الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة أبي بكر بلقايد–تلمسان–

كلية الحقوق والعلوم السياسية

الحماية الجنائية للمعلومات على شبكة الأنترنت

مذكرة لنيل شهادة ماجستير في القانون العام

من إعداد:

- رصاع فتيحة

تحت تأطير الأستاذ الدكتور:

قلفاط شكري

أعضاء لجنة المناقشة:

أ. د.بوعزة ديدن	أستاذ التعليم العالي	جامعة تلمسان	رئيسا
أ. د.قلفاط شكري	أستاذ التعليم العالي	جامعة تلمسان	مشرفا ومناقشا
د. مامون عبد الكريم	أستاذ التعليم العالي	جامعة تلمسان	مناقشا

السنة الجامعية: **2011 –2012**

بسم الله الرحمن الرحيم

قال الله تعالى:

﴿رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَعَلَى وَالِدَيَّ وَأَنْ أَعْمَلَ صَالِحاً تَرْضَاهُ وَأَدْخِلْنِي بِرَحْمَتِكَ فِي عِبَادِكَ الصَّالِحِينَ﴾

الآية 19 سورة النمل

كـلـمـة شـكـر

قال الرسول صلى الله عليه و سلم:« إذا ساعدكم احد فكافئوه فان لم تجدوا بما تكافؤه فأثنوا عليه»

صدق رسول الله عليه أفضل الصلاة والسلام

أولا وقبل كل شيء نشكر الله عز وجل على انه هدانا بالقوة لإتمام هذا العمل المتواضع.

أحيطكم بالذكر انتم أساتذتي الكرام سفراء العلم سراج الظلام لأنكم كنتم و مازلتم مرجعنا و سندانا لأنكم أخذتم بأيدينا و كنتم مصفاد أفكارنا التي لولاكم لم تجسد هذا و ما كان هذا العمل ليكون .

نتفضل بفائق التقدير و الاحترام و جزيل الشكر إلي الاستاذ الدكتور المؤطر قلفاط شكري الذي وضع ثقته فينا و اتمم معنا هذا العمل المتواضع ..

أتقدم بكل الشكر إلى الأستاذين ديدن بوعزة ومامون عبد الكريم اللذان قاموا بكل المجهودات لتلاوة ونقد هذه المذكرة

كما لا يفوتني أن أتوجه بالتحية والشكر إلى كافة أساتذة كلية الحقوق و العلوم السياسية لجامعة تلمسان

إ هـد ا ء

أتقدم بخالص الشكرإلى:

سر الوجود ومنبع الحياة..... أمي. ..... رحمها الله وأدخلها فسيح جنانه

إلى فرحتي في الحزن وقوتي في الضعف .... أبي ..... بارك الله في حياته

إلى اخت رعتني صغيرة وصاحبتني كبيرة...عتوية....جـــزاها الله خيرا

الى زوج اختي وأبي .....عادل محمد نجيب.....حفظه الله

إلى إخوة رأوا في نجاحي نجاحاً لهم:

أنار الله دربهم

إلى شموع تشتعل لتنير الطريق أمام الأجيال... إلى الأساتذة الكرام

ما تبقى للنبوة من وريث

إلى كل راج الخير لهذه الأمّة

رصاع فتيحة

قـــائـــمـــة الـــمـــخـــتـــصـــرات

1- ج.ر.ج.ج.د.ش: الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية
2- ق.ع.ف: قانون العقوبات الفرنسي
3- ق.ع.ج: قانون العقوبات الجزائري
4- ق.ع.م: قانون العقوبات المصري
5- ق.م.ج: القانون المدني الجزائري
6- ق.م.ف: القانون المدني الفرنسي
7- م.ق.ج: المجلة القضائية الجزائرية
8- ج.م: الجريمة المعلوماتية
9- م.م: المجرم المعلوماتي

باللغة الأجنبية

1- O.C.D.E : L'Organisation de Coopération et de Développement écnomique
2- O.E.C.D : Organisation for Economic Co-operation and Development
3- D.A.R.P.A : Defense Advanced Research Project Agenecy
4- W.W.W. : World wide wele « le réseau d'information internationales »
5- C.C : Computer Crime : le crime par l'ordinateur la criminalité
6- T.C.P/I.P : Protocole de Transmission et de Contrôle.
7- F.T.P : File Transfer Protocol
8- op.cit : Opposition Citée

المقدمة

تعد شبكة الانترنت أحد تقنيات المعلوماتية والاتصالات في العصر الحالي، لما لها من دور كبير في نشر المعلومات بين البشر في كافة أنحاء العالم.

ومن خلال هذه الشبكة بدأ العالم بأسره يندمج مع بعضه البعض يشاهد ويتحاور، وتدريجيا بدأ يتحرر من قيود المكان إلى أن أصبح العالم قرية صغيرة وهذا الفضل يرجع لشبكة الانترنت.

وبالتالي يمكننا القول بأن عصر الجغرافيا بدأ يتضاءل لصالح عصر بلا حدود، تتلاشى فيه سيادات الدول، وتسود فيه اختراعات الأقمار الصناعية والفاكس والحاسبات الآلية.

وظهرت الشبكات العملاقة التي تعمل في مجال صناعة الشبكات، وأصبح هناك تنافس شديد بين هذه الشركات، وقد ساهمت هذه الشبكة في تطوير الفكر والثقافة وإحداث التقارب بين شعوب العالم. وبالتالي لا يمكننا نكران الفوائد التي عادت على العالم من وراء هذه الشبكة.

أي هناك فوائد ايجابية، ولكن هذا كان في الأول نظرا لمحدودية استخدام شبكة الانترنت حيث كانت قاصرة على أغراض البحث العلمي فقط علاوة على كونها مقصورة على فئة معينة من المستخدمين وهم الباحثين والعلماء وطلبة الجامعات.

لكن مع مرور الزمن ظهر الجانب السلبي للشبكة وذلك مع بزوغ فجر الثورة المعلوماتية La Révolution Informatique، وتوسع استخدام شبكة الانترنت وبدأ استخدامها في المعلومات التجارية ودخول جميع فئات المجتمع إلى قائمة المستخدمين، فبدأت تظهر أنماط إجرامية مستحدثة على هذه الشبكة.

مشكلة البحث:

ولقد أثارت هذه الأنماط الإجرامية المستحدثة على شبكة الانترنت عدة مشاكل نظرا لأنه من الصعب السيطرة على هذه الشبكة، وعلى الجرائم التي ترتكب عبرها، هذا من جهة، ومن جهة أخرى من الصعب اكتشاف هذه الجرائم أو تحديد مصدرها، لأن الجاني يستخدم اسما مستعارا أو غير حقيقي.

ومن الصعب أيضا إيقاف ارتكاب الجريمة عبر الشبكة بسبب سرعة نشر المعلومات وتسجيلها على الحاسبات الخادمة في الخارج مما يجعلها تجوب العالم في لحظات.

وذكرنا بأن هذه الجرائم ترتكب عن طريق أنماط إجرامية مستحدثة، وتتمثل هذه الأنماط الإجرامية في الفيروسات و سرقة الأسرار السياسية و التجارية وهذا يدفعنا إلى التساؤلات التالية:

- هل هذه الانماط الاجرامية المستحدثة تختلف عن انماط الجريمة التقليدية؟
- وهل للمجرم المعلوماتي خصائص تميزه عن باقي المجرمين التقليديين؟
- وعلى اي اساس تحظى المعلومة بالحماية الجنائية؟سواء على المستوى الدولي او على المستوى الاقليمي العربي؟
- هل يستلزم فى المعلومة توفر شروط معينة حتى تحظى بالحماية الجنائية؟
- هل نصوص قانون العقوبات السارية كافية لمواجهة هذه الأفعال الإجرامية وهل توفر الحماية القانونية لها؟
- أم يجب استحداث نصوصا جديدة نظرا لارتكاب هذه الجرائم بأساليب وأدوات تقنية جديدة؟

- وحداثة شبكة الانترنت وتدويل شبكات الاتصالات قد خلقت فراغا تشريعيا، فكيف سيواجه الفقه والقضاء هذه المشكلة؟ علما بأن نصوص القانون تعجز أمام هذه الظاهرة الإجرامية المستحدثة على شبكة الانترنت.

هذا ما سوف نراه في بحثنا الآتي.

أهمية البحث:

ترجع أهمية هذا البحث إلى أنه من الموضوعات الحديثة المرتبطة بتطور وسائل الاتصالات الحديثة.

وإن اختيار الحماية الجنائية للمعلومات على شبكة الانترنت لما تمثله المعلومات من قيمة اقتصادية لا تقل بأي حال من الأحوال عن قيمة الأشياء المادية، ويتعين وضع نظام ملائم لحمايتها من الناحية الجنائية. ومما زاد من أهمية هذا البحث هو ظهور أنماط إجرامية مستحدثة بشأن الاعتداء على المعلومات على شبكة الانترنت. مما جعل الفقه والقضاء المقارن يحاول التصدي لهذه الظاهرة وهذا ما سوف نعالجه في موضوعنا وذلك ببيان مفهوم الجريمة المعلوماتية، وأنواعها، والجهود المبذولة لمكافحتها، وذلك بمحاولة لسد الفراغ التشريعي في القوانين القائمة.

أهداف البحث:

إن الهدف من هذه الدراسة يتمثل في الأتي:

- التعرف على كيفية إسباغ الحماية الجنائية على شبكة الانترنت وتحديد المقصود بالجرائم المعلوماتية والمجرم المعلوماتي.
- بيان مدى صلاحية النصوص التقليدية في التعامل مع جرائم المعلومات المستحدثة.

منهج البحث:

سوف نتبع في دراسة هذا الموضوع منهجا تأصيليا وتحليليا ومقارنا. فهو أولا منهج تأصيلي يرد النقاط التفصيلية إلى أصولها النظرية، فعندما نعالج جريمة من جرائم الكمبيوتر نردها إلى الأركان العامة في التجريم.

وعندما نحلل نشرح كل جريمة على حدى ، وسنتخذ منهجا مقارنا للمقارنة بين تشريعات الدول.

وهذا بالتعرض الى واقع الانترنت والجريمة المستحدثة كفصل أول، وبعد ذلك نتناول أشكال الاعتداءات على المعلومات و الحماية الموفرة لها كفصل ثاني.

الفصل الأول

واقع الانترنت والجريمة المستحدثة

المعلومة من اغلى الاشياء في الوجود ومن يملك المعلومة فقد امتلك القوة وزادت قوة المعلومة باقترانها بوسائل الاتصال من بينها الانترنت وكما جاءت هذه الاخيرة بايجابيات خدمت المجتمع أفرزت قي نفس الوقت سلبيات أساءت للمجتمع وخلقت مايسمى بالجريمة المعلوماتية و المجرم المعلوماتي. وهذا ماسوف نتعرض له في هذا الفصل.

المبحث الأول: الانترنت

أصبح استخدام تكنولوجيا المعلومات في الحصول على المعلومات ونقلها من أهم الركائز التي تمكننا من مواكبة التطور والتقدم في كافة المجالات، إضافة إلى أثر ذلك في توفير الوقت والجهد والمال، وذلك بفضل تطور مفهوم واستعمالات تكنولوجيا المعلومات والانترنت. وبفضل هذه الأخيرة أصبح العالم يشبه القرية الكونية الصغيرة.

المطلب الأول: ماهية الانترنت وتطورها

إن تطور مصادر المعلومات كمًا ونوعاً، وكذلك الموضوعات المتشعبة والمتداخلة التي تعكسها مثل تلك المعلومات، قد فرضت علينا اللجوء إلى تكنولوجيا المعلومات المعاصرة. كنتيجة حتمية لتأمين السيطرة على المعلومات وتهيئتها للباحثين والمستفيدين الآخرين، بالسرعة والشمولية والدقة التي يتطلبها منطق العصر، ومن أية بقعة جغرافية في هذا العالم، الذي أصبح يتمثل بقرية صغيرة ينظر إليها الإنسان من خلال شاشة صغيرة، هي شاشة الحاسوب، ومن هذا المنطلق يمكننا النظر إلى الانترنت.[1]

أولا: ماهية الانترنت

لقد اختلفت التسميات التي أطلقت على الانترنت، ما بين "الشبكة العالمية" أو "شبكة الشبكات" أو "الشبكة العنكبوتية" أو "الطريق السريع الرقمي" أو"كود النقل اللامتزامن"....

فالانترنت لغة: هي كلمة جديدة في القاموس اللغوي لمختلف لغات العالم، وهي كلمة انجليزية ومختصرة من مقطعين Inter وهي اختصار لمصطلح "International" وتعني دولي، وNet

[1] الأستاذ الدكتور عامر إبراهيم قنديلجي- الدكتورة إيمان فاضل السامرائي، تكنولوجيا المعلومات وتطبيقاتها، الورالي للنشر والتوزيع، ص 427.

وهي اختصارا لكلمة Network والتي تعني الشبكة. وبجمع الكلمتين أي:International network فإن المعنى الكامل المتحصل عليه هو الشبكة الدولية هذا من الناحية اللغوية.

ويمكن تعريف الانترنت بأنها "شبكة عالمية دولية" ووسيلة من وسائل الاتصال والتواصل بين الشبكات.

