتكاب أو المشاركة في ارتكاب الأفعال التالية التي تقوم بها جماعة إجرامية منظمة :

1- أي تهديد بالقوة أو استعمالها أو غير ذلك من أشكال القسر أو الإختطاف أو الاحتيال أو الخداع أو إساءة إستعمال السلطة أو استغلال حالة الضعف وذلك من أجل استخدام أو نقل أو إيواء أو إستقبال أشخاص لغرض إستغلالهم بشكل غير مشروع في ممارسة الدعارة

(البغاء) أو سائر أشكال الإستغلال الجنسي أو السخرة أو الخدمة قسراً أو الإسترقاق أو الممارسات الشبيهة بالرق أو الاستعباد، ولا يعتد برضاء الشخص ضحية الاتجار في كافة صور الاستغلال متى استخدمت فيها الوسائل المبينة في هذه الفقرة.

2- يعتبر استخدام طفل أو نقله أو إيوائه أو إستقباله لغرض الاستغلال إتجاراً بالأشخاص حتى إذا لم ينطو على استعمال أي من الوسائل المبينة في الفقرة (1) من هذه المادة . وفي جميع الأحوال لا يعتد برضائه .

المادة (12)

انتزاع الأعضاء البشرية والاتجار فيها

تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير تشريعية وتدابير أخرى لتجريم ارتكاب أو المشاركة في ارتكاب أفعال انتزاع الأعضاء الجسدية أو الأنسجة العضوية، أو الاتجار فيها، أو نقلها بالإكراه أو التحايل أو التغرير، عندما تقوم بها جماعة اجرامية منظمة أو أحد أعضائها، ولا يعتد برضاء الشخص ضحية هذه الأفعال متى استخدمت فيها الوسائل المبينة في هذه المادة.

المادة (13)

تهريب المهاجرين

تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير في إطار قانونها الداخلي، لتجريم ارتكاب الأفعال التالية التي تقوم بها جماعة إجرامية منظمة:

1- تهريب المهاجرين عن طريق القيام بإدخال أحد الأشخاص على نحو غير مشروع إلى دولة طرف لا يعتبر ذلك الشخص من مواطنيها أو من المقيمين فيها، وذلك من أجل الحصول، بصورة مباشرة أو غير مباشرة، على منفعة مالية.

2- تسهيل تهريب المهاجرين بارتكاب أحد الأفعال التالية:

أ- إعداد وثيقة سفر أو تزويرها أو انتحال هوية أو تدبير الحصول على وثيقة من هذا القبيل أو توفيرها أو حيازتها.

ب- تمكين شخص، ليس مواطناً أو مقيماً دائماً في الدولة المعنية من البقاء فيها دون تقيد بالشروط اللازمة للبقاء المشروع في تلك الدولة، وذلك باستخدام إحدى الوسائل المذكورة في هذه المادة أو أية وسيلة أخرى غير مشروعة.

3- يتعين على كل دولة طرف رهناً بأحكام نظامها القانوني أن تعتمد ما يلزم من تدابير تشريعية وتدابير أخرى لاعتبار الظروف التالية أسباباً لتشديد عقوبة الجرائم الواردة في هذه المادة:

أ- تهديد حياة المهاجرين المعنيين أو تعريض سلامتهم للخطر.

ب- معاملة أولئك المهاجرين معاملة لا إنسانية أو مهينة.

4- ليس في هذه المادة ما يمنع أية دولة طرف من اتخاذ تدابير بحق أي شخص يعد سلوكه جرماً بمقتضى قانونها الداخلي.

المادة (14)

القرصنة البحرية

تتعهد كل دولة طرف بأن تتخذ ما يلزم من تدابير في إطار قانونها الداخلي، لتجريم القرصنة البحرية، عندما تقع من قبل جماعة إجرامية منظمة.

المادة (15)

الاستيلاء على الآثار والممتلكات الثقافية والفكرية والإتجار غير المشروع بها

1- تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير تشريعية وتدابير أخرى لتجريم ارتكاب أو المشاركة في ارتكاب الأفعال التالية عندما تقع عمدا من قبل جماعة إجرامية منظمة أو أحد أفرادها:

أ– تهريب آثار إلى الخارج.

ب- الاتجار غير المشروع في الآثار.

ج– سرقة آثار أو جزء منها أو إخفاؤها .

د– هدم أو إتلاف أو تشويه أو تغيير معالم أو فصل جزء من أثر.

هـ– القيام بعمل من أعمال التنقيب الأثرى دون ترخيص بذلك من السلطة المختصة .

و- حيازة غير مشروعة لأي آثار متى كان الحائز يعلم أو يفترض فيه أن يعلم بطبيعة الآثار موضوع الحيازة ".

ز- تقليد الآثار بقصد بيعها والاستفادة منها بوسائل الغش أو التضليل.

ح- سرقة الأشياء ذات الصبغة الثقافية والاتجار غير المشروع بها.

ط- سرقة اللوحات الفنية والاتجار غير المشروع بها.

ي- التعدي على حقوق الملكية الفكرية والاتجار غير المشروع بها.

2- تلتزم الدول الأطراف بإعادة الآثار التي خرجت بصورة غير مشروعة إلى مصدرها.

المادة (16)

الاعتداء على البيئة ونقل النفايات الخطرة والمواد الضارة

تتعهد كل دولة طرف أن تجعل ارتكاب أي جريمة من الجرائم الآتية خاضعاً لجزاءات أو تدابير احترازية أو الأمرين معاً، على أن تراعى فيها خطورة الجريمة وعدم اغفال العقوبات التبعية أو التكميلية:

1- الأفعال التي تلحق ضررا بأحد عناصر البيئة الأرضية أو الهوائية أو المائية، أو تنذر بإلحاق هذا الضرر، أو تسهم في اختلال التوازن البيئي.

2- استيراد أو نقل أو تداول المواد والنفايات الخطرة والمواد الضارة بشكل غير مشروع أو السماح بدخولها أو مرورها أو دفنها في أراضي أي دولة طرف أو إلقائها في مياهها الإقليمية.

المادة (17)

الاتجار غير المشروع بالنباتات والحيوانات البرية والأحياء البحرية

تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير في إطار قانونها الداخلي، لتجريم ارتكاب أو المشاركة في ارتكاب الأفعال التالية التي تقوم بها جماعة اجرامية منظمة:

1– بيع النباتات المحظور إقتلاعها والحيوانات البرية والأحياء البحرية ومشتقاتها المحظور صيدها، وفقاً لقانون الدولة الطرف، أو شراؤها، أو استعمالها، أو تداولها، أو الاتجار فيها على أي نحو.

2- حيازة أو إخفاء المتحصلات الناشئة عن أحد الأفعال المجرّمة في الفقرة السابقة.

المادة (18)

الأنشطة المتعلقة بالمواد المخدرة والمؤثرات العقلية

تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير تشريعية وتدابير أخرى لتجريم ارتكاب أو المشاركة في ارتكاب الأنشطة غير المشروعة المتعلقة بالمواد المخدرة والمؤثرات العقلية، وفقاً للأحكام المعتمدة في الاتفاقية العربية لمكافحة الاتجار غير المشروع بالمخدرات والمؤثرات العقلية، وذلك في حال ارتكابها من مجموعة إجرامية منظمة .

المادة (19)

الإنتاج أو الاتجار غير المشروعين بالأسلحة

تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير لتجريم الأفعال التالية عندما تقع عمداً من جانب جماعة إجرامية منظمة أو أحد أعضائها:

1- الانتاج غير المشروع لأية مواد متفجرة أو أسلحة نارية أو ذخائر، أو صنعها، أو تجميعها، أو تهريبها، أو الاتجار أو الوساطة فيها، أو تسليمها، أو تسلمها، أو حيازتها، أو اقتنائها، أو نقلها، أو التصرف فيها.
2- صنع أجهزة أو آلات أو أدوات أو مواد أو أجزاء تستخدم في إنتاج الأسلحة النارية أو الذخائر أو المتفجرات، أو الاتجار أو الوساطة فيها، أو تسليمها، أو تسلمها، أو حيازتها، أو اقتنائها، أو نقلها، أو التصرف فيها.
3- تنظيم أو إدارة أو تمويل أي من الأفعال المذكورة في الفقرتين (1 ، 2) أعلاه.

المادة (20)

سرقة وتهريب العربات ذات المحرك

تتعهد كل دولة طرف بأن تتخذ ما يلزم من تدابير في إطار قانونها الداخلي، لتجريم سرقة العربات ذات المحرك كالسيارات والشاحنات وما يشابهها من آليات وتهريبها، عندما تقع من قبل جماعة إجرامية منظمة.

المادة (21)

الاستعمال غير المشروع لتقنية أنظمة المعلومات

تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير في إطار قانونها الداخلي، لتجريم ارتكاب أو المشاركة في ارتكاب الأفعال التالية التي تقوم بها جماعة اجرامية منظمة في نطاق الاستعمال غير المشروع لتقنية أنظمة المعلومات:

1- الاختراق غير المشروع أو تسهيل الاختراق غير المشروع على نحو كلي أو جزئي لأحد نظم المعلومات.
2- تعطيل أو تحريف تشغيل أحد نظم المعلومات.
3- إدخال بيانات بطرق غير مشروعة في أحد نظم المعلومات أو مسح أو تعديل أو نسخ أو نشر البيانات التي يحتويها هذا النظام بطريق غير مشروع.
4- استيراد، أو حيازة، أو عرض، أو ترك، أو اتاحة إحدى المعدات أو الأدوات أو برامج تقنية المعلومات، بدون سبب مشروع بهدف إرتكاب إحدى الجرائم المنصوص عليها في الفقرات الثلاث السابقة.
5- أي جريمة من الجرائم التقليدية ترتكب باحدى وسائل تقنية أنظمة المعلومات.

المادة (22)
إعاقة سير العدالة

تتعهد كل دولة طرف أن تجعل ارتكاب أي جريمة من الجرائم الآتية خاضعاً لجزاءات أو تدابير احترازية أو الأمرين معاً، على أن تراعى فيها خطورة الجريمة وعدم اغفال العقوبات التبعية أو التكملية، وذلك عندما ترتكب عمداً، وفي نطاق جريمة من الجرائم المشمولة بهذه الاتفاقية:

1- شهادة الزور في جريمة والتحريض على ذلك .
2- إكراه شاهد على عدم أداء الشهادة أو على الشهادة زوراً .
3- الانتقام من شاهد لادلائه بشهادته.
4- إفساد الأدلة أو العبث بها .
5- عدم الإبلاغ عن الجريمة أو الإدلاء بمعلومات غير صحيحة.
6- من علم بوقوع جناية أو جنحة أو كان لديه ما يحمله على الاعتقاد بوقوعها وأعان الجاني بأي طريقة كانت على الفرار من وجه العدالة .
7- استعمال القوة او التهديد لمنع موظف في جهاز العدالة أو الأمن من أداء مهامه الرسمية في إجراءات تتعلق بارتكاب جرائم مشمولة بهذه الاتفاقية.

المادة (23)
الاشتراك في جماعة إجرامية منظمة

تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية جنائياً:

1- الاتفاق مع شخص آخر أو أكثر على ارتكاب جريمة خطيرة لغرض له صلة مباشرة أو غير مباشرة بالحصول على منفعة مالية أو منفعة مادية أخرى وينطوي حيثما يشترط القانون الداخلي ذلك على فعل يقوم به أحد المشاركين يساعد على تنفيذ الاتفاق، أو تضلع فيه جماعة إجرامية منظمة.
2- قيام الشخص بأعمال المشاركة مع علمه بهدف الجماعة الإجرامية المنظمة ونشاطها الإجرامي العام أو بعزمها على ارتكاب الجرائم المنصوص عليها في هذه الاتفاقية.
3- يمكن الاستدلال على العلم أو القصد أو الهدف أو الغرض أو الاتفاق المشار إليه في الفقرتين (1) و (2) أعلاه من ملابسات الوقائع الموضوعية.

المادة (24)
التقادم

تحدد كل دولة طرف وفقاًَ لقانونها الداخلي مدة تقادم طويلة لأية جريمة مشمولة بهذه الاتفاقية.