وفي الوقت الحاضر طغى مسمى الانترنت على جميع المسميات الأخرى، سواء على المستوى العلمي أو للاستخدام العام، وإن التعريف العلمي للانترنت الذي أقر من قبل المجلس الاتحادي لشبكة المعلومات Federal Networking Council يعرف الانترنت بأنه نظام عالمي للمعلومات:

- مرتبط علميا بعنوان مميز مبنى على مواصفات خاصة بالانترنت والأنظمة المشتقة منه والمتفرعة عنه.
- يمكن من خلاله دعم الاتصالات عن طريق استخدام مواصفات النظام أو مواصفات أخرى مطابقة.
- يوفر ويستخدم أو يسمح باستخدام خدمات عالية في مجال الاتصالات بواسطة القطاع العام أو الخاص.[1]

وباختصار يمكن تعريف الانترنت بأنها وسيلة اتصال بين الناس عن طريق استخدام الحاسوب.[2] ولحد الساعة لا يوجد تعريف كامل شامل لمصطلح الانترنت لذلك حاول الفقه والقضاء وضع تعريفات اتسمت بالطابع التقني للشبكة والبعض الآخر وضع تعريفات لها متسمة بالطابع الموضعي للشبكة والتي نبرزها في ما يلي:

1-المحاولات الفقهية لبيان مفهوم شبكة الانترنت:

[1]http : // www. Aluah. Net/ culture/ /128516/.
[2]The Related crimeon computerRecommandation N R89 – 9 , P83.

إن الفضل في ظهور مصطلح الانترنت يرجع إلى العالمين الأمريكيين وهما Bob Khan, و Vintserfمبتكري بروتوكوليTCP/IP.

ويرى هذا الاتجاه أن شبكة الانترنت هي: " شبكة تسمح بإنظمام شبكات معلوماتية مختلفة إليها عن طريق استخدام بروتوكول TCP/IP، والبريد الالكتروني e- mail، ومجموعات الأخبار News groups، والصفحات des fichiers (FTP)، وبنوك المعلوماتles banques de données".

ويعتبر هذا الاتجاه أن الانترنت ظاهرة تقنية وفنية، لها صفات تميزها من حيث عدم ملكيتها لأحد في العالم، بالإضافة إلى أنها مفتوحة فهي مجال ليس لأحد سلطان عليه، وعبره نستطيع فعل ما نريد[1]، ولكن يدار بواسطة جمعية للانترنت، وهي منظمة دولية غير حكومية، تعمل على التنسيق العالمي للانترنت وتكنولوجيا المعلومات، وهي تتشكل من أعضاء تنظيميين وفرديين يرتبطون فيما بينهم من أجل الإسهام المشترك في الحفاظ على جدوى وقيمة وعالمية الشبكة[2].

ويعرفها البعض الآخر من الناحية التقنية أيضا بأنها: "شبكة عالمية من الحاسبات التي تعتمد على بروتوكول TCP/IP، والبروتوكولات الأخرى للاتصالات فائقة السرعة بين الآلاف من النقاط والملايين من المستخدمين.[3]

وعرفت بأنها شبكة تتألف من عدد من الحسابات الآلية التي ترتبط فيما بينها، إما عن طريق الخطوط التليفونية أو الأقمار الصناعية لتكون شبكة كبيرة تتيح لمستخدميها الدخول في أي وقت متى كان الحاسب الآلي الخاص به مزودا بجهاز مودم " Modem".

ونعني بكلمة مودم Modemتركيب مزجي بين كلمتين هما Modulatoire, démodulateurوتعني المغير أو المحول، لأن المودم جهاز مهمته تحويل الرسائل الرقمية التي يمكن

[1]KAPLAN, YASMINE- internet, zone de non droit?1996,p2.
[2]The internet Society hime page online available:http:// www.Isoc.org.
[3]http://at.Wikipedia.Org/wiki.

استيعابها من جانب كل من المنفذ والحاسب إلى رسائل أو إشارات تناظرية يمكن نقلها عبر الخطوط التليفونية، هذا عن المودم.

كما عرفها أحد الأساتذة بجامعة "بركلي" Berkeley بالولايات المتحدة الأمريكية بأنها: " شبكة الشبكات"Network of networks[1].

فنلاحظ أن هذه المحاولات كانت محاولات لوصف الشبكة من الناحية الفنية وطريقة عملها لذلك اهتم جانب آخر من الفقه وبعض العلماء ببيان الجانب الوظيفي لشبكة الانترنت وذلك بجانب بيان الجانب التقني لها، وذلك من خلال بيان أسلوب الاتصال بها وأدوات هذا الاتصال، من خلال البروتوكول المنسق وهو TCP/IP، مع الإشارة إلى الخدمات التي تؤديها الشبكة وهذه المحاولات يطلق عليها المحاولات الوظيفية.

فيرى البعض أن شبكة الانترنت هي شبكة اتصالات دولية متصلة ببنوك المعلومات، ومراكز البحث العلمي ومراكز المعلومات المفتوحة والخاصة، التي يتم بها الحصول على معلومات من قبل المشتركين بالشبكة ولكل منهم كلمة المرور وصندوق البريد الالكتروني، وموقع مخصص له. كما ذهب البعض الآخر إلى أن شبكة الانترنت هي: "الطرق الدولية للمعلومات".

2-المحاولات القضائية لبيان مفهوم شبكة الانترنت: اتجهت أغلب أحكام المحاكم في القانون المقارن التي تناولت شبكة الانترنت إلى الاهتمام برصيد القيمة الإنسانية لهذه الشبكة، وبيان وظائفها في خدمة البشرية، بالإضافة إلى بيان الجانب التقني لها.

[1]Georgio BOVENZI, labilités of system opératoires an the internet, Berkeley technologie law journal-voll. Lart.1, p2, available on line at : http : // www.Berkeley. Edu/ journal/ ptlg/ articles/ 1111 Bovenzi/ htm 1/ text/ htm.

فقد وصفت شبكة الانترنت من قبل المحكمة العليا في الولايات المتحدة الأمريكية بأنها: "شبكة دولية من الحاسبات المترابطة والمتصلة وتعد أهم وسائل الاتصال الحديثة، ولا يوجد لها حدود إقليمية"[1].

كما صدر تعريف لها من المحكمة الابتدائية لجنوب أوهايو، القسم الشرقي في الحكم الصادر في 1997/2/3 في قضية شركة كومبيوسيرف Compuserve وشركة ستانفورد ولكي Stanford Wallaceبأنها: "شبكة الشبكات" . وذهبت المحكمة الابتدائية لشرق فرجينيا (قسم الإسكندرية) إلى تعريف شبكة الانترنت بأنها: "الطريق الدولي للمعلومات، فهي شبكة اتصالات معقدة يرتبط بها شبكات حاسوب عامة وخاصة، أنظمة وأفراد وهي تتكون من حاسبات وقواعد بياناتها متصلة من خلال خطوط هاتف".[2]

وعن المحاولات الدولية لوضع تعريف لشبكة الانترنت نجد الاتفاقية الأوروبية للجريمة الافتراضية Convention on cyber crime of 23novembre 2001 (ETS. NO 185) قد عرفت في نص المادة 1 (أ)،Article a... والانترنت هي شبكة عالمية تتكون من العديد من الشبكات المتصلة، وجميعها يستخدم ذات البروتوكول. وهو تعريف يهتم بالجانب التقني للانترنت وطريقة عملها.[3]

ونرى أن شبكة الانترنت: "هي شبكة عنكبوتية تواصل بين شبكات عنكبوتية من الحاسبات الآلية المتصلة عبر الدول، تسمح بتبادل المعلومات عبرها، بين الأفراد والمؤسسات والشركات، عن طريق استخدام بروتوكول TCP/ IP.[4]

[1]Re No V.American civil liberties union,0000u,s96-511,1997,http://Supect. Lawi.Carnell.Edu/htmt/ 96-511.ZS.htm/.
[2]http://www.Bna.Com/e-law/ docs/aolcuber.Htm/.
[3]http:// www.Conventions.Coe.Int/ treaty/en/projects/finalcyberapex.Htm.
[4]رشدي محمد علي محمد عيد علي، الحماية الجنائية للمعلومات على شبكات الانترنت، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ص44.

ثانيا: التطور التاريخي لشبكة الانترنت

ترجع الأصول التاريخية للانترنت إلى عام 1962، وهو التاريخ الحقيقي لولادة الانترنت، على يد العلماء العاملين في وكالة الأبحاث والمشروعات المتطورة في الولايات المتحدة الأمريكية The Advanced research Project agency والتي كانت إحدى الوكالات المدعمة رسميا من قبل وزارة الدفاع الأمريكية وكانت تعرف اختصارا ARBA، وهذا المشروع كان يستهدف تحقيق هدفا استراتيجيا، وهو إرسال تعليمات التصويب من خلال مركز التحكم إلى قواعد الصواريخ حتى ولو بعد تدمير جزء من شبكات الاتصال نتيجة لتعرضها لهجوم.[1]

وقد عرفت هذه الوكالة في ما بعد باسم DARBA.

وعقب الحرب العالمية الثانية، وظهور الحرب الباردة cold war بين الولايات المتحدة الأمريكية والاتحاد السوفياتي، قامت مؤسسة "راند" "Rand corporation"وهي المؤسسة الرئيسية لإعداد الأفكار لمواجهة الحرب الباردة في عام 1964 بإعداد مقترحات بشأن كيفية الاتصال بين سلطات الولايات المتحدة الأمريكية في حالة حدوث كوارث طبيعية أو من صنع الإنسان أو غيرهم كهجوم ذري أو نووي مثلا، وانتهت إلى إمكانية إعداد برنامج للاتصال يعمل في كافة الظروف من خلال شبكة الاتصال. وإن هذه الشبكة لن يكون عليها أي سلطة مركزية لأية دولة في العالم.[2]

وفي عام 1968، تمت أولى تجارب هذه الشبكة في معمل الأبحاث الوطنية في بريطانيا، وبعد ذلك في عام 1969 أقامت وكالة ARBA باستخدام هذه الشبكة رسميا وسميت ARBANET. وقد

[1]JARVELOPP HARRY- An introduction to law of the internet (part 1) op- cit, p1.
http : // www. Cbi. Um n. edu/ darpa/ ipto. Htm/.

[2]رشدي محمد علي محمد عيد علي، الحماية الجنائية للمعلومات على شبكات الانترنت، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ص35.

أنشأت هذه الشبكة بهدف تطوير شبكة المعلومات بدون " حاسب آلي مركزي "، يسمح بإنشاء ونشر معلومات عسكرية آمنة.[1]

وكانت تضم مواقع أربعة مشاركة في الشبكة، هي جامعة كاليفورنيا في مدينة لوس أنجلس (USA) ومعهد ستانفورد للأبحاث (SRI) وجامعة كاليفورنيا في مدينة سانتاباربارا (UCSB) وجامعة يوتا (Utahu).

ثم بدأت هذه الشبكة تنمو وتتطور منذ ذلك التاريخ وكان أساس تصميم هذه الشبكة هو استخدام نفس المحددات، أو ما يطلق عليها البروتوكول (protocoles)، وكما ذكرنا سلفا أن شبكة أربانت صممت بشكل لا مركز على أساس أن إذا ما تعطلت من الحواسيب الموصلة والمرتبطة عن العمل لأي سبب كان، فإنه يستمر العمل على نقل المعلومات عن طريق الحواسيب الأخرى.[2]

وذلك بهدف مقاومة التدمير الجزئي الذي يصيب الشبكة. وللتوضيح أكثر إذا حصل أي عطل فإنه يتم التواصل بين الحواسيب عن طريق استخدام أسلوب القنوات المطولة التي تستمر في عملها حتى لو أصاب جزء من الشبكة بعض الأعطال.

إذا مشروع أربانت الذي أطلق عام 1969 هو مشروع من وزارة الدفاع الولايات المتحدة، أنشأ هذا المشروع من أجل مساعدة الجيش الأمريكي عبر شبكات الحاسب الآلي وربط الجامعات ومؤسسات الأبحاث لاستغلال أمثل للقدرات الحسابية للحواسيب المتوفرة.

وفي عام 1973 كانت البداية الحقيقة للانترنت، بربط الحسابات الآلية المختلفة والتي تستخدم بروتوكول مشترك للاتصال TCP/IP وهذا البروتوكول هو القاعدة المعيارية المحددة للاتصال

[1] رشدي محمد علي محمد عيد علي، الحماية الجنائية للمعلومات على شبكات الانترنت، المرجع السابق، ص36.

[2] د. مدحت رمضان جرائم الاعتدار على الأشخاص والانترنت، دار النهضة العربية، القاهرة، 2000، ص3.

عبر الانترنت وهو يقوم بتقسيم المعلومات المراد إرسالها من حاسوب عبر الانترنت إلى حزم Packets، ثم إعادة تجميعها من جديد في حاسوب آخر في الجهة المرسلة إليها.

فهذا البروتوكول يقوم بتسيير عمليات الاتصال وتبادل المعلومات بين الشبكات وحواسيبها المختلفة، ذات الأنظمة والبرامجيات المتباينة.[1]

ولتوضيح أكثر نقصد ب TCP/IP بروتوكولان معروفان باسم بروتوكول النقل والسيطرة Transmission and control Protocolواختصارا TCP.

وبروتوكول انترنت (internet protocol) واختصاراً IP.[2]ويعتبر هذا الأخير قاعدة الاتصال بالانترنت، إلا أنه بالإضافة إليه يوجد البروتوكول الآخر TCP الذي يكمل دوره IP ويعمل بطريقة إضافية، ويمنح تحكما أفضل في الكم الهائل من المعلومات التي يجري تناقلها عبر الشبكة. وعلى أساس عمل البروتوكولين بشكل متزامن لذا يشار إليهما (TCP/IP)، لذا أطلق عليه تسمية بروتوكول مشترك، فهذا البروتوكول يسمح للانترنت بأن تعمل على تحويل الحزم الخاصة بالبيانات لكي تصل إلى الجهة المرسلة إليها، وبسرعة فائقة.

وفي عام 1983 تم تقسيم ARBANET إلى شبكتين الأولى هي MILNET بحيث اقتصر استخدام هذه الأخيرة على النواحي العسكرية، والثانية ARBANET واقتصر استخدام هذه الأخيرة على الأغراض المدنية. وهذا التقسيم كان بقرار من وزارة الدفاع الأمريكية.[3]

وفي عام 1986 أصبحت ARBANET متاحة لكافة أشكال البحث العلمي وذلك بسبب نقل تشغيلها من وزارة الدفاع إلى شبكة مؤسسة العلوم الوطنية National Science

[1] رشدي محمد علي محمد عيد علي، الحماية الجنائية للمعلومات على شبكة الانترنت، المرجع السابق، ص36.
[2] العميد الدكتور أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الثانية، 2006، ص 52- 53.
[3] منير محمد الجنبيهي- ممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، 2006، ص8.

fondationواختصارا NSFNET. وإدارة الطيران المدني والفضاء الأمريكي The national aeronational and space administration وكذلك إدارة الطاقة pepartmentenergy-.

فأصبحت NSFNET العمود الفقري وحجر الأساس لنمو وازدهار الانترنت في أمريكا ومن ثم دول العالم الأخرى.

وكان ألبرت جو نائب الرئيس الأمريكي هو أول من استخدم إمكانات هذه الشبكة على نطاق عالمي وإنشاء ما يعرف بطريق المعلومات الرقمية أو طريق البيانات السريع، أو طريق المعلومات السريع أو فائق السرعة.[1]

وفي عام 1990 ظهرت الانترنت كتسمية جديدة وسمح للأفراد العاديين باستخدامها، وأوقفت الحكومة الأمريكية تمويلها للشبكة وتركت ذلك للقطاع الخاص بسبب إنتفاء الجدوى من بقائها.

وفي عام 1991 تمكن أحد مهندسي الاتصالات بانجلترا ويدعى Tim Bernerslee من اختراع .W.W.W أو (W3).

وبعد ان أثبت الاتصال الالكتروني فعاليته تم إنشاء عدد كبير من الشبكات الحكومية الضخمة في الولايات المتحدة وأوروبا لخدمة نظم الاتصالات والمعلومات، وازداد عدد الشبكات بشكل أكبر بعد دخول الشركات التجارية وتوفيرها خدمات الشبكة بأسعار منافسة.

ويتضح التطور الهائل الذي حدث في الثمانينات والتسعينات الميلادية بالنسبة لعدد المشتركين منذ بدء الشبكة سنة 1969م حتى سنة 1998 فقد قفز العدد المسجل من أربعة مواقع إلى حوالي أربعة ملايين موقع.

[1]http://www.Alukh.Net/culture/0/28516/

موقع الألوكة د. عبد الله عبد الرحمان آل عبد الجبار، الانترنت والتاريخ، (التطور والتطبيقات).

وهذا التطور السريع الذي حدث في بداية التسعينات، الفضل فيه يعود إلى سماح الحكومة الأمريكية للشركات استخدام الانترنت تجاريا لأول مرة بعد أن كان استخدامها مقصورا على القطاعات الحكومية والتعليم ومعاهد الأبحاث إضافة إلى الشركات المتعاونة مع القطاعات العامة.[1]

وبتزايد عدد المتعاملين بالانترنت بصورة كبيرة، أصبح يقال حاليا أن هناك دولة جديدة قد ظهرت وهي دولة المتعاملين مع الانترنت ويبلغ تعداد سكانها أكثر من حوالي 40 مليون مواطن يتزايدون بنسبة 5%شهريا، نظرا لأنه وكما ذكرنا سابقا لم يعد استخدامها قاصرا على باحثي الجامعات وموظفي المؤسسات العامة، وإنما استخدمت بمعرفة الأفراد والشركات الخاصة، وتزايد استخدامها من الناحية التجارية، ويتوقع تزايد عدد مستخدمي شبكة الانترنت إلى 720 مليون في المستقبل القريب.[2]

فخلال هذه الفترة الوجيزة استطاع العالم أن يحقق قفزة كبيرة في تبادل المعلومات عن طريق الانترنت التي أزاحت جميع العقبات الجغرافية والسياسية والمادية، فقد أصبح الفرد قادرا على الوصول إلى جميع مناطق العالم دون أن يتحرك من أمام شاشة حاسوبه، ولم يعد مقيدا بالإطلاع على صحيفة واحدة، فأمامه آلاف الصحف المحلية والعالمية، والمجلات العامة سواء كانت سياسية أو اقتصادية أو فنية أو رياضية، وكذلك الدوريات المتخصصة التي تلاءم اهتمامات وتطلعات كل متخصص، وغيرها من مصادر المعلومات المختلفة.

[1]Internet society, « ABrief History of internet and related networks.
http : // www. Isoc. Org/ internet/ history/ cerf. Shtm/.

[2]رشدي محمد علي محمد عيد علي، الحماية الجنائية للمعلومات على شبكة الانترنت، المرجع السابق، ص38.

المطلب الثاني: فوائد الانترنت وسلبياته

سيتم عرض ايجابيات شبكة الانترنت من خلال الخدمات المختلفة المقدمة عبرها، حيث سنرى أن هذه الخدمات يوجد الوجه الايجابي لها وكذلك السلبي، كما هو الحال عند طبيعة الأشياء.

وسنحاول تفسير هذا في نقطتين، حيث سنتناول في النقطة الاولى: فوائد وايجابيات شبكة الانترنت.

وسنتناول في النقطة الثانية: سلبيات شبكة الانترنت اي الوجه الخطير للانترنت.

أولا: فوائد أو ايجابيات شبكة الانترنت

شبكة الانترنت حصلت نتيجة لربط وتوحيد شبكات عديدة ومختلفة موجودة في جميع انحاء العالم، هذا التوحيد أدى إلى أن يكون كل مستخدم قادر على الحصول على كمية أكبر من المعلومات. لأنه أصبح بإمكانه استخدام الشبكات العديدة الأخرى والتي تحتوي على معلومات إضافية غير تلك الموجودة في الشبكة التي يتبع لها. {Kjaer, 1994}.

التنافس المستمر بين الشركات العديدة على اكتساب أكبر عدد من مستخدمي شبكة الانترنت لهم وأيضا اكتساب ثقتهم يؤدي إلى تطوير وإعطاء خدمات قيمة لهؤلاء المستخدمين أحد المقاييس لنجاح وشهرة موقع ما هو عدد زوار الموقع. لذا نرى خدمات عديدة في مواقع كثيرة يستطيع الزائر استخدامها دون أن يطالب بثمن لذلك. التهافت المكثف والمستمر من قبل مستخدمي شبكة الانترنت على موقع معين يجعل أصحاب هذا الموقع قادرين على نشر الدعايات عبر الموقع. وبهذا جلب الدخل الكبير لهذا الموقع ولتطوير خدمات أخرى لتستعمل مجاناً من قبل مستخدمي الشبكة، على سبيل المثال تساعد هذه الخدمات في الوصول إلى المعلومات المطلوبة (خدمات للبحث عن المعلومات). وأخرى تهدف إلى تقوية وتسهيل الاتصال بين مستخدمي الشبكة منها نذكر البريد الالكتروني، مجموعات الحوار والمحادثة، إضافة إلى ذلك تعطي مواقع كثيرة

إمكانية بناء مواقع شخصية لمستخدمي شبكة الانترنت دون طلب مقابل لذلك، أي أن استضافة هذه المواقع تكون مجاناً.

وفيما يلي سيتم عرض ايجابيات أيضا من خلال الخدمات المختلفة المقدمة عبرها وذلك في النقاط التالية:[1]

1- سرعة نقل وتمرير المعلومات:

أكثر الخدمات استعمالاً في شبكة الانترنت هي خدمة البريد الالكتروني التي تسمح لكل من له عنوان بريدي على الشبكة بأن يبعث ويستقبل رسائل بواسطة البريد الالكتروني.

حسنات البريد الالكتروني تكمن في الدمج بين سرعة نقل الرسائل والسعر الباهظ وكذلك في إمكانية بعث نفس الرسالة إلى مجموعة كبيرة من الناس، يمكن أن يتعدى عددهم مئات وآلاف الأشخاص (هذا الشيء يمكن تنفيذه عن طريق إعطاء هؤلاء الأشخاص اسم مجموعة ومن ثم بعث الرسالة إلى هذه المجموعة.

في الولايات المتحدة تعدى عدد الرسائل المبعوثة بواسطة البريد الالكتروني عدد الرسائل المبعوثة بواسطة البريد العادي. ولا يوجد أي سبب في عدم استخدامه بشكل ناجح من قبل طلبة ومعلمي المدارس والمعاهد لفرض الاتصال وتبادل المعلومات.

2- بنوك ومجمعات المعلومات:

بنوك ومجمعات المعلومات في شبكة الانترنت موجودة تقريبا في جميع المجالات وتغطي غالبية المواضيع، فعلى سبيل المثال يمكن الدخول إلى مواقع تحتوي على القرآن الكريم بأكمله والأحاديث النبوية الشريفة في مجمع معلومات والبحث عن الشيء المطلوب وفق أساليب بحث مختلفة كذلك يوجد الكثير جداً من الموسوعات الضخمة والغنية بالمعلومات والقواميس المختلفة والمهمة على شبكة

[1] http : // yomgedid. Kenanaonline.Com/ posts/ 8407.

الانترنت التي يمكن استخداماه بسهولة وبشكل حر، مما يزيد من التساؤل في مدى ضرورة شراء هذه الموسوعات والقواميس كمرجع بيتي. كمية ونوعية المعلومات الموجودة في مجمع معلومات وسهولة استعماله تعتبر من أهم العوامل التي تساعد على نجاح وشهرة هذا المجمع، يمكن استغلال مجمعات المعلومات في العملية التعليمية والتثقيفية في المدارس والمعاهد المختلفة بشكل مفيد للطالب.

مثال: مجمع ابن خلدون للمواد التعليمية باللغة العربية الذي طور في المعهد الأكاديمي لإعداد المعلمين العرب يعتبر أحد الأمثلة لمجمعات معلومات مفيدة الاستعمال لجمهور الطلبة والمعلمين في المدارس والكليات العربية. عنوان هذا المجمع هو http // : mawad. Beitberl. Acil.

3-الانترنت كحقيبة معلومات شخصية متنقلة مع المستخدم:

يمكن اعتبار الانترنت حقيبة معلومات شخصية متنقلة مع المستخدم، لأن كل شخص قادر على بناء موقع يتضمن المعلومات التي يريدها ولأنه قادر على الوصول إلى هذا الموقع من كل مكان في العالم (بالطبع بشرط أن يكون لديه حاسب وخط اتصال).[1]

4-تعدد الوسائط في الشبكة العالمية (www):

الشبكة العنكبوتية العالمية world wide web تعتبر أكبر شبكة حاسب من بين الشبكات المكونة لشبكة الانترنت، تسمح هذه الشبكة بإظهار المعلومات بأشكال مختلفة، أي بوسائط عديدة (نصوص، صور، رسومات، صوت...الخ). مما يساعد في نشر المعلومات بشكل واضح وممتع، لذا فهي تعتبر أشهر شبكة لمستخدمي الانترنت. حواسيب هذه الشبكة تستخدم ثلاث تقنيات حديثة، هي النصوص الفائقة (hyper texte)، بروتوكول لنقل النصوص الفائقة HyperText (http Transfer Protocol)، وبرامج التصفح (Browser).

5-الانترنت مكتبة لكل شخص:

[1] (طيبي 1997): طيبي مؤنس، العالم يتحول إلى قرية، الرسالة بيت بيرل، 1997.

في الحقيقة يوجد في الانترنت كتب عديدة وقيمة، يمكن قراءتها وطباعتها عبر الشبكة (أي في وقت التصفح) أو نسخها بأكملها إلى الحاسب الشخصي، يوجد موقع باسم Backs online يحتوي على آلاف الكتب للقراءة والطباعة الحرة، إضافة إلى ذلك هناك الجرائد، والمجلات والمقالات في العديد من المجالات التي يمكن الاستفادة منها.

لذا بإمكان كل شخص استخدام الشبكة كمكتبة شخصية له، يستطيع من خلالها الإطلاع على الموضوعات التي يرغبها.

6-مجموعات الحوار والمحادثة:

يمكن استغلال مجموعات الحوار لتبادل الأفكار مع أشخاص آخرين وأيضا من أجل طرح الأسئلة على مجموعة خبراء والحصول على مساعدة في المجال المطروح, ويوجد مجموعة حوار مغلقة وأخرى مفتوحة لكل من يريد الاشتراك في الحوار.

أنظمة المحادثة تسمح بالمكاتبة المباشرة وكذلك المحادثة الصوتية والمصورة بين الأشخاص في مواضع مختلفة، إلا ان الموضوع السائد في أنظمة المحادثة هو التعارف. يمكن استخدام مجموعات الحوار كحلقة دراسية في مجال التعليم.[1]

ثانيا: سلبيات شبكة الانترنت أو الوجه الخطير لشبكة الانترنت

[1](طيبي 1999): طيبي مؤنس: شبكة الانترنت للطالب والمعلم، صدى التربية 47، آذار 1999.