المادة (25)
الاعفاء أو التخفيف من العقوبة

تتعهد كل دولة طرف أن تتخذ ما يلي:

1- الاعفاء من العقوبات المقررة للجرائم المشمولة بهذه الاتفاقية لكل من بادر من أعضاء الجماعة الإجرامية المنظمة بإبلاغ السلطات القضائية أو الإدارية بما يعلمه عن الجريمة قبل البدء في تنفيذها.
2- التخفيف من العقوبات المقررة للجرائم المشمولة بهذه الاتفاقية لكل من بادر من أعضاء الجماعة الإجرامية المنظمة بإبلاغ السلطات القضائية أو الإدارية بما يعلمه عن الجريمة

بعد تنفيذها ومكن بهذا الإبلاغ السلطات المختصة أثناء التحقيق من القبض على مرتكبي الجريمة الآخرين أو على مرتكبي جريمة أخرى مماثلة لها في النوع أو الخطورة .

الفصل الثالث: التعاون القانوني والقضائي

المادة (26)

المساعدة القانونية المتبادلة

1 – تتعهد الدول الأطراف أن تقدم كل منها للأخرى أكبر قدر من المساعدة القانونية المتبادلة فى الملاحقات وإجراءات الإستدلال، والتحقيقات، والإجراءات القضائية الأخرى فيما يتعلق بالجرائم المشمولة بهذه الاتفاقية.

2 - للدول الأطراف أن تطلب فيما بينها المساعدة القانونية المتبادلة لأحد الأغراض الآتية:

أ – ضبط الممتلكات والأموال المتحصلة من الجرائم المشمولة بهذه الاتفاقية أو حجزها أو تجميدها أو مصادرتها أو تسليمها.

ب – القيام بعمليات التفتيش .

ج – فحص الأشياء ومعاينة المواقع .

د – الحصول على أدلة أو أقوال من الأشخاص وتلقي تقارير الخبراء .

هـ- تبادل صحف الحالة الجنائية وتبليغ المستندات القضائية عموماً .

و- كشف المتحصلات أو الممتلكات أو الأدوات أو الأشياء الأخرى أو اقتفاء أثرها لأغراض الحصول على أدلة .

ز - تيسير مثول الأشخاص فى الدولة الطرف التى تطلب ذلك .

ح - أي شكل آخر من أشكال المساعدة بما لا يتعارض مع قانون الدولة الطرف متلقية الطلب.

3 - يجوز للسلطات المختصة في كل دولة طرف فيما لا يتعارض مع قانونها الداخلي ودون أن تتلقى طلبا مسبقا أن تحيل معلومات متعلقة بمسائل جنائية إلى سلطة مختصة في دولة طرف أخرى متى قدرت أن هذه المعلومات قد تساعد تلك السلطة على القيام بالتحريات والإجراءات الجنائية أو إتمامها بنجاح، أو أن المعلومات قد تفضي إلى قيام تلك السلطة بتقديم طلب عملا بهذه الاتفاقية. ويتعين على السلطة المختصة التي تتلقى المعلومات أن تمتثل لأي طلب بإبقاء تلك المعلومات طي الكتمان بشكل دائم أو مؤقت أو بفرض قيود على استخدامها.

4 - يصاغ طلب المساعدة القانونية بشكل يحدد فيه نطاق الجريمة أو الواقعة أو الإجراء محل المساعدة، في حال الاستعجال يقدم الطلب بأية وسيلة من وسائل الاتصال الأكثر سرعة التي تترك أثراً كتابياً أو مادياً ، ويتعين أن يتضمن طلب المساعدة على وجه الخصوص البيانات الآتية:

أ - السلطة مقدمة الطلب .

ب- موضوع وطبيعة التحقيق أو الملاحقة أو الإجراءات التي يتعلق بها الطلب، واسم ووظائف السلطة التي تتولى التحقيق أو الملاحقة أو الإجراءات.

ج- ملخصا للوقائع ذات الصلة بالموضوع وتكييفها القانوني باستثناء الطلبات المقدمة لغرض تبليغ مستندات قضائية .

د- وصفا للمساعدة القانونية الملتمسة وتفاصيل أي إجراء آخر تود الدولة الطرف الطالبة إتباعه.

ه- هوية الشخص المعني وجنسيته وحيثما أمكن مكان وجوده.

و- الغرض الذي تطلب من أجله الأدلة أو المعلومات أو التدابير.

5 - لا يجوز للدول الأطراف أن ترفض طلب مساعدة قانونية لمجرد أن الجرم يعتبر أيضاً منطوياً على مسائل مالية.

المادة (27)

حالات رفض المساعدة القانونية المتبادلة

لا يجوز للدولة الطرف متلقية الطلب رفض تقديم المساعدة القانونية إلا في الحالات التالية مع بيان سبب الرفض إذا كانت المساعدة:

1- تمس سيادتها أو أمنها أو مصالحها الأساسية .
2- تتعارض مع قوانينها الداخلية .
3- ستلحق ضرراً بالتحقيقات أو الإجراءات القائمة على إقليمها في الجريمة موضوع طلب المساعدة.
4- تتعارض مع حكم قضائي بات صادر في إقليمها.

المادة (28)

التحقيقات المشتركة

تنظر الدول الأطراف في إبرام اتفاقيات أو ترتيبات ثنائية أو متعددة الأطراف تجيز للسلطات المختصة المعنية أن تنشئ هيئات أو لجان تحقيق مشتركة فيما يتعلق بالمسائل التي هي موضوع تحقيقات أو ملاحقات أو إجراءات قضائية في دولة أو أكثر. وفي حال عدم وجود اتفاقيات أو ترتيبات كهذه، يجوز القيام بالتحقيقات المشتركة بالاتفاق في كل حالة على حدة وتكفل الدول الأطراف المعنية الاحترام لسيادة الدولة الطرف التي سيجري ذلك التحقيق داخل إقليمها.

المادة (29)

نقل الإجراءات الجنائية

تنظر الدول الأطراف في إمكانية أن تنقل إحداها إلى الأخرى إجراءات الملاحقة المتعلقة بجرم مشمول في هذه الاتفاقية في الحالات التي يعتبر فيها ذلك النقل في صالح حسن سير العدالة وخصوصاً عندما يتعلق الأمر بعدة ولايات قضائية وذلك بهدف تركيز الملاحقة.

المادة (30)

تسليم المتهمين

1 - على كل دولة طرف، ومع مراعاة الأحكام الواردة في الاتفاقيات ذات الصلة ، اتخاذ التدابير اللازمة لتفعيل نظام تسليم الأشخاص المتهمين أو المحكوم عليهم بسبب إحدى الجرائم المشمولة بهذه الاتفاقية .
2 - تتعهد كل من الدول الأطراف بتسليم المتهمين والمحكوم عليهم في الجرائم المشمولة بهذه الاتفاقية المطلوب تسليمهم إلى أي من هذه الدول وذلك طبقا للقواعد والشروط المنصوص عليها في هذه الاتفاقية.
3 - إذا لم تقم الدولة الطرف بتسليم المتهم الموجود لديها فيما يتعلق بإحدى الجرائم المشمولة بهذه الاتفاقية استناداً إلى ثبوت ولايتها القضائية بملاحقة هذا الجاني، وجب عليها أن تحيل القضية دون إبطاء إلى سلطاتها المختصة لاتخاذ الإجراءات القانونية لمحاكمته.
4 - لا يجوز للدول الأطراف أن ترفض طلب التسليم لمجرد أن الجرم يعتبر أيضاً منطوياً على مسائل مالية.

5 - يجوز لكل دولة طرف أن تمتنع عن تسليم مواطنيها فيما يتعلق بإحدى الجرائم المشمولة بهذه الاتفاقية. ولكن يتعين عليها اتخاذ الإجراءات القانونية لمحاكمة الشخص المطلوب تسليمه أو تنفيذ الحكم الصادر ضده وفقا لأحكام المادة (35) من هذه الاتفاقية.

6 - يعتد بجنسية الشخص في وقت ارتكاب الجريمة المشمولة بهذه الاتفاقية والمطلوب من أجلها التسليم.

المادة (31)

الحالات التي يجوز فيها رفض التسليم

يجوز للدولة الطرف المطلوب منها التسليم رفض طلب التسليم في الحالات التالية :

1- إذا كانت الجريمة المطلوب من أجلها التسليم قد ارتكبت في إقليم الدولة الطرف المطلوب منها التسليم إلا إذا كانت هذه الجريمة قد أضرت بالمصالح الجوهرية للدولة الطرف طالبة التسليم وكان قانون هذه الدولة يمنحها ولاية قضائية بملاحقة مرتكبي هذه الجرائم ما لم تكن الدولة المطلوب منها التسليم قد بدأت إجراءات التحقيق أو المحاكمة.

2- إذا كانت الجريمة المطلوب من أجلها التسليم قد صدر بشأنها حكم قضائي من محاكم الدولة الطرف المطلوب منها التسليم أو من محاكم دولة أخرى وكان هذا الحكم باتاً غير قابل للطعن بأي من أوجه الطعن وفقاً لقانون الدولة التى أصدرت الحكم .

3- إذا كانت الدعوى العمومية الناشئة عن الجريمة المطلوب من أجلها التسليم ، عند وصول طلب التسليم قد انقضت أو كانت العقوبة المحكوم بها قد سقطت لأي سبب من أسباب السقوط أو الانقضاء، وفقاً لقانون الدولة طالبة التسليم.

4- إذا كانت الجريمة قد ارتكبت خارج إقليم الدولة الطرف طالبة التسليم من شخص لا يحمل جنسية هذه الدولة وكان قانون الدولة الطرف المطلوب منها التسليم لا يجيز ملاحقة مثل هذه الجريمة إذا ارتكبت خارج إقليم الدولة من مثل هذا الشخص.

5- إذا كانت الجريمة المطلوب من أجلها التسليم معتبرة بمقتضى القوانين النافذة لدى الطرف المطلوب منه التسليم جريمة ذات صبغة سياسية أو تنحصر في الاخلال بالواجبات العسكرية.

المادة (32)

ضبط ومصادرة وتسليم الأشياء والمتحصلات

الناتجة عن الجريمة

1 - تلتزم كل دولة طرف إثر تلقيها طلباً من دولة طرف أخرى لها ولاية قضائية بشأن إحدى الجرائم المشمولة بهذه الاتفاقية أن تتخذ ما يلزم من تدابير لكشف المتحصلات الإجرامية أو الممتلكات أو الأدوات أو أي أشياء أخرى ذات صلة بالجريمة واقتفاء أثرها وتجميدها أو ضبطها بغرض مصادرتها .

2 - يكون للدولة الطرف أن تحيل إلى سلطاتها المختصة طلب المصادرة المتعلقة بالجرائم المشمولة بهذه الاتفاقية والصادر من سلطات الدولة الطرف الطالبة لتنفيذه بالقدر المطلوب، وذلك وفقا للقواعد والإجراءات التي يتضمنها قانونها الداخلي.

3 - إذا تقرر تسليم الشخص المطلوب تسليمه ، تلتزم الدولة الطرف المطلوب منها التسليم بضبط وتسليم الأشياء والعائدات المتحصلة من إحدى الجرائم المطلوب فيها التسليم أو المستعملة فيها أو المتعلقة بها للدولة الطرف الطالبة سواء وجدت في حيازة الشخص المطلوب تسليمه أو لدى الغير ما لم تعد حيازة هذه الأشياء جريمة في الدولة المطلوب منها التسليم. أو أن تلك الأشياء تعتبر جزءاً من الأدلة في تحقيق أو محاكمة ضد ذلك الشخص ،

ويجوز تسليم هذه الأشياء ولو لم يتحقق تسليم الشخص المقرر تسليمه بسبب هروبه أو وفاته أو لأي سبب آخر.

4 - لا يجوز تفسير أحكام هذه المادة على نحو يخل بما يثبت من حقوق مقررة لأي من الدول الأطراف أو الغير حسن النية على الأشياء أو المتحصلات المذكورة.

5 - تتصرف كل دولة طرف في المتحصلات أو الممتلكات المصادرة أو الأموال الناتجة عن بيعها وفقاً لأحكام قانونها الداخلي، ويجوز للدول الأطراف المعنية الاتفاق فيما بينها على كيفية التصرف فيها مع النظر في إمكانية رد عائدات الجرائم أو الممتلكات المصادرة إلى الدولة الطرف الطالبة لتقديمها أو جزء منها كتعويضات إلى أصحابها الشرعيين.