مما ذكر أعلاه يتضح أن لشبكة الانترنت إيجابيات عديدة تساهم جيداً في تطوير طريقة العمل في المجالات المختلفة، هذه الايجابيات تزيد على السلبيات التي علينا أيضا أن نعرفها، لذا سنتطرق فيما يلي إلى أبرز سلبيات شبكة الانترنت.

1-عدم الرقابة والإباحة:

بالمقابل إلى ما ذكر أعلاه يؤكد ظهور شبكة الانترنت كنتيجة لتوحيد شبكات عديدة على أن هذه الشبكة عالمية لا تتبع أي دولة، مؤسسة أو شخص، هذه الحقيقة توضح أن نشر المعلومات عبر الشبكة لا يمر على أي نوع من الرقابة، بذلك يكون كل شخص قادراً على نشر ما يريد من المعلومات في موقع خاص به بسرعة وسهولة وحتى بدون أن يدفع مقابلا لنشر هذا الموقع، لذلك نجد في شبكة الانترنت الكثير من المواقع الغير مقبولة عند الأنظمة الاجتماعية الصالحة، منها مثلا مواقع العنف، مواقع الجنس، مواقع عنصرية وغيرها من المواقع التي يجب أن تكون ممنوعة في مجال التربية والتعليم وبالتأكيد في جميع المجالات الأخرى، حل هذه المشكلة ليس سهلا، لذا لا نجد حتى الآن حلولا ناجحة لها، تسمح باستخدام شبكة الانترنت في المدارس مثلاً ومنع في نفس الوقت الطلبة من الوصول إلى هذه المواقع غير المرغوبة.[1]

2-الإدمان:

الشعور بالحاجة الملحة إلى الإبحار في شبكة الانترنت يحصل عند الكثير من المستخدمين، هذه الحاجة تعتبر إحدى ظواهر الإدمان على الشبكة، كما انه يوجد أشخاص مدمنون على التلفاز، ليس غريبا أن نجد أشخاصاً مدمنين على شبكة الانترنت، بالطبع يصبح الإبحار في شبكة الانترنت لأوقات طويلة قلة الحركة التي من الممكن أن تؤدي إلى مشاكل جسدية بسبب الجلوس الغير الصحي، أمام الحاسب أو إلى مشاكل في النظر بسبب الأشعة الناتجة عن الشاشة.

[1]http://www.Kenana online.Com/page/8907

3- العزلة:

عند العمل في شبكة الانترنت يجلس المستخدم عادة وحيداً أمام الحاسب، حيث بإمكانه أن يقضي ساعات طويلة تعزله عن المجتمع القريب والبعيد عنه، فالإبحار في الشبكة مصحوب بعزلة معينة عن المجتمع المجاور(العائلة والأصدقاء)، مما قد تؤدي في حالات كثيرة إلى مشاكل أخرى منها اجتماعية، تتمثل في صعوبة الاتصال والتعامل مع المجتمع المحيط وأخرى نفسية تتمثل في الانزواء والانطواء عن النفس.

لذا على الأهل الانتباه لمثل هذه الحالات ومراقبة أولادهم وقت التصفح لكي لا يتضرر أحد منهم.[1]

4- الاعتقاد بأن المعلومات على الشاشة دوما صحيحة:

نلاحظ في كثير من الأحيان أن متصفحي شبكة الانترنت يعتقدون بان المعلومات الموجودة على شبكة الانترنت هي دوما صحيحة ويمكن الأخد بها دون التأكد من صحتها ومن صحة مصدرها، هذا الافتراض غير صحيح، فهناك معلومات خاطئة على الشبكة، ولذا يجب التأكد دوماً من مصدر هذه المعلومات.[2]

5- نسخ معلومات واستعمالها كأنها شخصية:

حقوق النشر والطباعة على شبكة الانترنت ما زالت غير واضحة تماما، كثيراً ما نرى نسخاً لمعلومات ووظائف ومن ثم استعمالها كأنها شخصية، هذه الظاهرة لها أبعاد سلبية، خصوصاً عند

[1] http://www.Cksu.Com/vb/sHowthread.Phpt=201452.
[2] http://alyaseer.Net/vb/sHowthread.Phpt=13301.

انتشارها بين الطلبة، إذ لا يحتاج الطالب لإجهاد نفسه في التفكير وفي حل الوظائف، بل يحاول الوصول إلى الوظائف المحلولة ليسهل على نفسه الطريق.[1]

خلاصة نجد أن الجهود لإقامة شبكة الانترنت لم تأتي إلا بعد أن لوحظ بأنه لا يوجد انسجام وتلاؤم بين المعلومات الموجودة في شبكة الانترنت الحالية، الهدف الأساسي لشبكة الانترنت هو تغيير المعلومات والمحتويات الموجودة في الشبكة والمحافظة على أن تكون الانترنت شبكة أكاديمية وعلمية، تخدم المعاهد والجامعات والبحوث العلمية.

فكما لاحظنا هناك استفادة كبيرة من وجود شبكة الانترنت وهناك الخدمات الجيدة والملائمة أيضا لمجال التعليم التي يجب علينا الاخد بها وتطويرها، لكن في نفس الوقت علينا الحذر والابتعاد عن السلبيات الناتجة عن الاستعمال غير السليم لهذه التطورات في مجال الحاسوب والتكنولوجيا، نحن نعي أن للسيف حدين وكذلك لشبكة الانترنت وجهان، نأمل أن يأخذ مجتمعنا الوجه السليم لهذه الشبكة.

المطلب الثالث: ماهية المعلومة وطبيعتها القانونية

إن امتلاك المعلومة يعني القدرة على امتلاك الحاضر والمستقبل، لأنها هي الأداة لتنظيم المعرفة، والمعرفة هي مجموعة المعاني والمعتقدات والمفاهيم والتصورات الفكرية التي تتكون لدى الإنسان نتيجة المحاولات المتكررة لفهم الظواهر والأشياء المحيطة به، وتمثل حصيلة خبرة ومعلومات ودراسة طويلة يمتلكها الشخص في وقت معين.

ويختلف رصيد المعرفة من شخص لآخر، وفقا لنسبة حصوله على المعارف والخبرات الجديدة.

والمعلومة أصبحت تحيط بنا في كل مكان ومن كل اتجاه حتى أصبحت كالغشاء الهوائي الذي يوفر لنا الحياة.

[1] http://yomgedid.Kenanainline.Com/topics/57592/posts/84072

ونظراً لحداثة علم المعلومات فإن مفاهيمه وتعريفاته غير مستقرة، ولم تحظى بالاتفاق الكامل عليها.

وسوف نحاول توضيح ذلك بالتعرض إلى :

- مفهوم المعلومة كنقطة اولى.
- أنواع المعلومات كنقطة ثانية.
- الشروط الواجب توافرها في المعلومة محل الحماية الجنائية وطبيعتها القانونية كنقطة ثالثة.

أولا: مفهوم المعلومات

المعلومة وجدت منذ خلق الله سبحانه وتعالى الإنسان عندما خلق آدم عليه السلام وعلمه الأسماء كلها، قال الله تعالى في كتابة العزيز: **" وعلم آدم الأسماء كلّها ثم عرضهم على الملائكة فقال أنبئوني بأسماء هؤلاء إن كنتم صادقين"** صدق الله العظيم.[1]

قال الله تعالى: " **إقرأ باسم ربك الذي خلق (1) خلق الإنسان من علق (2) إقرأ وربك الأكرم (3) الّذي علّم بالقلم (4) علم الإنسان ما لم يعلم (5)"**صدق الله العظيم.[2]

فالمعلومات هي أغلى ما يمتلكه الإنسان في حياته على مر العصور لذا سعى إلى جمعها وتسجيلها على وسائط حفظ مختلفة بدءً من جدران المقابر والمعابد وأوراق البردي في عصر الفراعنة إلى أن تم اختراع الورق في الصين.

ويرجع الفضل في الإبقاء على الحضارات محفورة في ذاكرة التاريخ، هو تسجيل هذه الحضارات لحضاراتهم على الجدران، وجدران المقابر والمعابد... وأحسن مثال لذلك الحضارة المصرية،

[1] سورة البقرة الآية "31".

[2] سورة العلق من الآية رقم "1 " حتى الآية رقم "5 ".

وعدم تسجيل المعلومات هو كذلك السبب في عدم ذكر التاريخ لحضارات عظيمة قد اندثرت لعدم تسجيلها.

فلذلك تعتبر المعلومات رمزاً من رموز الحضارة الإنسانية على مدى التاريخ، وإذا فقد الإنسان معلوماته فهذا يعني فقدانه لذاكرته ومن ثم تضيع حضارته.[1]

والمعلومات من حيث المصطلحات التي تكاد تفقد وزنها الدلالي من كثرة الاستعمال وهي من الكلمات المراوغة صعبة المراس حيث أن جميع التعريفات التي ذكرت في المعلومات تعبر بشكل كبير عن آراء ووجهات نظر أصحابها، وهذه التعريفات قد تكون مقبولة عند بعض التخصصات ومرفوضة عند البعض الآخر.[2]

والمعلومات أصبحت في بيئة اليوم ترتبط بمختلف جوانب الحياة، وتمثل ركيزة نشاط الإنسان الاقتصادي والاجتماعي والثقافي والسياسي، وتتيح له المعرفة بالواقع ومشكلاته وأبعاد هذه المشكلات، بل أنها أصبحت تتيح مكينة اتخاذ القرارات في كافة المجالات تقريباً.[3]

وتم تقدير تعريفات المعلومات حتى الآن بـ 400 تعريف وسوف نحاول توضيح مجموعة من هذه التعريفات كما يلي:

1- مفهوم المعلومة لغة:

المعلومات من حيث مدلولها اللغوي مشتقة من المادة اللغوية "علم"، وهي مادة غنية بالكثير من المعاني كالعلم والإحاطة بباطن الأمور والوعي والإدراك واليقين والإرشاد والإعلام والشهرة، والتميز والتيسير، وتحديد المعالم، والمعرفة، والتعليم والتعلم، والدراية... إلى آخر ذلك من المعاني المتصلة بوظائف العقل.

[1] العميد د. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الثانية، 2006، ص70.

[2] http://Ahmad Farag.bbF/aSh.Net/t49-topic.

[3] د. خالد ممدوح إبراهيم، الجريمة الالكترونية، الدار الجامعية، 2008، ص26.

وترجع كذلك إلى كلمة " مَعْلَم "، أي الأثر الذي يستدل به على الطريق وInformation هي المقابل الانجليزي لكلمة معلومات، وهذه الكلمة الانجليزية مشتقة من اللاتينية informationوالتي كانت تعني في الأصل الاتصال والتلقي.[1]

وهناك مصطلح آخر للمعلومة مشتق من التصور "Informatum" والذي يعني "الرسم" أو "التخطيط". غير أنه يلاحظ أن هذين المعنيين هما وجهان لحقيقة واحدة. فالأول يوضح الجانب الحركي للمعلومة، والثاني يبين الجانب الوصفي لها.

2- مفهوم المعلومات اصطلاحاً:

والمصطلح هو ما اصطلح عليه القوم، وغالبا تتمثل التعريفات الاصطلاحية فيما ورد في معاجم وموسوعات التخصص، وفيما يلي بعض تعريفات المعلومات كما وردت في بعض المعاجم والموسوعات:

فقد عرفت المعلومات وفقاً للمعجم الموسوعي لمصطلحات المكتبات والمعلومات أنها:[2]

" البيانات التي تمت معالجتها لتحقيق هدف معين أو لاستعمال محدد، لأغراض اتخاد القرارات، أي البيانات التي أصبح لها قيمة بعد تحليلها، أو تفسيرها، أو تجميعها في شكل ذي معنى والتي يمكن تداولها وتسجيلها ونشرها وتوزيعها في صورة رسمية أو غير رسمية وفي أي شكل". وعرفت المعلومات كذلك على أنها المقومات الجوهرية في أي نظام للتحكم.

وكذلك عرفت المعلومات في قاموس البنهاوي الموسوعي على أنها:

" الحقائق الموصلة، ولها تعريف آخر بأنها رسالة تستخدم لتمثيل حقيقة أو مفهوم استخدام وحدة وسط بيانات ومعناه، أيضا عرفت بأنها عملية توصيل حقائق أو مفاهيم من أجل زيادة المعرفة.

[1] رشدي محمد علي محمد عيد علي، المرجع السابق، ص10.

[2] http://Ahmad Farag.bbF/aSh.Net/ t 49- topic

وإذا رجعنا إلى تعريف المشرعين والفقهاء نجد أن:

المشرع الأمريكي عرف المعلومات في قانون المعاملات التجارية الالكترونية لسنة 1999 بالفقرة العاشرة من المادة الثانية بأنها: "تشمل البيانات والكلمات والصور والأصوات والرسائل وبرامج الكمبيوتر والبرامج الموضوعة على الأقراص المرنة وقواعد البيانات أو ما شابه ذلك.[1]

وكذلك عرف الأستاذ CATALA المعلومة بأنها: " رسالة ما نعبر عنها في شكل لها قابلية للنقل أو الإبلاغ للغير ".

وذهب أحد الفقهاء إلى أن: " المعلومة عبارة عن تعبير وصيغ لكي تكون رسالة معلنة، ثم تعلن أو يمكن أن تعلن بواسطة رموز مختارة لنقل الرسالة إلى الغير ".

فما يميز هذا التعريف أنه ينتقل بالمعلومة من حيز الفكرة إلى الشكل لأن الفكرة لا يمكن أن تاخد شكل المعلومة ما دامت لم تأخذ شكل إشارة أو رمزاً ملموساً.[2]

وعرفها أيضاً أحد الفقهاء وهو ينتسب إلى مدرسة شيكاغو l'école de Chicago بانه:"هي التمثيل الأفضل لكل الاختيارات، أو هي تحكم أو توجه كل اختيار".

ثانيا: أنواع المعلومات

تصنف المعلومات من قبل البعض إلى طوائف وأنواع ثلاث:

- الطائفة الأولى: المعلومات الاسمية

أ- المعلومات الشخصية

ب- المعلومات الموضوعية

[1] د. خالد ممدوح إبراهيم، المرجع السابق، ص27.

[2] رشدي محمد علي محمد عيد علي، المرجع السابق، ص16.

- الطائفة الثانية: المعلومات الخاصة بالمصنفات الفكرية
- الطائفة الثالثة: المعلومات المباحة أو الشاغرة

وسنتناول هذه الطوائف بالتفصيل:

1- الطائفة الأولى: المعلومات الاسمية: les informations nominatives:

ويقصد بالمعلومات الاسمية المعلومات الشخصية والموضوعية المتعلقة بالأشخاص. حيث نصت المادة الرابعة من القانون الفرنسي رقم 17 الخاص بالمعلوماتية والحريات الصادر في 6يناير1978 على أن: "المعلومات تكون اسمية إذا كانت تسمح مباشرة أو غير مباشرة، وتحت أي شكل بالتعرف على الشخص محل هذه المعلومات، أو تجعله قابلا للتعرف عليه". فما المقصود بالمعلومات الشخصية والمعلومات الموضوعية؟

أ- المعلومات الشخصية: les informationspersonnelles:

نقصد بالمعلومات الشخصية المعلومات المتعلقة بأحد الأشخاص وذلك من حيث اسمه، لقبه، موطنه، جنسيته، وضعه الاجتماعي... كل شيء يتعلق بحياته الخاصة.

وبما أنه ذكرنا أنها تتعلق بالحياة الخاصة للشخص فهذا يوحي بالخصوصية ولا يجوز للغير أن يطلع على هذه المعلومات في أي نظام معلوماتي بدون الحصول على إذن من المعني بالأمر فصاحب الشيء هو مالكه ولا يجوز للغير التعدي عليه.

وهذا الأمر أكدت عليه نصوص القانون الفرنسي رقم 17 الصادر في 6 يناير سنة 1978 بشأن نظم المعلوماتية والحريات.[1]

ب- المعلومات الموضوعية: les information objectives:

[1]Loi N°17-78 du Janvier 1978 relative à l'informatique aux fichiers et aux libertés (J.O du 7 Janvier 1978).

المعلومات الموضوعية هي المعلومات المنسوبة إلى شخص ما معبرا بها عن رأيه اتجاه الغير. ومثل ذلك مقالات الصحف، الملفات الإدارية للعاملين لدى جهة معينة.

فهذه المعلومات لا تتعلق بالشخص القائل أي الصادرة عنه وإنما تتعلق بشخص آخر.

مثلا: الصحفي الذي يكتب مقالا عن أحد الأشخاص له حق على هذا المقال، ولكن في نفس الوقت يجب عليه عدم التعدي على حق الشخص محل المقال. ومن هذه النقطة نجد أن التشريعات أثمت جرائم القذف وغيرها.

2-الطائفة الثانية: المعلومات الخاصة بالمصنفات الفكرية:

يقصد بهذه المعلومات "كل عمل مبتكر أدبي أو فني أو علمي أيا كان نوعه أو طريقة التعبير عنه أو أهميته أو الغرض من تصنيفه".[1]

فهذه المعلومات يتمتع مؤلفيها بحقوق مالية وأدبية عليها. وهذه الحقوق تتمثل في حق الأبوة، حق الاستئثار بالاستغلال لهذه المعلومات أو المصنف.

ونتاج القول أن هذه المعلومات أو المصنفات الفكرية محمية بتشريعات الملكية الفكرية الأدبية والفنية والملكية الصناعية ولا يجوز التعدي عليها بأي شكل من الأشكال.

3-الطائفة الثالثة: المعلومات المتاحة أو الشاغرة:

المعلومات المباحة هي المتاحة لكافة الناس للحصول عليها ومن غير إذن، وذلك لأنها بدون مالك "Rescommunis" ومثال ذلك النشرات الجوية وتقارير البورصة. فهذه المعلومات تنقضي بالاستعمال الأول. لكن يمكن لهذه المعلومات أن تتمتع بالحماية التشريعية والجنائية في حالة قيام أحد

[1] المادة 138 فقرة أولى من القانون رقم 82 لسنة 2002 الصادر بشأن حماية الملكية الفكرية في مصر.

الأشخاص ببذل مجهود فكري وذهني في جمعها وصياغتها وذلك إعمالا لقاعدة "الجمع والصياغة" Collect-Formulation وكذلك احتراما لما يبذل من مجهود في الجمع والصياغة.[1]

ثالثا: الشروط الواجب توافرها في المعلومة محل الحماية الجنائية و طبيعتها القانونية

1: الشروط الواجب توافرها

يجب توافر شروط معنية في المعلومة لكي تتمتع هذه الأخيرة بالحماية الجنائية، وتكمن هذه الشروط فيما يلي: أن تكون المعلومة محددة ومبتكرة، وأن يتوافر فيها السرية والاستئثار، وهناك شرط آخر اتفق عليه البعض واختلف عليه البعض الآخر وهو شرط المعالجة الآلية للمعلومة.

الشرط الأول: أن تكون المعلومة محددة ومبتكرة:

قال أحد الفقهاء في تعريفه للمعلومة بأنها: "تعبير وصياغة محددة، تجعل رسالة ما قابلة للتبليغ والتبادل عن طريق علامات أو إشارات مختارة".

فوفقا لهذا التعريف فإنه يجب أن تكون المعلومة محددة précise، فإذا انعدم تحديدها تكون المعلومة منعدمة. فالمعلومة المحددة هي التي تكون محصورة في إطار معين أما عن المعلومة المبتكرة "l'Information Originale".

فيجب أن تكون المعلومة مبتكرة، أي أن تتسم بالأصالة ولم تكن موجودة من قبل. وبمفهوم المخالفة فإن المعلومة غير المبتكرة، ولا تعد معلومة بالمعنى الفني الدقيق لهذه الكلمة، أي أنها معلومة شائعة يسهل الوصول إليها من قبل أي شخص، فهي لا ترتبط بشخص معين، فهي ليست ملك لأحد.[2]

[1] رشدي محمد علي محمد عيد علي، مرجع سبق ذكره، ص.25.

[2] الدكتور محمد هلي العريان، الجرائم المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة الإسكندرية، ص.39-40.

الشرط الثاني: أن يتوافر في المعلومة السرية أو الاستئثار:

أن تكون المعلومة سرية "l'Information confidentielle": يقصد بها أن تكون محيطة بجدار من السرية أي ضرورة الاحتفاظ بهذه المعلومة في نطاق محدد من الأشخاص. أي أن تكون الرسالة التي تحملها محددة بمجموعة معينة من الأشخاص.

وبدون هذه السرية فالمعلومة تكون عامة شائعة بين الناس، وبالتالي لا تتمتع بأي حماية جنائية. فصفة السرية لازمة للمعلومة. وتكتسب المعلومة هذه الصفة أي السرية إما بإرادة الشخص باكتشاف مجال حديث، أو بحسب طبيعتها كاكتشاف شيء لم يكن معروفا من قبل، أو باجتماع الأمرين معا كالرقم السري للبطاقة الائتمانية هذا عن صحة السرية.

أما عن ضرورة توافر الاستئثار في المعلومة "l'Information exclusive": والمقصود بالاستئثار أن تكون المعلومة تخص أحد الأشخاص، بحيث يكون مستأثرا بها، فالاستئثار خاصية لا غنى عنها في مجال المعلومات حتى تستكمل المعلومة عناصرها القانونية.

وللتوضيح أكثر، إذا كان شخص معين في حوزته معلومة فهي من قبيل الأسرار الخاصة، طالما لهذا الشخص السلطة في التصرف في المعلومة التي تخصه، لذلك عندما يحدث اعتداء غير مشروع على قيم معينة، نجد أن الفاعل في هذه الحالة يستأثر بسلطة تخص الغير بصفة مطلقة. فكيف يكون للشخص الحق بالاستئثار؟

يرجع الاستئثار بالمعلومة إلى سلطة شخص ما في التصرف فيها، ويكون ذلك بناءا على رابطة بينه وبين المعلومة ويتحقق ذلك في فرضين:

الفرض الأول: في حالة المعلومات التي ينصب موضوعها على حقيقة أو واقعة معينة، فهذا النوع من المعلومات غير سري ولكنه إذا تم جمع المعلومات وحفظها، ففي هذه الحالة ينشئ لهذا الشخص الحق في الاستئثار بالمعلومة والتصرف فيها وذلك بناءا على التجميع والحفظ.[1]

الفرض الثاني: أن تتوافر رابطة بين المعلومة وصاحبها، ويحدث هذا عندما يكون موضوع هذه المعلومة فكرة أو عمل ذهني فصاحب هذه المعلومة له حق استئثاري وأي اعتداء على المعلومة من الغير يجعل صاحبها يشعر بأنه قد سرق وسلب.

خلاصة القول إذا كانت المعلومة بوصفها نتاجا لنشاط إنساني على مر العصور، إذن لابد وأن تكون هذه المعلومة من جهة محددة ومبتكرة، ومن جهة أخرى يجب أن تحتفظ بالسرية والاستئثار.

ولكن هناك البعض من الفقهاء يضيفون شرطا آخر لكي تتمتع المعلومة بالحماية الجنائية والبعض الآخر يستبعد هذا الشرط ألا وهو شرط: أن تكون المعلومة معالجة آليا.

الشرط الثالث: المعالجة الآلية للمعلومات:

يشترط بعض الفقهاء، لكي تتمتع المعلومة بالحماية الجنائية أن تكون معالجة آليا. ونقصد بالمعالجة الآلية للمعلومات، تلك العمليات المتعددة التي تتم بصفة آلية على معلومات لكي تتحول إلى معطيات عن طريق معالجتها داخل نظام آلي.

2: الطبيعة القانونية للمعلومات

انقسم الفقه الى اتجاهين هما:

[1] الدكتور رشدي محمد علي محمد عيد علي، مرجع سبق ذكره، ص.27-28.

1-الاتجاه الأول: اتجاه تقليدي: المعلومة لها طبيعة من نوع خاص:

لا يرى أنصار هذا الاتجاه في المعلومة قيمة مادية، حتى تدخل ضمن القيم المالية القابلة للتملك، فالمعلومات ذات طبيعة معنوية، وبالتالي لا تندرج في مجموعة القيم المحمية، إلا إذا كانت تنتمي للمواد الأدبية أو الفنية أو الصناعية التي تحميها حقوق الملكية الأدبية أو الفنية أو الصناعية.[1]

ويرى بعض أنصار هذا الاتجاه في المعلومة قيمة اقتصادية لا يمكن إبعادها، وعليه يمكن إدراجها ضمن نطاق الحقوق المالية دون إدراجها ضمن القيم المالية، وذلك بإدخالها ضمن طائفة المنافع والخدمات.

فالمعلومة كما يرونها وثيقة الصلة بالخدمة أو المنفعة والتي يمكن تقويمها بالمال، وهو ما قد يؤدي للخلط، ووصف المعلومة بأنها ذات قيمة مالية.[2]

وبالرغم من استبعاد المعلومة من نطاق القيم المالية، فهذا لم يمنع الفقه والقضاء الفرنسي من إسباغ الحماية القانونية عليها، سواء بالتوسع في نظرية التصرفات الطفيلية، أو بتأسيس الخطأ على نظرية الإثراء بلا سبب أو المسؤولية التقصيرية (الخطأ والضرر وعلاقة السببية).

فليس من مقتضى هذا الاستبعاد أن تظل هذه المعلومات عارية عن أية حماية إذا ما جرى الاستيلاء عليها أو استخدامها استخداما غير مشروع فهذه المسؤولية تتحرك وفق قواعد المسؤولية المدنية المستندة إلى نص المادة 1382 من ق.م.ف وبالاعتراف بالخطأ تكون المحكمة قد اعترفت بوجود الحق وهو "الحق في المعلومات" مما مؤداه أن يكون للمعلومات طبيعة خاصة تسمح بأن يكون الحق الوارد عليها من نوع الملكية العلمية.[3]

---

[1]Le système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparents, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé des données.

[2]الدكتور أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دراسة مقارنة، رسالة دكتوراه، جامعة القاهرة، كلية الحقوق، ص.12-13.

[3]الدكتور خالد ممدوح إبراهيم، مرجع سبق ذكره، ص.35.

فخلاصة القول أن هذا الاتجاه يدرج المعلومة ضمن نطاق الحقوق المالية.

2-الاتجاه الثاني: اتجاه حديث: المعلومات مجموعة من القيم:

يرى أنصار هذا الاتجاه، ومن بينهم الأستاذ CATALA، أن للمعلومة قيمة مالية أشبه بالسلعة، فهي نتاج بشري، ولكي تكون صالحه للتملك فيجب على من يحوز العناصر المكونة لها بطريقة مشروعة، أن توضع في شكل يصلح للإطلاع عليها، وتبليغها بشكل مفهوم، بغض النظر عن الوسيط المادي الذي يمكن أن يتضمنها.