المادة (33)
حصانة الشهود والخبراء

كل شاهد أو خبير يطلب حضوره لدى أحد الدول الأطراف ، ويحضر بمحض اختياره لهذا الغرض أمام الهيئات القضائية لدى الدولة الطرف الطالبة ، يتمتع بحصانة تحول دون اتخاذ أية إجراءات جزائية بحقه أو القبض عليه أو حبسه عن أفعال أو تنفيذ أحكام سابقة على دخوله إقليم الدولة الطرف الطالبة ، ويتعين على الجهة المعنية التي طلبت الشاهد أو الخبير إخطاره كتابة بهذه الحصانة قبل حضوره لأول مرة. وتزول هذه الحصانة عن الشاهد أو الخبير بانقضاء ثلاثين يوما من تاريخ طلبه أصولاً باستغناء السلطات المختصة لدى الدولة الطرف الطالبة عنه دون أن يغادر هذه الدولة مع عدم قيام ما يحول دون ذلك لأسباب خارجة عن إرادته أو إذا عاد إليها بمحض اختياره بعد أن غادرها.

المادة (34)
نقل الشهود والخبراء والضمانات الخاصة بهم

1- تلتزم كل دولة طرف أن تتخذ التدابير المناسبة للسماح بنقل الشهود والخبراء المسلوبة حريتهم لديها المطلوب حضورهم في دولة طرف أخرى للإدلاء بشهادتهم، أو للمساعدة في التحقيقات إذا قبل الشخص المعنى بذلك صراحة. ولا يجوز أن يكون النقل لغرض المثول للمحاكمة.

2 - يمنع على الدولة الطرف الطالبة التي ينقل إليها أي من الأشخاص الوارد ذكرهم في الفقرة (1) من هذه المادة أن تقوم بتسليمهم إلى دولة ثالثة أو اتخاذ أية اجراءات جزائية بحق أي منهم أو تنفيذ أحكام سابقة عليه .

3 - تلتزم الدولة التي ينقل إليها الشخص المشار إليه في الفقرة (2) من هذه المادة أن تبقى عليه محبوسا وأن تعيده إلى الدولة التي نقل منها فى الأجل الذي تحدده تلك الدولة، أو بمجرد زوال المبررات التي دعت إلى طلبه، أو حسبما يتفق عليه بين الدولتين.

4 - تحتسب المدة التي يقضيها الشخص المحبوس المطلوب نقله في الدولة الطرف التي نقل إليها ضمن مدة العقوبة المقررة عليه أصلاً في الدولة الطرف المنقول منها.

المادة (35)

مصروفات سفر وإقامة الشهود والخبراء

للشاهد أو الخبير الحق في تقاضي مصروفات السفر والإقامة وما فاته من أجر أو كسب من الطرف المتعاقد الطالب ، كما يحق للخبير المطالبة باتعابه نظير الإدلاء برأيه ويحدد ذلك كله بناء على التعريفات والأنظمة المعمول بها لدى الطرف المتعاقد الطالب.

وتبين في أوراق الإعلان المبالغ التي تستحق للشاهد أو الخبير ويدفع الطرف المتعاقد الطالب مقدما هذه المبالغ إذا طلب الشاهد أو الخبير ذلك .

المادة (36)

حماية الشهود والخبراء والضحايا

1 - تلتزم كل دولة طرف أن تتخذ ما يلزم من تدابير لتوفير الحماية من أي انتقام أو ترهيب محتمل للشهود والخبراء الذين يوافقون على الإدلاء بأقوالهم بخصوص إحدى الجرائم المشمولة بهذه الاتفاقية، وكذلك لأقاربهم وسائر الأشخاص وثيقي الصلة بهم حسب الاقتضاء.

2 - تتخذ كل دولة طرف ما يلزم من تدابير لتوفير المساعدة والحماية من أي انتقام أو ترهيب لضحايا الجرائم المشمولة بهذه الاتفاقية وأن توفر لهم سبل الحصول على التعويض وجبر الأضرار التي لحقت بهم.

3 - تنظر الدول الأطراف في أن تشمل التدابير المشار إليها في الفقرتين السابقتين ما يأتي:

أ - توفير الحماية لأولئك الأشخاص، من خلال تغيير أماكن اقامتهم وعدم افشاء أية معلومات تتعلق بهوياتهم وأماكن وجودهم.

ب - إتاحة الإدلاء بالشهادة على نحو يكفل سلامة الشهود والخبراء والضحايا، ويجوز استخدام التقنيات الحديثة في هذا المجال.

4 - للدول الأطراف أن تنظر في إبرام اتفاقات أو ترتيبات فيما بينها أو مع دولة أخرى من أجل توفير الحماية للشهود والخبراء والضحايا.

المادة (37)

تدابير مكافحة الجريمة المنظمة

تتعهد الدول الأطراف فيما بينها بالقيام بما يلي لتعزيز فاعلية تنفيذ القوانين التي تستهدف مكافحة الجرائم المشمولة بهذه الاتفاقية:

1- الحيلولة دون اتخاذ اقليمها مسرحاً للتخطيط لأي من الجرائم المنظمة أو تنفيذها أو الشروع أو الاشتراك فيها بأي صورة من الصور، والعمل على منع تسلل العناصر الإجرامية إلى اقليمها أو اقامتها فيها أفراداً أو جماعات .

2- تطوير الأنظمة والقوانين المتعلقة بإجراءات المراقبة وتأمين الحدود والمنافذ البرية والبحرية والجوية.

3- تبادل المعلومات بشأن الجرائم المشمولة بهذه الاتفاقية بما في ذلك صلاتها مع الأنشطة الإجرامية الأخرى، وكذلك الوسائل التي تستخدمها الجماعات الإجرامية المنظمة لاسيما تلك التي تتم باستخدام التقنيات الحديثة

4- إجراء التحريات الرامية إلى رصد حركة متحصلات الجرائم أو الممتلكات أو المعدات أو سائر الأدوات المستخدمة أو المراد استخدامها في ارتكاب تلك الجرائم.

5- الكشف عن هوية الأشخاص المشتبه في ضلوعهم في ارتكاب أي من الجرائم المشمولة بهذه الاتفاقية وأنشطتهم وأماكن تواجدهم .
6- تفعيل التنسيق بين مختلف الأجهزة والجهات المعنية بمكافحة الجرائم المنظمة وتشجيع تبادل زيارة العاملين والخبراء في تلك الجهات ، وتطوير برامج تدريب مشتركة خاصة بالعاملين في الأجهزة المعنية بتنفيذ القانون الجنائي بمن فيهم أعضاء النيابة العامة وقضاة التحقيق وغيرهم.
7- زيادة وعي الناس بوجود الجريمة المنظمة وأسبابها وجسامتها والخطر الذي تشكله.

المادة (38)
الاعتراف بالأحكام الجنائية والمدنية

على كل دولة طرف، في شأن تنفيذ أحكام هذه الاتفاقية وتحقيق الغاية منها ، أن تعترف بالأحكام الجزائية والمدنية الباتة الصادرة من محاكم دولة طرف أخرى بشأن إحدى الجرائم المشمولة بهذه الاتفاقية، ويستثني من ذلك الاعتراف الآتي :
1- الأحكام المخالفة للشريعة الإسلامية أو للأنظمة الأساسية أو لأحكام الدستور أو النظام العام في الدولة المطلوب إليها الاعتراف.
2- الأحكام التى مازالت قابلة للطعن فيها بأحد أوجه الطعن المقررة في قانون الدولة التى صدر الحكم من احدى محاكمها.
3- الأحكام الصادرة في جريمة تدخل أصلا ضمن الولاية القضائية للدولة المطلوب منها أخذ الحكم في الاعتبار متى باشرت فيها أيا من إجراءات التحقيق أو المحاكمة.

المادة (39)
الولاية القضائية بملاحقة الجرائم المشمولة بهذه الاتفاقية

1 - تتخذ الدول الإطراف ما يلزم من تدابير لتقرير اختصاص سلطاتها وأجهزتها القضائية بملاحقة وبالنظر في الجرائم المشمولة بهذه الاتفاقية في الحالات الآتية :
أ - عندما تقع الجريمة كلها أو أحد عناصرها في إقليم الدولة، أو حينما يتم الإعداد أو التخطيط أو الشروع بالجريمة أو تتحقق إحدى صور المساهمة فيها في هذا الإقليم، أو حينما تمتد آثار الجريمة إليه .
ب- عندما ترتكب الجريمة على النحو السابق ذكره في الفقرة السابقة على متن سفينة ترفع علم الدولة أو طائرة مسجلة في سجلات الدولة .
ج– عندما تقع الجريمة من قبل أو ضد أحد مواطني الدولة .
د - إذا وجد فاعل الجريمة أو الشريك أو المساهم في ارتكابها في إقليم الدولة سواء كان يقيم فيها على نحو معتاد أم عابر .
هـ- إذا كانت الجريمة تمثل اعتداء على أحد المصالح العليا للدولة.
2 - لا تستبعد هذه الاتفاقية ممارسة أي اختصاص جنائي مقرر من قبل أي دولة طرف وفقا لقانونها الداخلي.

المادة (40)

آلية تنفيذ الاتفاقية

يتولى مجلسا وزراء العدل والداخلية العرب بالتنسيق مع المجالس الوزارية المعنية الإشراف على متابعة تنفيذ هذه الاتفاقية ولهما في هذا الصدد إنشاء الآليات اللازمة لذلك الغرض وعلى وجه الخصوص :

1- إنشاء قاعدة بيانات فيما يتصل بتطبيق هذه الاتفاقية.
2- إنشاء سجل جنائي عربي بشأن الأشخاص المحكوم عليهم بأحكام إدانة نهائية وباتة عن إحدى الجرائم المشمولة بهذه الاتفاقية.

الفصل الرابع: أحكام ختامية

1- تكون هذه الاتفاقية محلا للتوقيع والتصديق عليها أو قبولها أو إقرارها من الدول الأعضاء، وتودع وثائق التصديق أو القبول أو الإقرار لدى الأمانة العامة لجامعة الدول العربية في موعد أقصاه ثلاثون يوما من تاريخ التصديق أو القبول أو الإقرار، وعلى الأمانة العامة إبلاغ سائر الدول الأعضاء بكل إيداع لتلك الوثائق وتاريخه.
2- تدخل هذه الاتفاقية حيز التنفيذ بعد مضي ثلاثين يوما من تاريخ إيداع وثائق التصديق عليها أو قبولها أو إقرارها من سبع دول عربية.
3- يجوز لأية دولة من دول الجامعة العربية غير الموقعة على هذه الاتفاقية أن تنضم إليها، وتعتبر الدولة طرفاً في هذه الاتفاقية بعد مضي ثلاثين يوماً على تاريخ إيداع وثيقة التصديق أو القبول أو الإقرار أو الانضمام لدى الأمانة العامة لجامعة الدول العربية.
4- لا تخل هذه الاتفاقية بالاتفاقيات الخاصة بين بعض الدول الأعضاء وفي حالة تعارض أحكام هذه الاتفاقية مع أحكام أي اتفاقية خاصة فتطبق الاتفاقية الأكثر تحقيقاً لمكافحة الجريمة المنظمة عبر الحدود الوطنية.
5- لا يجوز لأية دولة من الدول الأطراف أن تبدي أي تحفظ ينطوي على مخالفة لنصوص هذه الاتفاقية أو خروج على أهدافها.
6- يجوز تكملة هذه الاتفاقية بملحق أو أكثر ولا تكون الدولة الطرف في هذه الاتفاقية ملزمة بأي ملحق ما لم تصبح طرفاً فيه وفقاً لأحكامه.
7- يجوز للدولة الطرف أن تقترح تعديل أي نص من نصوص هذه الاتفاقية وتحيله إلى الأمين العام لجامعة الدول العربية الذي يقوم بإبلاغه إلى الدول الأطراف في الاتفاقية لاتخاذ قرار باعتماده بأغلبية ثلثي الدول الأطراف، ويصبح هذا التعديل نافذاً بعد مضي ثلاثين يوما من تاريخ إيداع وثائق التصديق أو القبول أو الإقرار من سبع دول أطراف لدى الأمانة العامة لجامعة الدول العربية.
8- يمكن لأية دولة طرف أن تنسحب من هذه الاتفاقية بناء على طلب كتابي ترسله إلى أمين عام جامعة الدول العربية.