ويستند الأستاذ CATALA إلى حجتين:[1]

أولهما القيمة الاقتصادية للمعلومة وإمكانية تقويمها بسعر السوق وثانيهما علاقة التبعية بين المعلومة ومؤلفها وهي العلاقة التي تربط المالك بالشيء المملوك، وهو ما يحقق ميزتين لصاحبهما هما: حقه في ضمان سرية المعلومة، والتعويض عن أي عمل غير مشروع يتعلق بها.

فقد أشار أحد الفقهاء إلى أن: "الجوهر على قدر كبير من الأهمية في مجال المنفعة الاقتصادية بالمقارنة بنظيره في مجال البيانات المادية وأنه من الواضح أن أي قانون يرفض أن يرى قيمة في شيء له أهمية اقتصادية سيبقى حتما بمعزل عن الحقيقة، ومن المقبول إذن، ووفقا لأهمية المعلومة، فإن وصف القيمة ينطبق عليها".

حيث يستخلص مما سبق، أن المعلومة تندرج تحت القيم المعلوماتية Les Biens Informationels وهذه الأخيرة غير مستحدثة، ولكنها موجودة ومخصصة من أجل إجازة الأشياء المملوكة ملكية معنوية، وأن المعلومة قيمة قائمة بذاتها بسبب خصائص حق الملكية التي تعد محلا له.[2]

[1] الدكتور أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الثانية، 2006، ص.107.

[2] الدكتور رشدي محمد علي محمد عيد علي، مرجع سبق ذكره، ص.32.

والمعلومة غير المحمية بقوانين خاصة، ولها قيمة اقتصادية أو أمنية، فإنه رغم طبيعتها المعنوية يجب علينا النظر إلى قيمتها الاقتصادية أو الأمنية، وذلك من شأنه أن يغير النظرة التقليدية إلى الأشياء في القانون الجبائي، فضلا عن أن اعتبار المعلومة قيمة في ذاتها من شأنه مسايرة التطور التكنولوجي وما يستتبعه من مخاطر الإجرام المعلوماتي، فضلا عن أن محل الحماية الجنائية أو القانونية بصفة عامة هو المصلحة وليس المال.

المبحث الثاني: الجريمة المعلوماتية و المجرم المعلوماتي

«الجريمة المعلوماتية هي:

الإبن غير الشرعي.....

الذي جاء نتيجة للتزاوج بين .....

ثورة تكنولوجيا المعلومات .....

مع العولمة.

أو هي:

المارد ..... الذي خرج من القمقم.....

ولا تستطيع العولمة أن تصرفه .....

بعد أن أحضرته ..... الممارسة السيئة لثورة تكنولوجيا المعلومات.....»[1]

الجريمة المعلوماتية جريمة حديثة نسبيا، وذلك لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات. ونتيجة لحداثة هذه الجريمة فقد كانت هناك اتجاهات مختلفة في تعريفها، كما أنها اتسمت بمجموعة من الخصائص والسمات التي ميزتها عن غيرها من الجرائم الأخرى.

كما أن هذه الجريمة المعلوماتية جلبت معها طائفة جديدة من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية.

[1] ورقة عمل مقدمة من: الدكتور محمود صالح العادلي – الجرائم المعلوماتية – ماهيتها وصورها – ص2.

المطلب الاول: ماهية الجريمة المعلوماتية وخصائصها

عصر الانترنت أو عصر السموات أو عصر التكنولوجيا الرقمية أو عصر المعلوماتية، كل هذه الأوصاف إنما تعبر عن مدى ضخامة القفزات العلمية الهائلة التي تحققت ومدى تنوع الانجازات التي طرحت ثمارها بشكل ملحوظ في حياتنا في الآونة الأخيرة.[1]

ويبدو بالفعل أن تكنولوجيا المعلومات هي وقود الثورة الصناعية الثالثة، وأن المعلومات في حد ذاتها هي المادة الخام الأساسية للإنتاج التي يعتمد المجتمع على إنتاجها وإيجادها والاستفادة منها.

وفي الواقع إن هذا الوجه المشرق لتقنية المعلومات يخل من الجانب المظلم الذي تمثل في الإجرام المعلوماتي والذي كان موجوداً ليستغل هذه التقنيات المتطورة لتحقيق مصالح ومآرب تتنوع وتتعدد.

أولا: تعريف الجريمة المعلوماتية

تمخض وتوخى عن استخدام المعلوماتية والتقنية الحديثة المتمثلة بالكمبيوتر والانترنت، الجريمة المعلوماتية أو الالكترونية والتي أشاب تعريفها كثير من الإبهام والغموض، حيث تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لهما، ولكن الفقه لم يتفق على تعريف محدد، بل أن البعض ذهب إلى ترجيح عدم وضع تعريف بحجة أن هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب الكتروني.[2]

فالجرائم المعلوماتية هي صنف جديد من الجرائم، ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين، انتقل بالجريمة من صورها التقليدية إلى أخرى الكترونية قد يصعب التعامل معها.[3]

---

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، 1429هـ- 2008م، ص 46.

[2] د. خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الطبعة 2008، ص 40- 41

[3] Pierre CATALA « la propriété de l'information » Cité par F.Toubal ;le logiciel- analyse juridique FUDUL .L.G.D.J.1986 P 126-127 .

ففي بداية ظهور هذه الجرائم كانت هناك إشكالية تواجه المختصين في كيفية مكافحتها، لأنها تتعلق بالبيانات والمعلومات، أي الكيان المنطقي للحاسب الآلي.

فنتيجة التطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات حتى الآن حال ذلك دون وضع تعريف فقهي جامع وشامل لمفهوم الجريمة المعلوماتية أو الالكترونية.

وبصيغة أخرى وكما هو شأن كل جديد، فإن استخدامات الحاسب الآلي، قد أفرزت بعض الاختلافات الجوهرية بين شراح القانون بصفة عامة، والقانون الجنائي بصفة خاصة.[1]

ومما لا شك فيه أن عدم وضع تعريف للجريمة المعلوماتية يثير العديد من المشاكل لعل أهمها، صعوبة مواجهتها وتعذر إيجاد الحلول المناسبة والملائمة لمكافحتها.

وفيما يلي سنعرض أهم آراء الفقه التي حاولت سد الفراغ التشريعي ووضع تعريف محدد للجريمة المعلوماتية على النحو التالي:

ولقد بدل الفقه جهوداً مضنية في محاولة لوضع تعريف محدد لماهية الجريمة المعلوماتية ، فانقسم الفقه بين اتجاهين، الأول يضيق من مفهوم الجريمة المعلوماتية ، والآخر يوسع من مفهومها.[2]

1- المفهوم الضيق لمفهوم الجريمة المعلوماتية:

فمن التعريفات المضيقة لمفهوم الجريمة المعلوماتية التعريف الاتي " كل فعل غير مشروع يكون بتكنولوجيا الكمبيوتر بقدر كبير لازماً لارتكابه من ناحية وملاحقته من ناحية أخرى". كما عرفها هذا الاتجاه أنها: " هي التي تقع على جهاز الكمبيوتر أو داخل نظامه فقط". وكذلك عرفها على

[1] د. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، 2004، ص 11.

[2] نهلا عبد القادر المومني/ الجرائم المعلوماتية، المرجع السابق، ص 48- 49.

أنها: " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقه ". الأستاذ Rosenblatt.

وعرفت كذلك بأنها: " غش Fraude معلوماتي ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها ". حيث يرى الأستاذ " Tredmann" "أن الجريمة المعلوماتية تشمل أي جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات ".[1]

ويرى الأستاذ "Mass" أن المقصود بالجريمة المعلوماتية " الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح".

وعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية من خلال تعريف C .C: "بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً "[2]

وكذلك عرفها "L'eslie D. Ball": " بأنها فعل إجرامي ستخدم الحاسب في ارتكابه كأداة رئيسية ".

فحسب هذه التعريفات يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة بل كذلك لملاحقتها والتحقيق فيها، وهذه التعاريف تضيق بدرجة كبيرة من الجريمة المعلوماتية وتخرج من نطاقها العديد من الأفعال غير المشروعة التي يستخدم الحاسب أداة لارتكابها.

2-المفهوم الموسع لمفهوم الجريمة المعلوماتية:

وفي المقابل فإن هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية ، فعرفها البعض على أنها: " كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال المادية أو المعنوية ".

[1] د. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الثانية، 2006، ص 84.

[2] د. محمد علي العريان، المرجع السابق، ص 44.

وتم تعريفها كذلك بأنها: " كل سلوك إجرامي يتم بمساعدة الكمبيوتر " أو هي "كل جريمة تتم في محيط أجهزة الكمبيوتر" أو هي : "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"[1].

وأعطى الخبير الأمريكي Parkerمفهوماً أو تعريفاً للجريمة المعلوماتية حيث ذكر أنها: " كل فعل إجرامي متعمد أياً كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه أو مكسب يحققه الفاعل "[2].

وهناك كذلك تعريف قريب من تعريف الخبير الأمريكي، وهو تعريف مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية OCDE، بحيث عرفتها بأنها: " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية ".

وكذلك عرفتها في سنة 1983 بقولها: " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها".هذا بخصوص منظمة التعاون الاقتصادي والتنمية.

ولقد أقر المجلس الأوروبي في التقرير الخاص بالجرائم المتعلقة بالحاسوب: بقيام المخالفة أي (الجريمة) في كل حالة يتم فيها "تغيير معطيات أو بيانات أو برامج الحاسوب أو محوها أو كتابتها أو أي تدخل آخر في مجال إنجاز البيانات أو معالجتها، وتبعاً لذلك تسبب في ضرر اقتصادي أو فقد حيازة ملكية شخص آخر، أو بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص آخر".

[1] د. خالد ممدوح إبراهيم، النرجع السابق، ص 42.

[2] تأليف عفيف كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون.

وتم كذلك تعريف الجريمة المعلوماتية بأنها: " كل سلوك سلبي أم إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأية صورة كانت ".

وكذلك من التعريفات الموسعة لمفهوم الجريمة المعلوماتية ما أتى به الفقيهان Credo وMichel من أن سوء استخدام الحاسب أو جرائم الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه وسرقة بياناته.[1]

كما تمتد جرائم الحاسب لتشمل الاعتداءات المادية، وسواء كان هذا الاعتداء على جهاز الحاسب ذاته أو المعدات المتصلة به.

وكذلك الاستخدام غير المشروع لبطاقات الائتمان، وانتهاك ماكينات الحاسبات الآلية، بما تتضمنه من شبكات تمويل الحسابات المالية بطريقة الكترونية، وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة جهاز الحاسب في حد ذاته أو مكون من مكوناته.

وإن رجعنا للفقه المصري، فهناك من يرى أن تعريف الجريمة المعلوماتية هي: " كل فعل أو امتناع عندي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداءات على الأموال المعنوية أو المادية ".

وكذلك ما جاء به في مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين فقد تبنى التعريف الآلي للجريمة المعلوماتية إنها: " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية".

[1] د. محمد علي العريان، المرجع السابق، ص 44- 45.

وما يمكن قوله عن المفهوم الواسع للجريمة المعلوماتية أنه يحيط بكل شكل من أشكال التعسف في مجال استخدام المعلوماتية معتبراً أن هذا التعسف ما هو إلا فعل خسارة ويحقق الفاعل ربحاً متعمداً.[1]

ثانيا: خصائص الجريمة المعلوماتية

إن ارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الانترنت، أضفى عليها مجموعة من الخصائص والسمات المميزة التي ميزتها عن الجرائم التقليدية ولعل من أهمها مايلي:[2]

1- الجرائم المعلوماتية جرائم ترتكب بواسطة الحاسب الآلي:

الحاسب الآلي أداة الجريمة لأنه يمكن الشخص من الدخول على شبكة الانترنت وقيامه بتنفيذ جريمته أياً كان نوعها بمعنى أن الحاسب الآلي هو الأداة الوحيدة لارتكابها أي جريمة من الجرائم التي ترتكب على شبكة الانترنت.[3]

2- الجرائم المعلوماتية جرائم ترتكب عبر شبكة الانترنت:

إن شبكة الانترنت هي حلقة الحلقة الوصول الرئيسية بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك والشركات وغيرها من الأهداف التي ما تكون غالباً الضحية لتلك الجرائم، الأمر الذي دعا معظم تلك الأهداف أن تلجأ إلى نظام الأمة الالكتروني لتحد على الأقل من خسائرها من تلك الجرائم.[4]

3- الجريمة المعلوماتية متعدية الحدود أو جريمة عابرة للدول:

[1] د. أحند خليفة الملط، المرجع السابق، ص 85.-

[2] د. خالد ممدوح إبراهيم، المرجع السابق، ص 44.

[3] http : // www. inF- te. Com/ Vb/ ihF 2548.

[4] المستشار عمرو عيسى الفقي، الجرائم المعلوماتية، المكتب الجامعي الحديث، طبعة 2006، ص 84- 85.

إن المجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود.

فبظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، لكن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أصقاع الأرض، قد انعكست على طبيعة الأعمال الإجرامية التي يعمد فيها المجرمون إلى استخدام هذه التقنيات في انتهاكاتهم للقانون، وهو ما يعني أن مساحة مسرح الجريمة المعلوماتية لم تعد محلية، أي أنها أصبحت عالمية.