ويرتب الانسحاب أثره بعد مضي ستة أشهر من تاريخ إرسال الطلب إلى أمين عام جامعة الدول العربية.

حـررت هـذه الاتفاقيــة باللغــة العربيــة بمدينــة القــاهرة فــي جمهوريــة مصــر العربيــة في 1432/1/15هـ ، الموافق 2010/12/21م من أصل واحد مودع بالأمانـة العامـة لجامعة الدول العربية (الأمانة الفنية لمجلس وزراء العدل العرب)، ونسخة مطابقة للأصل تسلم للأمانـة العامة لمجلس وزراء الداخلية العرب ، وتسلم كذلك نسخة مطابقة للأصل لكل دولـة من الدول الأطراف .

وإثباتاً لما تقدم، قام أصحاب السمو والمعالي وزراء الداخلية والعدل العرب، بتوقيع هذه الاتفاقية، نيابـة عن دولـهم.

قائمة الدول العربية الموقعة والمصدقة على
الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية

1- وافق عليها مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 1432/1/15هـ الموافق 2010/12/21م.

2- دخلت هذه الاتفاقية حيز النفاذ بتاريخ 2013/10/5 بعد مضي ثلاثين يوما من تاريخ إيداع وثائق التصديق أو القبول أو الإقرار من سبع دول عربية لدى الأمانة العامة وذلك عملاً بالفقرة (2) من الأحكام الختامية للاتفاقية.

الدولة	تاريخ التوقيع	تاريخ التصديق أو الانضمام
المملكة الأردنية الهاشمية	2010/12/21	2013/1/8
دولة الإمارات العربية المتحدة	2010/12/21	2012/7/4
مملكة البحرين	2010/12/21	
الجمهورية التونسية	2010/12/21	
الجمهورية الجزائرية الديمقراطية الشعبية	2010/12/21	
جمهورية جيبوتي		
المملكة العربية السعودية	2010/12/21	2012/6/24
جمهورية السودان	2010/12/21	
الجمهورية العربية السورية	2010/12/21	
جمهورية الصومال		
جمهورية العراق	2010/12/21	2013/5/12
سلطنة عمان	2012/2/15	
دولة فلسطين	2010/12/21	2013/5/21
دولة قطر	2010/12/21	2012/3/5
جمهورية القمر المتحدة		
دولة الكويت	2010/12/21	2013/9/5
الجمهورية اللبنانية		
دولة ليبيا	2010/12/21	
جمهورية مصر العربية	2010/12/21	
المملكة المغربية	2010/12/21	
الجمهورية الإسلامية الموريتانية	2010/12/21	
الجمهورية اليمنية	2010/12/21	

قوانين

قانون رقم 09 – 04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إن رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 119 و120 و122 – 7 و126 منه،

– وبمقتضى الأمر رقم 66 – 155 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 66 – 156 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 75 – 58 المؤرّخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدّل والمتمّم،

– وبمقتضى القانون رقم 2000 – 03 المؤرّخ في 5 جمادى الأولى عام 1421 الموافق 5 غشت سنة 2000 الذي يحدّد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 03 – 05 المؤرّخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003 والمتعلق بحقوق المؤلف والحقوق المجاورة،

– وبمقتضى القانون رقم 08 – 09 المؤرّخ في 18 صفر عام 1429 الموافق 25 فبراير سنة 2008 والمتضمن قانون الإجراءات المدنية والإدارية،

– وبعد رأي مجلس الدولة،

– وبعد مصادقة البرلمان،

يصدر القانون الآتي نصه :

الفصل الأول
أحكام عامة

الهدف

المادّة الأولى : يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المصطلحات

المادّة 2 : يقصد في مفهوم هذا القانون بما يأتي :

أ – الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية،

ب – منظومة معلوماتية : أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين،

ج – معطيات معلوماتية : أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها،

د – مقدمو الخدمات :

1 – أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات،

2 – وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها،

هـ – المعطيات المتعلقة بحركة السير: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة،

و – الاتصالات الإلكترونية : أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

مجال التطبيق

المادّة 3 : مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

الفصل الثاني
مراقبة الاتصالات الإلكترونية

الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية

المادّة 4 : يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية :

أ – للوقاية من الأفعال الموصوفة بجرائم الإرهاب أوالتخريب أوالجرائم الماسة بأمن الدولة،

ب – في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني،

ج – لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية،

د – في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة "أ " من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه، إذنا لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة "أ " من هذه المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

الفصل الثالث
القواعد الإجرائية

تفتيش المنظومات المعلوماتية

المادّة 5 : يجوز للسلطات القضائية المختصة وكذا ضبّاط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول، بغرض التفتيش، ولو عن بعد، إلى :

أ – منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب – منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة "أ " من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

حجز المعطيات المعلوماتية

المادّة 6 : عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة

تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

الحجز عن طريق منع الوصول إلى المعطيات

المادّة 7 : إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

المعطيات المحجوزة ذات المحتوى المجرم

المادّة 8 : يمكن السلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة ، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

حدود استعمال المعطيات المتحصل عليها

المادّة 9 : تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

الفصل الرابع

التزامات مقدمي الخدمات

مساعدة السلطات

المادّة 10 : في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

حفظ المعطيات المتعلقة بحركة السير

المادّة 11 : مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ :

أ – المعطيات التي تسمح بالتعرف على مستعملي الخدمة،

ب – المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

ج – الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،

د – المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

هـ – المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ " من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل.

دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج.

يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات.

تحدد كيفيات تطبيق الفقرات 1 و2 و3 من هذه المادة، عند الحاجة، عن طريق التنظيم.

الالتزامات الخاصة بمقدمي خدمة "الإنترنت"

المادّة 12 : زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي خدمات "الإنترنت" ما يأتي :

أ – التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن،

ب – وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

الفصل الخامس

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

إنشاء الهيئة

المادّة 13 : تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم.

مهام الهيئة

المادّة 14 : تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام الآتية :

أ – تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته،

ب – مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية،

ج – تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

الفصل السادس

التعاون والمساعدة القضائية الدولية

الاختصاص القضائي

المادّة 15 : زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

المساعدة القضائية الدولية المتبادلة

المادّة 16 : في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

يمكن، في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أوالبريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

تبادل المعلومات واتخاذ الإجراءات التحفظية

المادّة 17 : تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل.

القيود الواردة على طلبات المساعدة القضائية الدولية

المادّة 18 : يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام.

يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.

المادّة 19 : ينشر هذا القانون في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009.

عبد العزيز بوتفليقة

قائمة المراجع

قائمة المراجع

❖ المراجع باللغة العربية

المراجع العامة:

1. أبو الفضل جمال الدين محمد بن مكرم ابن منظور، لسان العرب، دار صاد، بيروت.
2. أبو زكريا محيي الدين يحيى بن شرف النووي، المنهاج شرح صحيح مسلم بن الحجاج، دار إحياء التراث العربي ، بيروت، الطبعة 2.
3. أحمد بن محمد بن علي الفيومي المقرئ المصباح المنير في غريب الشرح الكبير، مكتبة لبنان، 1987 .
4. جابر إبراهيم الراوي، الحدود الدولية، مطبعة دار السلام،ط1، بغداد، 1975 .
5. جمال إبراهيم الحيدري، شرح أحكام القسم الخاص من قانون العقوبات، ج 1،مطبعة الفائق، بغداد، 1998.
6. عبد الله سليمان، شرح قانون العقوبات قسم عام الجزء الأول للجريمة، دار الهدى.
7. فوزية عبد الستار، شرح قانون العقوبات القسم العام، دار النهضة العربية، القاهرة 1992.
8. محمد بن يعقوب الفيروز آبادي مجد الدين، القاموس المحيط، مؤسسة الرسالة، 2005 الطبعة 8.
9. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية بالقاهرة.
10. مونتغمري، الحرب عبر التاريخ، ترجمة فتحي نسيب نمر، مكتبة الانجلو مصرية، القاهرة، 1967 .

المراجع الخاصة :

1- أبو بكر محمود الهوش، الحكومة الالكترونية، الواقع والآفاق، مجموعة النيل العربية،ط1،مصر،2006.

2- أحمد أمين أبو سعدة ،الدليل العلمي لمتطلبات تطبيق تكنولوجيا المعلومات في المكتبات، الدار المصرية اللبنانية. بدون سنة نشر.

3- أحمد حلمي جمعة، عصام فهد العربيد، زياد أحمد الزعبي، نظم المعلومات المحاسبية، مدخل تطبيقي معاصر، دار المناهج للنشر والتوزيع،ط1 ،2003م.

4- أحمد شرف الدين، عقود التجارة الالكترونية وقانون التجارة الدولية، كلية الحقوق، جامعة عين شمس، القاهرة،2000.

5- أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية،القاهرة،1988 .

6- أمال قارة، الحماية الجزائرية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة و النشر، الجزائر 2006 .

7- أمل وجيه حمدي، المصادر الإلكترونية للمعلومات، الدار المصرية اللبنانية، القاهرة، ط1،2007.

8- بهجة بومعرافي، دورية الاتجاهات الحديثة في المكتبات، ع 20، 2003.

9- بيل جيتس، المعلوماتية بعد الانترنت، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون و الآداب، الكويت، 1998 .

10- ثابت عبد الرحمن ادريس، نظم المعلومات الادارية في المنظمات المعاصرة، الدار الجامعية،الاسكندية،2005.

11- جابر إبراهيم الراوي ، الحدود الدولية، الطبعة1، مطبعة دار السلام، بغداد، 1975 .

12- جاسم محمد جرجس وبديع محمود القاسم، مصادر المعلومات في مجال الإعلام والاتصال الجماهيري، مركز الإسكندرية للوسائط الثقافية والمكتبات،مصر،1998.

13- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، دار البداية، ط1، 2007.

14- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات ، رؤية جديدة للجريمة الحديثة، دار البداية،ط1، 2010 .

15- جلال الزعبي، جرائم تقنية نظم المعلومات، دراسة مقارنة، من دار الثقافة للنشر و التوزيع،الأردن،2014.

16- جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية،القاهرة،ط1، 1992م،

17- حسام شوقى، حماية وأمن المعلومات على الإنترنت، دار الكتب العلمية للنشر والتوزيع، القاهرة، 2003 .

18- حسن طاهر داوود، جرائم نظم المعلومات، الرياض، الأكاديمية نايف العربية للعلوم الأمنية ، 1999.

19- حسن طاهر داود، جرائم نظم المعلومات، الرياض ،أكاديمية نايف العربية للعلوم الأمنية، 2000.

20- حسن طاهر داوود، أمن الشبكات المعلومات، معهد الادارة العامة: السعودية، 2004.

21- حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية، القاهرة.

22- حسن مظفر الرزو، الفضاء المعلوماتي، مركز دراسات الوحدة العربية، بيروت، 2007 ،ص250.

23- حسني عبد الرحمن الشيمي، اللاورقية أو الكتاب الورقي بين الزوال والبقاء،ط1، مصر،1993.

24- حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة جرائم الإنترنت، الإتحاد العربي للتحكيم الإلكتروني2007 .

25- حسين شفيق، الإعلام الجديد و الجرائم الالكترونية، الإرهاب الالكتروني، دار الفكر للطباعة و النشر و التوزيع،2015.

26- حمد خليفة الملط، الجرائم المعلوماتية، الفكر الجامعي، الإسكندرية ،ط2، 2006.

27- حمدون إ. توريه، سامي البشير المرشد، دليل الأمن السبراني للبلدان النامية، الاتحاد الدولي للاتصالات، ط 2007.

28- الحميد نجم عبد الله السامرائي، نظم المعلومات الإدارية، دار وائل،عمان،2005.

29- خالد بن سليمان الغثير، محمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، مركز التمييز لأمن المعلومات، جامعة الملك سعود،ط1 ،2009.

30- خالد بن محمد الغثير، الاصطياد الإلكتروني، الأساليب والإجراءات المضادة، مكتبة الملك فهد الوطنية، الرياض، 2008 .

31- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر و التوزيع،2011

32- هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992.

33- ذياب البداينة، الأمن وحرب المعلومات، ط 1، دار الشروق، عمان، 2002.