هذه الطبيعة التي تتميز بها الجريمة المعلوماتية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة لحدود بشكل عام.[1]

وهذه الجريمة أي المعلوماتية هي نوع من الجرائم التي يتم ارتكابها عبر المسافات، حيث لا يتواجد الفاعل على مسرح الجريمة بل يرتكب جريمته عن بعد وهو يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة. بحيث يتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين النتيجة أي المعطيات محل الاعتداء، وبالتالي لا تقف الجريمة المعلوماتية عند الحدود الإقليمية لدولة معينة بل تمتد إلى الحدود الإقليمية لدولة أخرى مما يزيد من صعوبة اكتشافها.

[1] http://www.Shaimaatalla.Com/Vb/SHowthread.Php?t=3951.

وبالتالي هذا يثير إشكالية أخرى تتعلق بالتعارض مع سيادة الدولة وهذا التعارض مع سيادة الدول يزيد الطين بلة، بحيث يعقد من إمكانية القيام بعمل دولي مشترك للحد من جرائم تقنية المعلومات، بحيث يدفع بتلك الجهود إلى أن تتركز في الأطر القانونية لكل دولة على حدة.[1]

4- الجاني في الجرائم المعلوماتية:

قد يكون الجاني في الجرائم المعلوماتية شخصاً طبيعيا يعمل لحسابه، ويهدف إلى تحقيق مصلحة خاصة به من وراء الجريمة التي يرتكبها ضد أحد نظم المعالجة الآلية للبيانات والمعلومات، ولكن يحدث كثيراً أن يقترف الشخص الطبيعي الفعل المؤثم جنائياً ليس لحسابه الخاص، وإنما لحساب أحد الأشخاص المعنوية، كشركة عامة أو خاصة تعمل في مجال المعلوماتية، أو تعمل في مجال آخر، ولكن تقدم السطو على أنظمة المعلوماتية، أو تحدث ضرراً للغير عن طريق اللجوء لأحد نظم المعالجة الآلية للمعلومات.

5- صعوبة اكتشاف الجريمة المعلوماتية:

تتميز الجريمة المعلوماتية بصعوبة اكتشافها، وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة. فالجرائم المعلوماتية لا تحتاج إلى أي عنف أو سفك للدماء، أو آثار اقتحام لسرقة الأموال وإنما هي أرقام وبيانات تتغير أو تمحى تماماً من السجلات المخزونة في ذاكرة الحسابات الآلية.

بحيث يمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة المعلوماتية إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية هذا من جهة، ومن جهة ثانية فإن الجاني يمكنه ارتكاب هذه الجريمة في دول وقارات أخرى، لأنه كما سبق وأشرنا أن الجريمة المعلوماتية هي جريمة عابرة للحدود، بالإضافة إلى قدرة الجاني على تدمير دليل الإدانة في أقل من ثانية واحدة، فهذا يشكل عاملاً إضافياً في صعوبة اكتشاف هذا النوع من الجرائم.

[1] نهلا عبد القادر المومني، المرجع السابق، ص 51- 52.

كما أن المجني عليه، يلعب دوراً رئيسياً في صعوبة اكتشاف وقوع الجريمة المعلوماتية، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بين موظفيها عما تعرضت له، وتكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنباً للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها.[1]

6- صعوبة إثبات الجريمة المعلوماتية:

إن اكتشاف الجريمة المعلوماتية كما سبق وأشرنا ليس بالسهل ولكن حتى في حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها، فإن إثباتها أمر يحيط به كذلك الكثير من الصعاب.

فما يزيد من صعوبة إثبات هذه الجرائم هو ارتكابها عادة في الخفاء، وعدم وجود أي أثر إيجابي لما يجري خلال تنفيذها من عمليات أو أفعال إجرامية، حيث يتم بالنبضات الالكترونية نقل المعلومات، أضف إلى ذلك إحجام مجتمع الأعمال عن الإبلاغ عنها تجنباً للإساءة إلى السمعة وهز الثقة في كفاءة المنظمات والمؤسسات المجني عليها كما سبق الذكر، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الزمنية.[2]

إضافة إلى عدم ملائمة الأدلة التقليدية في القانون الجنائي في إثباتها، ومن ثم يلزم البحث عن أدلة جديدة حديثة ناتجة من ذات الحاسب، ومن هنا تبدأ صعوبات البحث عن الدليل، وتبدأ مشكلات قبوله إن وجد، ومدى موثوقيته أو مصداقيته على إثبات وقائع الجريمة.[3]

7- أعراض النخبة:

[1] د. خالد ممدوح صالح إبراهيم، المرجع السابق، ص 45- 46- 47.

[2] د. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، 2004، ص 53- 54.

[3] http : // Knol. Google. Com/k/.

الملكية الفكرية والجريمة المعلوماتية، مقالة للمؤلف محمود هيبة.

إن بعض المتخصصين يعتقدون أو يرون في تقنية الحاسبات والمعلوماتية ان من مزايا مراكزهم الوظيفية ومهاراتهم الفنية استخدام الحاسبات الآلية وبرامجها وتقنياتها لأغراض شخصية، أو للتباري الفكري فيما بينهم، أو ممارسة بعض الهوايات الدائرة في فلك هذه التقنية. وهو ما يعبر عنه أو يطلق عليه أعراض النخبة Syndrome, elitistوقد يدفع ذلك بعضهم إلى التمادي في استخدام نظم الحاسب الآلي بطريقة غير مشروعة قد تصل إلى حد ارتكاب الجرائم الخطرة.[1]

8-أسلوب ارتكاب الجريمة المعلوماتية:

تبرز ذاتية الجرائم المعلوماتية بصورة واضحة أكثر في أسلوب وطريقة ارتكابها، لأن الجرائم التقليدية تتطلب نوعاً من المجهود العضلي، وصور هذا المجهود العضلي تكمن مثلاً في ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف، وكذلك في جريمة السرقة يظهر العنف في صورة الخلع أو الكسر وتقليد المفاتيح...

ولكن على غرار ذلك فإن الجرائم المعلوماتية طبيعتها هادئة بحيث يطلق عليها Soft Crime، لا تحتاج إلى العنف فكل ما تحتاج إليه هو القدرة والتعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة.[2]

وكذلك الجرائم المعلوماتية هي بحاجة ماسة إلى وجود W.W.W. أي الانترنت، مع توافر أو وجود مجرم يوظف خبرته وقدرته على التعامل مع الشبكة للقيام بجرائم مختلفة مثلاً: التجسس، اختراق خصوصيات الغير، التغرير بالقصر، كل ذلك دون حاجة لسفك.[3]

9-خصوصية مجرمي المعلوماتية:

[1]http : //// Knol. Google. Com/k/.

محمود هيبة، مقالة عن الملكية الفكرية والجريمة المعلوماتية.

[2] نهلا عبد القادر المومني، المرجع السابق، ص 58.

[3]عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، الطبعة الثامنة، 2007، ص 32.

إن المجرم المعلوماتي يتسم بخصائص تميزه عن المجرم الذي يقترف الجرائم التقليدية أي المجرم التقليدي.

فالجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها، باعتبارها قاعدة عامة، ولكن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب الأعم، والشخص الذي يرتكبها يكون من ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب أو التعامل مع شبكة الانترنت.[1]

وكذلك في هذا السياق يمكننا التحدث عن البواعث على ارتكاب المجرم المعلوماتي هذا النوع من الإجرام المعلوماتي.

فقد تكون هذه البواعث مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي.

10- الجريمة المعلوماتية جريمة مستحدثة:

الجرائم الالكترونية أو المعلوماتية تعد منّ أبرز الجرائم الجديدة التي يمكن أن تشكل أخطاراً جسيمة في ظل العولمة، فلا غرابة أن تعتبر الجرائم المعلوماتية من الجرائم المستحدثة، بحيث أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة بحيث نجد أن هذا التقدم بقدراته وإمكانياته قد تجاوز وفاق أجهزة الدولة الرقابية، وأكثر من ذلك فإنه قد أضعف من قدرات أجهزة الدولة في تطبيق قوانينها، التي أصبحت لا تواكب هذا التطور، وبالتالي هذا الضعف والعجز أصبح يهدد أمن الدولة وأمن مواطنيها.[2]

11- قلة الإبلاغ عن وقوع الجريمة المعلوماتية:

[1] http : // www. Lawjo.Net/ Vb/ SHowthread.Php ? t= 4225

[2] د. خالد ممدوح إبراهيم، المرجع السابق، ص 51.

في معظم الأحيان لا يتم الإبلاغ عن جرائم الانترنت وذلك راجع لسببين، أولهما هو الخشية والخوف من التشهير، لذلك نجد أن معظم جرائم الانترنت تم اكتشافها بالصدفة. وأكثر من ذلك يتم اكتشافها بعد فترة طويلة من ارتكابها.

والسبب الثاني هو عدم اكتشاف المجني عليه الضحية للجريمة وزد على ذلك أن الجرائم التي حدثت ولم يتم اكتشافها هي أكثر بكثير من الجرائم التي تم كشف الستار عنها.

فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة والعدد الذي تم اكتشافه، هو رقم خطير، والفجوة كبيرة بين الجرائم المرتكب والجرائم التي تم اكتشافها.[1]

وما يمكن قوله عن خصائص الجريمة المعلوماتية أنها جريمة العالم الافتراضي، الغير ملموس، وما يميزها أكثر الشخص الذي يقوم بهذه الجريمة الذي يختلف اختلافاً جدريا عن المجرم التقليدي، فالمجرم المعلوماتي يتميز بذكائه وقدرته على التعامل مع جهاز الحاسوب والشبكة العنكبوتية، اللذان يساعدانه على ارتكاب جرائمه بدون أي جهد عضلي أي لا ضرب ولا كسر ولا سفك دماء.

فالجريمة المعلوماتية تتم بتقنيات عالية، وكذلك هناك خاصية بارزة وهي عولمة هذه الجرائم يؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم فهذه الجرائم هي صورة صادقة من صور العولمة.

المطلب الثاني: المجرم المعلوماتي

[1] نفسه، ص 51.

المعلوماتية أضافت الكثير من الجوانب الإيجابية في حياتنا إلا أنها في المقابل وفي نفس الوقت جلبت معها نسلاً جديدا من المجرمين يختلف اختلافاً جذريا عن المجرمين التقليدين، ولقد اصطلح على تسميتهم بمجرمي المعلوماتية.

فالمجرم المعلوماتي هو محور ارتكاب الجريمة في المجال المعلوماتي، وطبقا للدرجة العلمية والمستوى الثقافي والتعليمي في التعامل مع التكنولوجيا الحديثة تتحدد طبيعة المتهم، لأنه يرتكب الجريمة في حدود ما لديه من قدرات تمكنه من ارتكاب الجريمة.[1]

وتقترب سمات المجرم المعلوماتي، في كثير من الأحيان من سمات المجرمين ذوي الياقات البيضاء.[2]، بحيث أن كل هؤلاء المجرمين قد يكونوا من ذوي المناصب الرفعية المستوى ومن ذوي التخصصات والكفاءات العالية ويتمتعون بالذكاء وبالقدرة على التكيف الاجتماعي في المحيط الذي يعيشون فيه، بل وأكثرهم يتمتع بثقة عالية واحترام ممن حوله في مجال عمله أو في المحيط الاجتماعي.

وإن فكرة المجرم المعلوماتي، هي فكرة جديدة على الفقه الجنائي، كون أن المجرم ذو مهارات تقنية وذو دراية بالتكتيك المستخدم في نظام الحاسب الالكتروني.

وسوف نتناول في هذا المطلب دراسة شخصية المجرم المعلوماتي من حيث سماته الخاصة وذلك في النقطة الأولى، وأعرض بعد ذلك لأهم طوائف وفئات مجرمي المعلوماتية وذلك في النقطة الثانية، وأخيراً نلقي الضوء على أهم الدوافع التي قد تحمل المجرم المعلوماتي على ارتكاب جريمته وذلك في اخر نقطة.

أولا: السمات الخاصة بالمجرم المعلوماتي

[1] د. أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، 2005، ص 11.

[2] مصطلح المجرمين ذوي الياقات البيضاء حديث نسبيا وأول من أطلقه عالم الاجتماع Suther land، حيث وضح أم هذه الجرائم ترتكب من قبل الطبقة الراقية في المجتمع ذوي المناصب الإدارية الكبيرة ونشمل أنواعاً مختلفة من الجرائم كغسل الأموال وتجارة الرقيقا الأبيض وتزوير العلامات التجارية وغير ذلك من الجرائم التي يقومون بارتكابها وهم جالسون في مكاتبهم الفخمة.
www. Minshawi. Com/ old/ intern et crime- in 20% law- htm.

إن مرتكبي جرائم المعلوماتية من الأفراد ذوي المهارات الفنية والتقنية العالية، والموظفين ذوي الياقات البيضاء، ويطلق على المجرم المعلوماتي أو مجرم الانترنت المتميز مصطلح الهاكر Haker أو Haking، ويقصد به مخترق شبكات الحاسب.[1]

والفضل في الكشف عن هذا المصطلح يرجع إلى كاتب الخيال العلمي الأمريكي " **وليم جيبسون ""w. Gibson"**، في مؤلفه the new- romancer الذي صدر سنة 1984، والذي ذكر فيه المجرم التقني، في حين أن هذا المصطلح كان يطلق قبل ذلك على الأشخاص الذين يملكون قدرات عالية المستوى في البرمجة، والذين يتميزون بقدرات إبداعية في معهد ماسشوستس للتكنولوجيا، وكذلك المبرمجين المبدعين في جامعة ستانفورد وجامعة Berkeley.