34- ذياب البداينة، المنظور الاقتصادي والتقني والجريمة المنظمة، أبحاث الحلقة العلمية حول الجريمة المنظمة وأساليب مكافحتها، نوفمبر 1998م، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 1999 .

35- رافي رينا، إدارة المحتوى و إدارة المعرفة في الحكومة، العراق.

36- سارة الشريف، خصوصية البيانات الرقمية، سلسلة أوراق الحق في المعرفة تصدر عن مركز دعم لتقنية المعلومات، القاهرة.

37- سعيد السيد قنديل، التوقيع الالكتروني، ماهيته وصوره وحجيته في الإثبات، دار الجامعة الجديدة للنشر،الإسكندرية،2004 .

38- سليمان بن صالح العقلا و فؤاد أحمد إسماعيل إنشاء الشبكات، المبادئ الأساسية لإختصاصي المكتبات والمعلومات، مكتبة الملك فهد الوطنية، الرياض، 2000.

39- سليمان مصطفى الدلاهمة، نظم المعلومات المحاسبية و تكنولوجيا المعلومات، الوراق للنشر و التوزيع، عمان ، 2008 .

40- شريف درويش اللبان، تكنولوجيا الاتصال، المخاطر و التحديات و التأثيرات الاجتماعية، القاهرة، الدار المصرية اللبنانية،2000.

41- صالح محمد سعاده ومحمد محمود الراميني و علاء علي حمدان، مقدمة إلى الانترنت، مكتبة المجتمع العربي، عمان ،2008.

42- ضياء أمين مشيمش، التوقيع الالكتروني، دراسة مقارنة، منشورات صادر الحقوقية، لبنان.

43- ضياء علي أحمد نعمان، الغش المعلوماتي، الظاهرة والتطبيقات، مطبعة ووراقة الوطنية،ط1،المغرب، 2001.

44- طارق إبراهيم الدسوقي عطية، الموسوعة الأمنية، الأمن المعلوماتي، دار الجامعة الجديدة،الإسكندرية،2015.

45- طه طارق، إدارة البنوك ونظم المعلومات المصرفية، الإسكندرية، مصر، 2000.

46- عامر إبراهيم قنديلجي، إيمان فاضل السامرائي، حوسبة المكتبات، ط1، دار المسيرة، الأردن،2004.

47- عامر محمود الكسواني، التزوير المعلوماتي للعلامة التجارية، دار الثقافة للنشر و التوزيع، عمان،2014 .

48- عباس العبودي، الحماية القانونية لوسائل التقدم العلمي في الإثبات المدني، الأردن،2002 .

49- عبد الرحمن بن عبدالله السند، الأحكام الفقهية للتعاملات الإلكترونية، دار الوراق ودار النيربين للطباعة والنشر والتوزيع، الرياض 2005 .

50- عبد الرحمن شعبان عطيات، أمن الوثائق والمعلومات، جامعة نايف للعلوم الأمنية، الرياض،2008.

51- عبد الرحمن عبد العزيز الشنيفي، أمن المعلومات وجرائم الحاسب الآلي،ط1،المملكة العربية السعودية، 1994.

52- عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الاسكندرية، 2004.

53- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، 2002.

54- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، بدون ناشر، طبعة مزيدة ومنقحة، 2009.

55- عبد الفتاح بيومي مجازي، الأحداث والإنترنت، دار الفكر الجامعي ،الإسكندرية، 2002.

56- عبد الفتاح بيومي مجازي، صراع الكمبيوتر والانترنت، في القانون العربي النموذجي، دار الكتب القانونية، دار للنشر والبرمجيات، القاهرة 2007.

57- عبد الفتاح مراد، التجارة الالكترونية –البيع والشراء-على شبكة الانترنت، البهاء للنشر الالكتروني، مصر.

58- عبد الفتاح مراد، شرح النصوص العربي لاتفاقيات الجات و منظمة التجارة العالمية، دار الكتب والوثائق المصرية: الإسكندرية.

59- عبد الله الكرم، ونجيب محمد العلى، التعلم الإلكتروني، المفهوم والواقع والتطبيق، التربية والتعليم وتكنولوجيا المعلومات في البلدان العربية، الهيئة اللبنانية للعلوم التربوية، الكتاب السنوي 4، 2005.

60- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2003 .

61- علاء بن محمد صالح الهمص ،وسائل التعرف على الجاني، مكتبة القانون والاقتصاد ، الرياض،2012.

62- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، كلية الحقوق، الإسكندرية، 1999.

63- علي كمال شاكر ،نظم إدارة قواعد البيانات لأخصائي المكتبات والمعلومات، أسس وتطبيقات عملية، ط1،القاهرة،الدار المصرية اللبنانية،2005.

64- عماد عبد الوهاب الصباغ، كتاب نظم المعلومات ماهيتها ومكوناتها، دار الثقافة للنشر والتوزيع،الأردن،2004.

65- عمر محمد بن يونس، المخدرات والمؤثرات العقلية عبر الإنترنت، دار الفكر الجامعي، الإسكندرية 2004.

66- غانم مرضي الشمري، الجرائم المعلوماتية ماهيتها، خصائصها، كيفية التصدي لها، دار الثقافة للنشر و التوزيع، الأردن،2016.

67- القاضي جلال الزعبي، القاضي أسامة المناعسة، جرائم تقنية نظم المعلومات، دراسة مقارنة، دار الثقافة للنشر و التوزيع،الأردن،2014.

68- قطيشات منيب، قواعد البيانات، دار وائل،عمان،2005.

69- محمد احمد غانم ،الجوانب القانونية والشرعية للإثبات الجنائي بالشفرة الوراثية، دار الجامعة الجديدة،2008.

70- محمد أديب رياض الغنيمي، شبكات المعلومات، الحاضر والمستقل، المكتبة الأكاديمية، القاهرة، 1999.

71- محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، الجريمة المعلوماتية، دار الثقافة للنشر و التوزيع، الأردن ،2011.

72- محمد حسام لطفي، الحماية القانونية لبرامج الحاسب الآلي، دار الثقافة للطباعة والنشر، القاهرة 1987 .

73- محمد حسن عمر مطابع الفرزدق، المراجعة والرقابة الداخلية على أعمال الحاسبات الإلكترونية،السعودية،1984.

74- محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة للنشر والتوزيع، الإسكندرية.

75- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري المقارن، دار الجامعة الجديدة،الازارطة،2008.

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

77- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، 2004.

78- محمد علي فارس الزغبي، الحماية القانونية لقواعد البيانات وفقا لقانون حق المؤلف، منشأة المعارف،الإسكندرية،2003.

79- محمد فتحي عيد، الإنترنت ودوره في انتشار المخدرات، مركز البحوث والدراسات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003.

80- محمد فواز مطالقة، النظام القانوني لعقود إعداد برامج الحاسب الآلي، دار الثقافة للنشر و التوزيع، الأردن،2004.

81- محمد محسن عمر، الإدارة والتقنية، شركاء في مواجهة عصر الإنترنت، 1997م.

82- محمود محمد أبو فروة، الخدمات البنكية الالكترونية عبر الانترنت، دار الثقافة للنشر و التوزيع، ط1 ،2009.

83- مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية،ط1 ،2001.

84- مزهر شعبان العاني، شوقي ناجي جواد، العملية الإدارية و تكنولوجيا المعلومات، الشارقة، إثراء للنشر و التوزيع، 2008 .

85- مزياني عبد الغني، الجرائم الماسة بأنظمة المعالجة الآلية للمعلومات، مجلس قضاء المسيلة ،وزارة العدل.

86- مصطفى عبد الغني، الجات و التبعية الثقافية، مركز الحضارة العربية، 1998.

87- مصطفى محمد، أساليب إجرامية بالتقنية الرقمية، ماهيتها و مكافحتها، دار الكتب القانونية، المجلة الكبرى، 2005.

88- منصور محمد عقيل وعلى قاسم، الإنترنت والأبعاد الأمنية، مركز البحوث والدراسات الشرطية، دبي، يناير 1996.

89- منير الجنبيهي وممدوح الجنبيهي، البنوك الالكترونية، دار الفكر الجامعي، مصر، 2006.

90- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي، دار الفكر الجامعي، الإسكندرية، 2004.

91- ناريمان متولي إسماعيل، اقتصاديات المعلومات، دراسة للأسس النظرية وتطبيقاتها العملية على مصر وبعض البلاد الأخرى ،المكتبة الأكاديمية، القاهرة،1995.

92- نايف شايع حسن الدوسري، سلمان بن محمد سلمان ،الأمن المعلوماتي، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الإدارية، السعودية ،2013.

93- نبيل محمد مرسي، نظم المعلومات الإدارية، المكتب الجامعي الحديث، مصر، 2006.

94- نسرين عبد الحميد نبيه، الجانب الإلكتروني للقانون التجاري، منشأة المعارف، الإسكندرية، 2008. جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، دار البداية،ط2010. محمد أمين الرومي، جرائم الكمبيوتر و الانترنيت، دار المطبوعات الجامعية،2003

95- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر و التوزيع، ط1 ، 2008.

96- نوري حمد خاطر، شرح قواعد الملكية الفكرية ، حقوق المؤلف والحقوق المجاورة، العين، جامعة الإمارات، 2008.

97- هاني شحادة ألخوري، تكنولوجيا المعلومات على أعتاب القرن الحادي و العشرين، مركز رضا للكومبيوتر، سوريا، 1998 .

98- هدى قشقوش، الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية، القاهرة.

99- هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة،مصر،1992 .

100-هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، مصر،1995.

101-هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقا عليها)، دار النهضة العربية، الطبعة الأولى، القاهرة، 2007.

102-هيل مايكل، أثر المعلومات في المجتمع، دراسة لطبيعتها وقيمتها و استعمالها ،مركز الإمارات للدراسات و البحوث، أبو ظبي،2004.

103- وسيم شفيق الحجار، الإثبات الإلكتروني، مكتبة صادر ناشرون، بيروت لبنان،2002.

104-ولفرد لانكستر، أساسيات استرجاع المعلومات، مكتبة الملك فهد الوطنية،ط2 ،الرياض،1997.

105-ونسه ديالا عيسى، حماية حقوق التأليف على شبكة الانترنيت، المنشورات الحقوقية، بيروت، 2010.

106-اليافي شادن، الإنسان و المعرفة في عصر المعلومات،دارالعبيكان،الرياض،2001.

107-يونس عرب، جرائم الحاسوب والانترنت، إتحاد المصارف العربية ،ط1، 2002.

108-يونس عرب، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والأنترنت، الجزء الأول، منشورات إتحاد المصارف العربية، ط1.

❖ مذكرات ورسائل الدكتوراه.

أولا : مذكرات الماجستير.

1. آمنة عبد ربه، الجزائر في مجتمع المعلومات سنة 2003 واقع و آفاق ،مذكرة ماجستير في علوم الاعلام و الاتصال، جامعة الجزائر، 2006/2005 .

2. انتصار عباس إبراهيم، اثر وسائل الاتصال في خدمات المكتبات ومراكز المعلومات، مذكرة ماجستير، الخرطوم، جامعة النيلين، 2005 .

3. جمال مزغيش، التجارة الالكترونية على شبكة الانترنت، حالة توجه المؤسسات الجزائرية نحو التجارة الإلكترونية، مذكرة ماجستير، جامعة الجزائر ،جوان2001 .

4. دليلة العوفي، مجتمع المعلومات في الجزائر واقع الفجوة الرقمية، مذكرة ماجستير في علوم الاعلام و الاتصال، جامعة الجزائر،2007/2006 .

5. شوقي شادلي، أثر استخدام تكنولوجيا الإعلام و الاتصال على أداء المؤسسات الصغيرة و المتوسطة، رسالة ماجستير في العلوم الاقتصادية ،جامعة ورقلة، الجزائر ، 2008.

6. محمد مجبر، التجارة الالكترونية و أفاق تطورها في العالم العربي، مذكرة ماجستير، جامعة سعد دحلب، كلية العلوم الاقتصادية، جوان 2006 .

7. مراد رايس،أثر تكنولوجية المعلومات على الموارد البشرية في المؤسسة، مذكرة ماجستير في علوم التسيير، فرع إدارة الأعمال ،جامعة الجزائر 2005- 2006 .

ثانيا : رسائل الدكتوراه

1. عبد الرحمن بن عبد الله السند، أحكام تقنية المعلومات، الحاسب الآلي وشبكة المعلومات، رسالة الدكتوراه في الفقه المقارن، جامعة الإمام محمد بن سعود الإسلامية، المعهد العالي للقضاء قسم الفقه المقارن، 2004.

2. عبد الكريم غالي، الحماية القانونية للإنسان من مخاطر المعلوماتيات، رسالة دكتوراه، كلية العلوم القانونية والاقتصادية والاجتماعية،الرباط،1995.

3. لمين علوطي، أثر تكنولوجيا المعلومات والإتصالات على إدارة الموارد البشرية بالمؤسسة، رسالة دكتوراه، كلية العلوم الاقتصادية، جامعة الجزائر، 2008 .

❖ **التشريعات الجزائرية و الدولية المتعلقة بالأمن المعلوماتي :**

أولا : الدستور:

الدستور الجزائري رقم 16-01 المؤرخ في 06 مارس *2016* الجريدة الرسمية رقم 14 المؤرخة في 7 مارس *2016*.

ثانيا: القوانين الجزائرية

1. الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966والمتضمن قانون العقوبات،ج.ر.71.المعدل القانون رقم 04-15 الصادر

في 10-11-2004المعدل و المتمم لقانون العقوبات، و المعدل والمتمم بالقانون رقم16-02المؤرخ في 14رمضان 1437الموافق ل19جوان 2016، ج.ر.ع37.

2. القانون رقم 06-22 الصادر في 20-12-2006المعدل والمتمم لقانون الإجراءات الجزائية.
3. القانون رقم 09-04 الصادرفي05-08-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها.
4. القانون رقم 04 – 14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66 – 155 المتضمن قانون الإجراءات الجزائية (الجريدة الرسمية عدد 71 بتاريخ 10 نوفمبر 2004)،تنشأ لدى وزارة العدل مصلحة لنظام آلي وطني لصحيفة السوابق القضائية مرتبطة بالجهات القضائية .
5. القانون رقم 08 – 04 المؤرخ في 23 جانفي 2008 المتضمن القانون التوجيهي للتربية الوطنية، يشير هذا القانون في مادتيه 02 و 04 إلى التكوين واكتساب المعارف في مجال تكنولوجيا الإعلام والاتصال وإدماجه في المحيط التربوي و مجتمع المعرفة. (الجريدة الرسمية عدد 04 بتاريخ 27 جانفي 2008).
6. القانون 2000-03المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.
7. القانون رقم 05 -10 المؤرخ في 20 جوان 2005 المعدل والمتمم الأمر رقم 5 – 58، ج.ر.ع. 44 بتاريخ 26 جوان 2005.المتضمن القانون المدني الجزائري
8. القانون رقم 15 - 04 المؤرخ في 01 فيفري 2015 المتضمن تحديد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين في الجزائر ،ج.ر.ع. 06 بتاريخ 10فيفري 2015.
9. القانون رقم 03-17 مؤرخ في 9 رمضان عام 1424 الموافق 4 نوفمبر عام 2003،يتضمن الموافقة على الأمر رقم 03-05 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 19يوليو عام 2003 والمتعلق بحقوق المؤلف والحقوق المجاورة.

10. قانون الإعلام الصادر بموجب القانون العضوي رقم 12-05 المؤرخ في 18 صفر 1433 الموافق 12 يناير 2012.
11. الأمر رقم 75 – 59 المؤرخ في 20 رمضان 1395الموافق 26-09-1975المتضمن القانون التجاري المعدل والمتمم. بالقانون رقم 15-20 المؤرخ في 18 ربيع لاول 1437الموافق 30-12-2015.ج.ر.ع71.
12. الأمر رقم 03-05 مؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو عام 2003, يتعلق بحقوق المؤلف والحقوق المجاورة.
13. المرسوم الرئاسي رقم 97-341 مؤرخ في 13 سبتمبر 1997 ، يتضمن انضمام الجمهورية الجزائرية الدمقراطية الشعبية، مع التحفظ، إلى اتفاقية برن لحماية المصنفات الأدبية والفنية المؤرخة في 9 سبتمبر 1886 والمتممة بباريس في 4 مايو 1896والمعدلة ببرلين في 13 نوفمبر 1908 والمتممة ببرلين في 20 مارس 1914والمعدلة بروما في 2يونيو 1928 وبروكسل في 26 يونيو 1948 وستوكهولم في 14 يوليو 1967 وباريس في 24 يوليو 1967 والمعدلة في 28 سبتمبر 1979 ، المنشور بالجريدة الرسمية الجزائرية، والصادر في العدد رقم61 .
14. المرسوم تنفيذي رقم 98 – 257 المؤرخ في 03 جمادي الأول الموافق 25 أوت 1998 الذي يضبط شروط وكيفيات إقامة خدمات "انترنات" واستغلالها.(الجريدة الرسمية عدد 63 بتاريخ 26 أوت 1998) .
15. المرسوم تنفيذي رقم 09 – 410 المؤرخ في 10 ديسمبر 2009 الذي يحدد قواعد الأمن المطبقة على النشاطات المتصلة بالتجهيزات الحساسة.
16. المرسوم التنفيذي رقم 01 – 123 المؤرخ في 09 ماي 2001 المعدل والمتمم، يعطي صلاحيات لسلطة ضبط البريد والمواصلات السلكية اللاسلكية بمنح الرخصة المتعلقة بإنشاء واستغلال خدمات التصديق الإلكتروني مرفقا بدفتر الشروط .
17. المرسوم التنفيذي رقم 07 – 162 المؤرخ في 30 ماي 2007المعدل والمتمم للمرسوم التنفيذي رقم 01- 123 المؤرخ في 09 ماي 2001، المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات، بما فيها اللاسلكية الكهربائية

وعلى مختلف خدمات المواصلات السلكية و واللاسلكية، أخضع خدمات التصديق الإلكتروني لنظام الرخصة ج.ر.ع.37 بتاريخ 07 جوان 2007).

18. المرسوم التنفيذي رقم 98-257 بتاريخ 25 أوت 1998،ج.ر.ع، 63 – 1998، والمعدل بمرسوم التنفيذي آخر يحمل رقم 307-2000 بتاريخ 14 أوكتوبر 2000، ج.ر.ع، 60 - 2000، الذي يحدد شروط وكيفيات وضع واستغلال خدمة الإنترنت.
19. المرسوم التنفيذي رقم 05-356 المؤرخ في 17 شعبان 1426،الموافق 21 سبتمبر 2005،يتضمن القانون الأساسي للديوان الوطني لحقوق المؤلف والحقوق المجاورة.

ثالثا : القوانين الدولية المستأنس بها :

1. القانون التونسي رقم 83 لسنة 2000 الصادر في أغسطس سنة 2000 في شأن المبادلات والتجارة الالكترونية .
2. قانون الجرائم الواقعة على نظم المعالجة الآلية للمعطيات الصادرة بتنفيذه الظهير رقم 197-03-01- بتاريخ 11نوفمبر 2003،ج رسمية5171.
3. القرار الوزاري السعودي رقم 79 المؤرخ في 1428/03/07ه،المتضمن الموافقة على نظام مكافحة جرائم المعلوماتية
4. مرسوم رقم 165-09-2 بتاريخ 21 ماي 2009 الموافق 25 من جمادى الأولى 1430 لتطبيق القانون رقم 09-08 المتعلق بحماية الأشخاص الذاتيين، تجاه معالجة المعطيات ذات الطابع الشخصي.
5. ظهير رقم 1.00.20 صادر في 9 ذي القعدة 1420 (15 فبراير 2000) بتنفيذ القانون رقم 2.00 المتعلق بحقوق المؤلف والحقوق المجاورة.

6. السويد قانون حماية المعطيات رقم 289 تاريخ 1973/5/11 المعدل في الأعوام 1979 و 1982 و 1986 و1990 و 1992،قانون البيانات الشخصية لعام 1998 حل محل القانون المشار اليه .

7. الولايات المتحدة الأمريكيةU S Aعلى المستوى الفيدرالي:

- قانون الخصوصية لعام 1974 وقانون خصوصية الاتصالات الالكترونية لسنة 1986 و قانون حماية خصوصية المستهلك لعام 1997 .
- قانون حماية خصوصية الضمان الاجتماعي على الخط لعام 1997 .
- قانون خصوصية الاتصالات لعام 1997 .
- قانون خصوصية المعطيات لعام 1997 .
- قانون حماية المعطيات تاريخ 1977/1/27 عدل جذريا بتاريخ 1990/12/20 كما جرى تعديله العام 1994 The data privacy act of 1997.
- مشروع قانون حماية البيانات عام 2000 المتوافق مع القانون الأوروبي لعام1995.

8. النمسا Austria

- القانون الفدرالي لحماية المعطيات 1978/10/18.
- قانون حماية البيانات لعام 2000..

9. الدانمارك

- قانون التسجيل الخاص رقم 293 تاريخ 1978/6/8 المعدل في 1988/4/1 .
- قانون تسجيل السلطات العامة 1978/6/8 المعدل ايضا بتاريخ 1988/4/1 .
- قانون معالجة البيانات الشخصية لعام 2000.

10.فرنسا:

1. *La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, plus connue sous le nom de loi informatique et libertés*

2. *La loi Godfrain du 5 janvier 1988, ou Loi no 88-19 du 5 janvier 1988 relative à la fraude informatique.*

المعاهدات:

1. معاهدة حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية ستراسبورغ، 28 يناير1981 .
2. تعديلات حول معاهدة حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية 15جوان 1999 .
3. بروتوكول إضافي حول معاهدة حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية 8نوفمبر 2001.
4. معاهدة حول جريمة الفضاء المعلوماتي بودابست23 نوفمبر2001.
5. إعلان بوخارست حول مكافحة التزوير والقرصنة 12 جويلية 2006.
6. اتفاقية الإجرام السيبيري و متوفرة على الموقع الالكتروني الخاص بالمجلس الاروبي . *http://www.conventions.coe.int*
7. توصية المجلس الأوربي رقم 13(R95) الصادرة في 1999/09/11م بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات.
8. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في 2010.

الملتقيات العلمية :

1. (دورثي إي)، قراصنة الكمبيوتر، ورقة عمل من إعداد مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر بواشنطن بالولايات المتحدة الأمريكية، 1998، ص8.
2. أخام بن عودة زواوي مليكة، تحديات ظاهرة الجريمة العابرة للأوطان و الثورة المعلوماتية، المؤتمر المغاربي الأول حول المعلوماتية و القانون، أكاديمية الدراسات العليا،ليبيا،30/27 أكتوبر 2009 .

3. إسماعيل عبد النبي شاهين، امن المعلومات في الانترنت بين الشريعة و القانون، مؤتمر القانون و الكمبيوتر و الإنترنت، المجلد الثالث، ص976.
4. إيهاب ماهر السنباطي، الجرائم الإلكترونية، قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد، مداخلة في الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر،16-20 يونيو 2007 بالمملكة المغربية، ص24.
5. الرزو حسن مظفر، القانون العراقي والمفاهيم المعلوماتية لجرائم الفضاء الافتراضي بالحاسوب، مؤتمر القانون العراقي وتطور المجتمع، كلية الحدباء الجامعة، 24-2001/3/25، الموصل، جمهورية العراق. راجع: *http://www.alukah.net*
6. زيد مراد، عصرنة نظام الدفع في البنوك و إشكالية اعتماد التجارة الالكترونية في الجزائر، الملتقى العلمي الدولي الرابع حول، عصرنة نظام الدفع في البنوك الجزائرية و إشكالية اعتماد التجارة الالكترونية في الجزائر، عرض تجارب دولية،يومي28-29 أفريل - 2011 .
7. شهاب بن أحمد الجابري، الإطار العام لقانون المعاملات الإلكترونية 2008/69م ،ندوة قانون المعاملات الإلكترونية الأولى،2008.
8. غزال عادل، الحكومة الإلكترونية في الجزائر والنفاذ إلى مجتمع المعلومات. الملتقى الوطني الثامن حول، مستقبل ثقافة المعلومات والاتصال لدى الشباب في الجزائر، بين صناعة المجتمع الجماهيري ومجتمع المعرفة والمعلومات من تنظيم جمعية الروافد الثقافية بالتعاون مع قسم علم المكتبات والتوثيق، بجامعة باتنة يومي 09/08-نوفمبر-2014. على الرابط التالي: ***https://adelghezzal.wordpress.com/2014/12/18***
9. فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا بليبيا في أكتوبر 2009 ،جامعة زيان عاشور بالجلفة كلية الحقوق والعلوم السياسية، ص 29.
10. ماجد عثمان، حماية البيانات المتداولة عبر الشبكات، المؤتمر الدولي الأول حول حماية أمن المعلومات في قانون الإنترنت،2008.

11. مفتاح بوبكر المطردي، الجريمة الالكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان ،المنعقد في 23-25 / 9 / 2012 .

12. هدى حامد قشقوش، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنيت للفترة من 1-3/ماي/2000،جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، ط3، المجلد الثالث، 2004م، ص6.

13. وليد العاكوم، مفهوم ظاهرة الإجرام المعلوماتي، مؤتمر القانون و الكمبيوتر و الإنترنت، المجلد الأول، ص 968.

14. يونس عرب، التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية، ورقة عمل مقدمة أمام، الدورة العلمية الخامسة حول دور التوثيق والمعلومات في بناء المجتمع العربي، النادي العربي للمعلومات، سوريا. راجع:***www.arablaw.org***

يونس عرب،نماذج من التشريعات المختلفة في مجال مكافحة الجرائم الالكترونية،هيئة تنظيم الاتصالات مسقط، سلطنة عمان ورشة عمل، تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، 2-4 ابريل 2006. راجع:***www.arablaw.org***

المجلات العلمية:

1. أنطون زحلان، الطبيعة الشاملة للتحدي التقاني، مجلة المستقبل العربي،العدد263، بيروت،2001/1.
2. باسل يوسف، الاعتراف القانوني بالسندات والتواقيع الالكترونية في التشريعات المقارنة، مجلة دراسات قانونية صادرة عن بيت الحكمة، العدد الثاني ،بغداد،2001.ص23 .
3. حسن بن أحمد الشهري، الأنظمة الالكترونية الرقمية المطورة لحفظ و حماية سرية المعلومات من التجسس، المجلة العربية للدراسات الأمنية و التدريب ، جامعة نايف العربية للعلوم الأمنية ، المجلد 28، العدد 56،الرياض، ص48.
4. صالح بن محمد المسند، عبد الرحمان بن راشد المهيني، جرائم الحاسب الآلي، الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية و التدريب، أكاديمية نايف العربية ،العدد 29 ،الرياض، 2000، ص 151.

5. طارق كميل، مقدمو خدمات المصادقة الالكترونية، التنظيم القانوني واجباتهم ومسؤولياتهم، مجلة جامعة الشارقة للعلوم الشرعية و القانونية، المجلد 5،العدد3،أكتوبر2008، ص253
6. طربيه جوزيف، الصيرفة الإلكترونية، تطبيق التكنولوجيا للصمود والنجاح في الاقتصاد الجديد، إتحاد المصارف العربية، العدد 244، المجلد 21، أبريل 2001، ص17.
7. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، العدد 24 ،1992، ص119-120.
8. محمد إبراهيم محمد الشافعي، النقود الإلكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س 12، ع1، يناير، 2004، ص142–148.
9. محمود ابقران، الانترنيت، دراسة اتصالية ومصطلحية، مجلة المعلومات العلمية والتقنية، العدد 01 ، ج9،الجزائر، 1999. ص21.
10. هشام سليمان، تكنولوجيا المعلومات والاتصال، مجلة علوم وتكنولوجيا، العدد2، سنة 2001. ص 25 .

الجرائد العلمية :

1. عبد المجيد ميلاد، نشر الطمأنينة وبناء الثقة في العصر الرقمي، استراتيجية أمن المعلومات، جريدة الصباح، 2006.
2. يحيى اليحياوي، الإرهاب والحروب الإعلامية الأولى، جريدة العلم،2002.

- ***Les ouvrages en français*** :

1. *A. Vitalis, Informatique, pouvoir et liberté,Economica,1988.*

2. Bernard Foray, La fonction RSSI (Responsable Sécurité Système d'Information) - Guide des pratiques et retours d'expérience - 2e édition, Dunod, 2011.

3. Emmanuel.Bresson,cryptographie,Laboratoire,decryptographie,SGDN/DCSSI-

4. Gérard Naulleau, Michel Rouach, Contrôle de gestion et stratégie dans la banque, Banque éditeur,2éme édition, Paris, 1994.

5. Ghislaine ,Labouret, Introduction à la cryptographie, Hervé Schauer Consultants (HSC).1999-2001.

1. Isabelle Mouton ,La Société numérique en question, Sciences Humaines, Seuil, Éditions, 2011.

6. Jean Guisenel, Guerres dans le cyberspace, services secrets et Internet, paris, la découverte,1995.

7. Laurent Bloch et Christophe Wolfhugel, Sécurité informatique - Principes et méthode, Eyrolles, 3e édition ,2011.

8. Michel Vivant, Informatique et propriété intelectuelle. A-propos des biens informatique, Édition générale ,doctrine,1984, no 3169.

9. Mostafa khiyati, Cybercriminalité et enfance en Algerie, edition FOREM 2007.

1. P.Catala, La propriété de l'information, et masse, la délinquance informatique aspects de droit pénal international.

10. R. Vouin et J.Léauté, Droit pénal et procédure pénale,2 meéd, Paris.

11. Renaud Dumont, Cryptographie et Sécurité informatique,Université de Liège, Faculté des Sciences Appliquées, 2010.

12. S.Proulx, L`informatisation, mutation technique, changement de société, Sociologie et société1984.

13. W.Dominique, Internet et après? une théorie critique des nouveaux medias, France, Flammarion, 1999.

14. Y.Padova, Un aperçu de la lutte contre la cybercriminalité en France, R.S.C. 2002.

❖ *Les ouvrages en anglais :*

1. Alan Calder, A Business Guide to Information Security, KOGAN,2005.

2. Alan Story, Intellectual Property and Computer Software, Lecturer in Intellectual Property Law, University of Kent, United Kingdom, Published by International Centre for Trade and Sustainable Development (ICTSD), International Environment House.

3. Anderson, J.M, Why we need a new definition of information securit, Computers-Security, 2003.

4. Anne Fitzgerald, E-crim proposed legistation, Computer and Telecommunications Law Review, Austrasia , 2001.

5. B.Dermott, Geer, D'Information security is information risk management, In Proceedings of the 2001 Workshop on New Security Paradigms NSPW .

6. Bensalem Abderezak, Investigating Judge at the Tribunal of Sidi M'Hamed, THE Algerian legal system to fight against cyber criminality.

7. Bruce sterling, The hacker Crackdown law and Disorder on the Electronic fron,tier,1994.

8. Cedric Laurant, Privacy, Human-Rights,Electronic Privacy Information Center، USA، 2003.

9. D.Marcus, Odom, Anand Kumar and Laura Saunders, "Web Assurance-Seals, How and Why they Influence Consumers Consumers, Decisions, Journal of Information Systems,Vol.16 No. 2, Fall 2002.

10. David Bainbridge, Introduction to computer law, third edition, Pit Man publishing 1996 .

11. E.M milner, managing information and knowledge in the public sector routledge, london, 2000.

12. Emmanuel C.L.Margaret N, The information age, Malaysia :UNDP-APDIP, 2003.

13. Forouzan, Behrouz A, Introduction to cryptography and network security,2008.

14. Franziska Boehm, information sharingand data protection in the area of freedom ,security and justice, towards harmonised data

protection principles for information exchange at Eu–level, Springer, Verlag, berlin ,Heidelberg,2012.

15. Fritze Grupe, Stephen G.Kerr, William Kuechler and Nilesh Patel, Understanding Digital Signatures, The CPA Journal, June 2003.

16. G.Mathieu, cyber terrorisme, Hype or reality? Computer fraud- security, February 2007.

17. Henri Kloetzer, Introduction à l'économie numérique, Lavoisier, management et information, collection dirigée par nicolas manson,2012 .

18. Jan Kosko, Computer Securit , Protection Is The Name of The Game, NIST Research Report, 1989.

19. John Dvorak, The Software Piracy Bluff, PC Magazine, May 12, 1992.

20. John K.Halvey and Barbara M.Melby, Information Technology Outsourcing Transaction,2nd edition.

21. John Wiley & Sons, Handbook of information security",volume.2,2006.

22. Joseph S.N Owens, W.A, America's Information Edge, Foreign Affairs, 1996.

23. Kenneth C.Laudon and Jane P.Laudon, Management Information Systems, Printice Hall International, Inc, sixth edition 2000.

24. Lyn Robinson, Installing a Local Area Network ,London, Aslib, 1995.

25. M.Conley Jonhn, M.Bryan Robert, A survey of computer crime legislation in United States, I.C.T.L , Vol .8.1, 1999.

26. Mann David, Sutton, Mike, Net crime, Brit.J. criminal, Vol.,38,No. 2, Spring 1998.

27. MarkS.Merkow, James-Breithaupt, TheE-Privacy Imperative, Protect Your Customers, Internet Privacy and Ensure Your Company's Survival in the Electronic.

28. Merwe vander, computer crimes and other crimes against information technology in south Africa .R.I.D.

29. Nancy F. DuC harme Robert F. Kemp, Copyright Protection for Computer Software in Great Britain and the United States, A Comparative Analysis, Santa Clara High Technology Law Journal , Volume 3.

30. P. Goldstein, Copyright, Principles, Law and Practice, Little Brown and Co, Boston, Toronto, London, 1989,vol I.
31. P.Rose, Commercial bank Management, Texas A&m university (Irwin Mc raw-Hill),1994.
32. Paul Taylor, How Ethical Hackers Pinpoint Security Weakness, Financial Times, September 3rd1997 .
33. S - Mcquade, Understandingand Managing Cyber Crime ,Boston, Allyn & Bacon, 2006.
34. Thomas M., The Growing Threat Of Computer Crime, DETCTIVE -US Army, Summer 1990
35. Tony Capaccio, Warfare in The Information Age,Popular Science, July 1996.
36. Ulrich sieber, Legal Aspects of Computer, Related Crime in the Information Society, Com crime Study,1998.
37. Vacca John,Internet Security secrets USA, Book World wide inc1996.
38. Volio، Fernando، Legal personality، privacy and the family in Henkin.
39. Walden, update on the computer misuse act 1990, Journal of Business Law,1994.
40. Warwick Ford ,Computer communications security,1994
41. Yaman Akdaniz, Clive Walker and David Wall (eds.),The internet, Law and Society, Longman Pearson Education, 2000.
42. Zeviar-Geese, G.The State of the Law on Cyberjurisdiction and Cybercrime on the Internet, California Pacific School of Law, Gonzaga Journal of International Law. Volume 1. 1997-1998.

ARTICLES:

1. A.Lucas, Les programmes d'ordinateurs comme objets de droits intellectuelles, JCP ,1982,1,Doct,3081.
2. Alain BENSOUSSAN, Internet, aspects juridiques, éd. Hermes, 1998, p. 198.
3. C. Meunier, La loi du 28 nov,2000 relative a la criminalité informatique. Rev.dr. pen. Crim. 2002, p.611.
4. Chris Reed & colleague, Computer Law, fifth edition, Oxford University Press, New York, 2003.

5. Francesco Miani, le cadre réglementaire des traitements de données personnelles, effectues au sein de l'union européenne, revue trimestrielle de droit européen,Dalloz,n2, 2000, p283.

6. Frédéric Bongat, Sécurité des Systèmes d'Informations, la cryptographie appliquée, GNU, Documentation License,2008-2009.

7. Fritze Grupe, Stephen G. Kerr, William Kuechler and Nilesh Patel, Understanding Digital Signatures, The CPA Journal, June 2003.

8. J. Francillon, Les crimes informatiques ET dautres crimes dans le domaine de la technologie informatique en France, Rev intpen, 1990, vol 64. p293.

9. J.Huet, La modification du droit sous l'influence de l informatique, aspect de droit privé,JCP,1983,1,Doct,3095 .

10. Jean Pradel, Les infractions relatives à l'informatique, Revue internationale de droit comparé Année 1990 Volume 42 Numéro 2, pp. 815-828 .

11. Kevin Freoa, La sécurité informatique dans l entreprise, projet professionnel, Dess droit et pratique du commerce électronique, université paris, René descarte,2004 .

12. M.Ali makouar, droit et informatique, rapport de synthèses, revue marocaine de droit et d économie de développement-n 11.1986, p186.

13. M.Vivant, Informatique et propriété intellectuelle ,JCP,1984,1 Doct,3081.

14. Martin WASIK, Computer Crimes and Other Crimes against Information Technology in the United Kingdom, Rev. int. dr. pén. 1993, P 554.

15. Rapport S.Nora et A.Minc, L`informatisation de la société, Point Seuil , 1978,P 11

Les colloques :

1. *Mahmoud saleh addle, Electronic Crime, The ITU / BDT Arab Regional Workshop on,Developing the Legislative Aspects for Combating Electronic Crime, Muscat 2nd- 4th April 2006.*

2. *nesrin saadoun, The Conference of Digital Information Technology, Modren Trends in The Information Technology, Amman - Jordan 9 - 11 October 2012.*
3. *The Conference of Digital Information Technology,Modren Trends in The Information Technology,Amman - Jordan 13-15 May 2014 .*
4. *S. Ghernauti-Heli: "From the Digital Divide to the lack of digital security: the challenges of developing and deploying a unified computer-security framework in a multi-dimensional context" in international cooperation and the information society, Section Swiss policy-making manual, publications University Institute for Development Studies (IUED) . Geneva, 21 November 2003*

- ***WEBOGRAPHIE:***

1. باشيوة سالم، الرقمنة في المكتبات الجامعية الجزائرية ،دراسة حالة المكتبة الجامعية المركزية ،بن يوسف بن خدة، مجلة ***Cybrarian Journal*** الالكترونية، ع2، ديسمبر 2009 متاح على الموقع التالى : ***www.journal.cybrarians.info***
2. بلعربي عبد القادر، لعرج مجاهد نسيمة، مغبر فاطمة الزهراء. تحديات التحول إلى الحكومة الإلكترونية في الجزائر، متاح على الخط المباشر: ***www.iefpedia.com***
3. التحديات القانونية للتجارة الإلكترونية على الموقع الإلكتروني الأتي: ***www.opendirectorysite.info***
4. الجزائر الإلكترونية، مقال إلكتروني متوفر على موقع ***www.mptic.dz***
5. جلال المندلاوي. ماذا يدور خلف السور العظيم. مجلة خالد العسكرية، تقارير ***www.islamonlin.net/***2004،
6. حرب المعلومات ومستقبل التجسس: قراءات استراتيجية. مركز الدراسات السياسية والاستراتيجية.ورد في ***www.ahram.org.eg/acpss/*** .

7. حسن مظفر الرزّو،الأطر المستقبلية لإعداد ملاكات الأمن المعلوماتي 6 /2009/4: www.alukah.net

8. سيف بن سعود المحروقي، الأمن المعلوماتي ضرورة وليس ترفا الاثنين،12 ربيع الثاني 1436هـ. 2 فبراير 2015م:www.omandaily.Com

9. الشبكة القانونية العربية، فرع القانون، جرائم الكمبيوتر والأنترنت، منشور على الرابط التالي : arab@wnet –lawsubjects-26/05/2015

10. عامر قنديلجي، علاء الدين الجنابي، نظام المعلومات المحوسب، المنشاوي للدراسات و البحوث، المقال متوفر على الموقع التالي : www.minshawi.com

11. عبد الرحمن رمزي عداس مدير مخاطر الائتمان بالبنك الأهلي التجاري، إدارة مخاطر الائتمان عن جريدة الوطن،ع728،الموافق لـ27سبتمبر 2002. www.alwatan.com.

12. عبد المجيد ميلاد، تشفير البيانات والتوقيع الإلكتروني على الموقع الأتي:www.arabcin.net

13. عبدالله بن عبدالعزيز الدهلاوي، أمن المعلومات في الحاسبات الآليه، مجلة الدفاع، العدد 93 , 1994م.لمزيد من التفاصيل انظر(موقع هيئة الاتصالات وتقنية المعلومات). www.citc.gov.sa.

14. علي بن ضبيان الرشيدي، مقال منشور على الرابط التالي :www.kkmaq.gov.sa

15. فايز عبدالله الشهري, الانترنت وتحديات الأمن القومي www.kkmaq.gov.sa .

16. قناة العربية: www.skynewsarabia.com

17. لجنة تنظيم أمن المعلومات ISR في دبي بالإمارات العربية المتحدة، و"سياسة تأمين المعلومات.www.alarabiya.net/ar/technology/2014/05/18

18. محمد بن عبدالله المنشاوي: المخاطر الأمنية للإنترنت ، بحث منشور على شبكة الإنترنت من خلال موقع الدراسات والبحوث: www.minshawi.com.

19. محمد عادل ريان، جرائم الحاسب الآلي و أمن البيانات: www.anaharonline.com

20. محمد عبدالله الخراشي، أهم التحديات التي تواجه الأمن القومي ***www.kkmaq.gov.sa***

21. محمد مكاوي، الادارة الافتراضية... مستقبل ام خيال ،قراءة لمستقبل مشروع الحكومة الاليكترونية، متوفر على الرابط التالي : ***alyaseer.net/vb/showthread.php?t=14328***

22. المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، ملتقى أمن المعلومات،الاجتماع الثاني لرؤساء الإدارات المختصة بتقنية المعلومات بالنيابات العامة العربية2012/03/7-5، بيروت، الجمهورية اللبنانية متوفر على الرابط التالي:***www.shatharat.net/vb/showthread.php?t=12161***

23. مصطفي سرهنك، إنترنت سيكيوريتي سيستمز، الشرق الأوسط، إحدى أبرز الشركات العالمية المتخصصة في مجال أمن المعلومات ***www.iss_sarhank.jpg***.

24. معتصم شفاعمري،حماية الخدمات المصرفية الإلكترونية ، أمن المعلومات – العدد (29)، 2008 مقال منشور على الموقع التالي: ***www.almaalomatia.com***

25. يسري زكي، تبسيط أمن المعلومات والإتصالات، متاح على الرابط:

26. *Allen, Julia H,The CERT Guide to System and Network Security Practices,Boston, MA, Addison-Wesley,2001,ISBN 0-201-73723-X.*

27. *Charlotte-Marie pitrat-Laurent le veneux:Protection du consommateur et des données personnelles. voir le site:* ***www.finance.gouv.fr***.

28. *Eric A. Caprioli, Les moyens juridiques de lutte contre la cybercriminalité,* ***www.caprioli-avocats.com.***

29. *Internet le nouveau supermarche de la drogue,* ***www.melty.fr***

30. *Tierry Leonard,E.Marketing et protection des données à caractère personnel,voir le site:* ***www.droit-technologie.org.***

❖ **المقالات على النت :**

1. *Abdelaziz Derdouri,La Cyber Sécurité,Etat des lieux en Algérie, Cybersécurité décembre 19, 2014.www.ssri.dz/la-cyber-securite-etat-des-lieux-en-algerie/*
2. *Cédras Jean, « Un aspect de la cybercriminalite en droit français : le téléchargement illicite d'œuvres protégées par le droit d'auteur », Revue internationale de droit pénal 3/2006 (Vol. 77)*
3. *Daniel Larkin. Fighting Online Crime. IC3 investigates the growing www.ic3.gov.*
4. *Forgery and Counterfeiting Act,1981, LONDON. www.legislation.gov.uk*
5. *HADDAD Sabine, définition de la cybercriminalité ,Article juridique publié le 04/02/2013,Disponible sur:www.legavox.fr*
6. *Meriem ALI MARINA ,Centre de prévention et de lutte contre la criminalité informatique et la cybercriminalité ,N° 98 – Août2016,Disponible à www.eldjazaircom.dz*
7. أفنان بنت ناصربن محمد العمراني،الأمن المادي ووسائل التحكم بالدخول للدوائر التلفزيونية المغلقة، ورقة السجل، مركز المعلومات، متوفر في:
8. جورج لبكي، المعاهدات الدولية للإنترنت، حقائق وتحدّيات، مجلة الدفاع الوطني اللبناني، العدد 83 ،2013، متوفر على الموقع التالي.www.lebarmy.gov
9. سعيد بشار، المؤسسات الجزائرية غير مؤمّنة ضد القرصنة ،مقال كتب بتاريخ 13أفريل2014 ،متاح على الموقع التالي :www.elkhabar.com
10. سنيم محمد الامين أكاديمي و باحث في العلوم الإستراتيجية، جامعة الجزائر3 متوفر على الموقع التالي: .snimedamine.maktoobblog.
11. شريف درويش اللبان، خبرة عربية منقوصة، أمن المعلومات في ظل تحديات البيئة الرقمية، المركز العربي للبحوث والدراسات، 2015 ،متوفر على الموقع التالي: www.acrseg.org
12. عبدالله بن شائع بيهان. ثقافة أمن المعلومات، كلية المعلمين ،قسم الحاسب، جامعة الملك سعود، مركز التميز لأمن المعلومات ،المقال متوفر على الرابط التالي : aalbaihan@ksu.edu.sa

13. فايزة دسوقي أحمد، بصمة اليد والعين والقياسات الحيوية في أمن المعلومات 15 ذو الحجة - 1431هـ| 21نوفمبر2010، مقال الرابط التالي
www.lahaonline.com/articles/view/37151
14. فتحي شمس الدين، الفجوة الرقمية في دول العالم الثالث ،مجلة الأهرام للكمبيوتر و الانترنت و الاتصالات، لغة العصر، 20-2-2016، مقال منشور على الرابط التالي:
15. aitmag.ahram.org.eg/News/38391.aspx
16. كريم كريمة، تأثير إستعمال التقنيات الحديثة في تحقيق الأمن القانوني مقال منشور على الرابط التالي manifest.univ-ouargla.dz/...national.../KARIM%20Karima.pdf . ص2.
17. مهران زهير المصري، السياسات الأمنية للمواقع الإلكترونية ،مجلة الباحثون العدد40 ،2010، متوفر على الموقع التالي:kenanaonline.com

الفهرس

الفهرس.

الملخص

إن السمة العولمية لشبكات المعلومات وسيادة الفضاء المفتوح، مع غياب المركزية وعدم وجود مرجعية تمسك بزمام أركان السلطة، داخل كيان الفضاء المعلوماتي، جعل المجتمع أكثر عرضة للتهديدات المعلوماتية، التي قد تعصف بكثير من مرتكزاته المعلوماتية الحيوية .

إضافة إلى وجود ثغرات امن معلوماتي، نتيجة لتنامي الخبرات لدى المستخدمين، وتقادم التقنيات الرقمية بسرعة كبيرة، تساهم بتعميق المخاطر المحتملة للمخاطر المعلوماتية .

من جهة أخرى فان التدفق الدائم للبيانات والمعلومات من مصادر مجهولة المورد، بات يحتم على المقيمين في مجتمع المعلومات، تبني معايير أمنية محكمة لضمان عدم تسلل الفيروسات الحاسوبية أو قراصنة المعلومات إلى نظم المعلومات، فيعيثون بها فسادا وتخريبا.

الكلمات المفتاحية :

الأمن السيبراني – تكنولوجيا المعلومات– الفجوة الرقمية- الجريمة الالكترونية– حماية البرمجيات.

Résumé

Le caractère mondialiste des sources, l'étendue de leur espace, l'absence d'une référence précise détenant les rennes du monde de l'information, ont rendu la société vulnérable, à la merci des menaces ébranlant ses fondements et son espace vitale. L'existence des failles sécuritaires, amplifiée par le développement de l'expertise des usagers, l'amplification de la technologie de l'information et aussi par absolutisme des techniques numériques de façon général constituent les véritables menaces. Enfin, le flux permanant des sources inconnue simplique aux experts en la matière de prendre des measures nécessaires au filtrage de l'information pour que celle-ci ne soit pas source de corruption.

Mots clés:

Cybersécurité - Technologies de l'information - La fracture numérique - cybercriminalité - la protection des logiciels.

Summary:

The global character of the sources, the extent of their space, the lack of a precise reference holding the reins of the world of information, have made the company vulnerable, thank you to the threats undermining its foundations and its vital space. The existence of security vulnerabilities, amplified by the development of the expertise of users, the amplification of the information technology and also digital absolutism of general technical way are the real threats. Finally, the flow of permanant unknown sources simplique the experts to take the necessary Measures for the filtering of information that the latter is not a source of corruption.

Keywords:

Cyber Security - Information Technology - The digital divide - cybercrime - protection software.