وكما سبق الذكر فإن فكرة المجرم المعلوماتي، فكرة جديدة على الفقه الجنائي، ففي جرائم الحاسوب والانترنت لسنا بصدد سارق أو محتال عادي ولكن نحن بصدد مجرم ذو مهارات تقنية ودراية بالتكتيك المستخدم في نظام الحاسوب، فهذه المهارات تمكنه من اختراق الكود السري لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق استخدام الحاسوب.[2]

فهذا المجرم قد ترك عالم المجرمين البؤساء ليدخل إلى عالم مجرمي المهارات المعلوماتية، فشخصية المجرم ميكانيكية لارتكابه للجريمة له سماته الخاصة بهذا النوع الجديد من الإجرام، تميزه عن غيره من المجرمين التقليديين وتتمثل هذه السمات في:

1- المجرم المعلوماتي يتمتع بالمهرة والمعرفة والذكاء:

[1] رشدي محمد علي محمد علي، الحماية الجنائية للمعلومات على شبكة الانترنت، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، 2009، ص 70-71.

[2] كوثر مازوني، الشبكة الرقمية وعلاقتها بالملكية الفكرية، مذكرة مجستير، كلية الحقوق جامعة بن عكنون الجزائر، 2004- 2005، ص112.

إن مجرموا المعلوماتية يتمتعون بقدر لا يستهان به من المعارة والمعرفة بتقنيات الحاسوب والانترنت. بل وأكثر من ذلك أن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آليا.[1]

فالمجرم المعلوماتي يتمتع باحترافية كبيرة في تنفيذ جرائمه، حيث أنه يرتكب هذه الجرائم عن طريق الكمبيوتر الأمر يقتضي الكثير من الدقة والتخصص والاحترافية في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية.[2]

والذكاء يعتبر من أهم صفات مرتكب الجرائم المعلوماتية، لأن ذلك يتطلب منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي والقدرة على التعديل والتغيير في البرامج وارتكاب جرائم السرقة والنصب وغيرها من الجرائم التي تتطلب أن يكون مرتكب الجريمة على درجة كبيرة من المعرفة لكي يتمكن من ارتكاب تلك الجرائم.[3]

والمجرم المعلوماتي يمكن أن يكون تصوراً كاملاً لجريمته قبل أن يقوم بتنفيذها. كيف ذلك؟

فالفاعل أو المجرم باستطاعته أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ الجريمة. وهذا بغرض أن لا يفاجأ بأمور غير متوقعة من شأنها إفشال مخططاته أو الكشف عنها.[4]

وما يمكن قوله عن المجرم المعلوماتي أنه بذكائه يقوم بارتكاب جرائمه دون استخدام العنف أو الإتلاف المادي، بل يحاول أن يحقق أهدافه بكل هدوء مستعيناً في ذلك بمقدرته العقلية. والمثال الذي

[1]Sutherland (Edwin H.) "White collar criminality " Gers (Gilbert) in white collar criminal The offender in business the professions atherton press 1968

[2]http : // ar. Wikipedia. Org/ wiki/.

[3] د. أيمن عبد الحفيظ، المرجع السابق، ص 13.

[4] نهلا عبد القادر المومني، المرجع السابق، ص 77.

يصاغ في هذا الحديث أنه جاء في حيثيات أحد الأحكام الصادرة عن إحدى المحاكم في الولايات المتحدة الأمريكية ضد أحد الأشخاص بسبب قيامه بممارسة النصب المعلوماتي عن طريق اختراق نظم حاسب مؤسسة لكروت الائتمان، إن المتهم ويدعى Justin Tanner Petersen، يمتلك معرفة ومهارة غير عادية في كيفية عمل الحاسبات الآلية، وكيفية تخزين البيانات والحركة الاسترادادية للمعلومة، وكيف يمكن التحكم في النظام الأمني للحاسبات أو تجنب التعامل معه.

فالذكاء الغير العادي الذي يتمتع به المجرم هو الذي يساعده على ارتكاب جرائمه ضد نظم المعلومات، وإتلاف الحاسب، أو الدعائم الممغنطة عن طريق استخدام تقنيات التدمير الناعمة ومن أمثلتها ما يعرف بالقنابل المنطقية.

فالإجرام المعلوماتي هو إجرام الذكاء كما يصرحون ولا يحتاج إلى استخدام العنف والقوة، وعادة هذه الجرائم المستحدثة تكون بين الفئة العمرية 18- 45 عاماً، وهذه الفئة يكون لها المهارة والإلمام الكامل والقدرة الفنية الهائلة في مجال نظم المعلومات، فمجرمي تلك المعلومات هم من طبقة المتعلمين والمثقفين ومن لديهم تخصص في التعامل مع أجهزة الحاسب الآلي، والقدرة على اختراق التحصينات والدفاعات التي تعدها شركات البرمجة، فقد يهدف المجرم المعلوماتي من جريمته إلى تحقيق مكاسب مادية معينة أو إثبات مهارته الفنية وقدرته على اختراق أجهزة الحاسب، وقد يرتكب مجرمو هذه الفئة جرائمهم بهدف التسلية أو الترفيه أو لمجرد الرغبة في إضرار الغير.[1]

2-المجرم المعلوماتي إنسان اجتماعي بطبعه "متكيف اجتماعياً":

[1]http : // www. Zinj- org/ Forum/ SHowthread.Php ? t = 2821.
صفات المجرم المعلوماتي- شبكة الزنج الإسلامية.

إن المجرم المعلوماتي لا يضع نفسه في حالة عداء سافر مع المجتمع، الذي يحيط به، بل أنه إنسان متكيف اجتماعياً.[1]

وهنا يمكن الاختلاف بين الإجرام المعلوماتي والإجرام التقليدي من حيث أن المجرم المعلوماتي في هذا الشأن يحيا وسط المجتمع ويمارس عمله في المجال المعلوماتي أو غيره من المجالات الأخرى.[2]

فهذا المجرم أصلاً مرتفع الذكاء كما ذكرنا سلفاً، وذكاءه هذا يساعده على التكيف مع المجتمع، ولا نعني بذلك التقليل من شأن م.م.، بل أن خطورته الإجرامية قد تزيد إذا زاد تكيفه الاجتماعي هذا مع توافر الشخصية لديه.[3]

ويتكيف المجرم مع مجتمعه يعطيه أو يزيده ثقة بأنه خارج إطار الشبهات وهذا الشعور يدفعه إلى التمادي في ارتكاب جرائمه التي قد لا تكتشف، وإذا اكتشفت فإنها تواجه صعوبة الإثبات ونقص الأدلة ونقص الخبرة لدى المحققين ولدى رجال القضاء.[4]

3- المجرم المعلوماتي يبرز ارتكاب جريمته:

يوجد شعور لدى مرتكب فعل الإجرام المعلوماتي أن ما يقوم به لا يدخل في عداد الجرائم المعاقب عليها، أو بمعنى آخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف السلوك عند قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، فهؤلاء الأشخاص لا يدركون أن سلوكهم يستحق العقاب.[5]

---

[1] د. المستشار عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، 2006، ص86.

[2] PARKER (DonnB) l'ouvrage précédent P144-146.

[3] محمد علي العريان، المرجع السابق، ص 86.

[4] نهلا عبد القادر المومني، المرجع السابق، ص 79.

[5] http : // www. Omanlega/ net/ journal/ ? p = 133.

الجرائم الإفتراضية وجهود سلطنة عمان التشريعية في مواجهتاه، مجلة عمان القانونية.

وفي هذا الصدد يقول الأستاذ "باركر" وهو أحد أهم الباحثين الذين عنوا بالجريمة المعلوماتية بشكل عام وبالمجرم المعلوماتي بصفة خاصة: " أن الفاعل في هذه الجرائم لا يتصور أن سلوكه يمكن أن يتصف بالإجرامي وأن يستتبع ذلك توقيع العقاب عليه. فمن خلال لقائه باثنين من المحكوم عليهم بسبب استعمال الحواسيب الخاصة برؤسائهم لأغراض شخصية وهو ما يندرج تحت جريمة الاستعمال غير المصرح به للنظام المعلوماتي، ذكر المتهمان أن ما فعلاه هو سلوك شائع ومقبول في نالمؤسسة التي يعملان بها وأن العاملين في المؤسسة يقومون باستخدام النظام لأغراض شخصية بعضها لتحقيق ربح مادي والبعض الآخر لمجرد التسلية في أوقات الفراغ".

4- خوف المجرم المعلوماتي من كشف جريمته:

يتصف مرتكبوا هذه الفئة من الجرائم بالخوف من كشف جرائمهم وافتضاح أمرهم وبالرغم من أن هذه الخشية تصاحب المجرمين على اختلاف أنماطهم، إلا أنها تميز مجرمي هذه الفئة من الجرائم بصفة خاصة لما يترتب على كشف أمرهم من ارتباك مالي وفقد المركز الوظيفي في كثير من الأحيان، وهذا الخوف لديهم مرده انتماؤهم في الغالب الأعم إلى وسط اجتماعي متميز سواء من حيث التعليم أو الثقة أو المستوى المهني وطبيعة العمل.[1]

5- المجرم المعلوماتي مجرم عائد للإجرام:

المجرم المعلوماتي يتميز بأنه يعود للجريمة دائماً، فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات، فهو قد لا يحقق جريمة الاختراق بهدف الإيذاء وإنما نتيجة شعوره بقدرته ومهارته في الاختراق.[2]

[1] نهلا عبد القادر المومني، المرجع السابق، ص 79.

[2] د. محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتاه، مركز الإعلام الأمني، وزارة الداخلية، الأكاديمية الملكية للشرطة.
www.policemc. Giv.Bh/ reports/ 2011/ april/ 1- 4…

6-المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي:

المقصود بالسلطة هنا الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته.

فأغلبية مجرمي المعلوماتية تكون لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة وتتمثل هذه السلطة مثلاً في الشيفرة الخاصة بالدخول أو الولوج إلى النظام الذي يحتوي على المعلومات. وهذه الشيفرة تعطي للمجرم المعلوماتي مزايا متعددة تمكنه مثلاً من فتح الملفات وقراءتها أو كتابتها، أو محو المعلومات، أو تعديلها أو أي فعل آخر مجرم.

فما يمكن قوله عن السلطة أنها الحق في استعمال الأنظمة المعلوماتية أو حتى مجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة.[1]

ثانيا: فئات مجرمي المعلوماتية

أسلفنا في ما مضى أن ظهور شبكة الانترنت وانتشارها الواسع والكبير أفرز أنماطاً مستحدثة من الظواهر الإجرامية، وبالتالي كان من الطبيعي أن تحمل ظاهرة الإجرام عبر شبكة الانترنت في جنباتها ولادة طائفة جديدة من المجرمين عرفت باسم مجرمي الانترنت.

وعلى الرغم من أنه حتى الآن لم تتضح الصورة جلياً في تحديد صفاتهم واستظهار سماتهم وضبط دوافعهم نظراً لقلة الدراسات الخاصة بهذه الظاهرة من جهة ولصعوبة الإلمام بمداها الحقيقي من جهة ثانية والتغير السريع الحاصل في نطاقها والمرتبط أساساً بالشارع الدهيب في ميدان الكمبيوتر والانترنت من جهة ثالثة.

[1] نهلا عبد القادر المومني، المرجع السابق، ص 81.

فالمزيد من الوسائل والمخترعات يعني المزيد من التغير في أنماط الجريمة ووسائل الاعتداء وهذا بدوره يساهم في إحداث تغير على السمات التي يتصف بها مجرمي الانترنت.[1]

ومع ذلك يمكن أن نصنف مجرمي الانترنت إلى فئتين:

الفئة الأول: فئة الهواة Hackers.

الفئة الثانية: فئة المحترفين Crackers.

1-الفئة الأولى: فئة الهواة Hackers: أو كما يطلق عليهم " صغار نوابغ المعلوماتية"

وهم الأشخاص الذين لهم القدرة الفائقة على اختراق الأجهزة والشبكات أيا كانت إجراءات وبرامج وتدابير الحامية التي تم اتخاذها إلا أنهم لا يقومون بأي من الإجراءات التي تؤدي من تم اختراق جهاز أو شبكته.[2]

ويقصد " بالهاكر " كذلك الشباب البالغ المفتون بالمعلوماتية والحاسب الآلي، الذين لديهم قدرة فائقة على اختراق الشبكات والإبحار في عالم البيانات، دون أهمية لحواجز كلمات المرور أو الشفرات، ولكن أهم ما يميز هذه الفئة أو الطائفة هو عدم وجود نية أو قصد لإتلاف المعلومات أو تخريب أنظمة الحاسب وشبكات الاتصال، ولكن هدفهم هو الاستكشاف والبحث عن الجديد في هذا العالم الخيالي. والميل إلى المغامرة والتحدي، ونادراً ما تكون أفعالهم المحضورة غير شريفة. والسبب في ذلك هو أنهم لا يقدرون النتائج المحتملة، والتي يمكن أن تؤدي إليها أفعالهم غير المشروعة بالنسبة لنشاط إحدى المنشآت أو الشركات التجارية. ويقومون بذلك بهدف كسب الخبرة، أو بدافع الفضول، أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.[3]

---

[1] http : // www. inF- te. Com/ vb/ inF 2548.

جرائم الانترنت، كلية الحاسوب وتكنولوجيا المعلومات.

[2] المؤلفان منير محمد الجنبيهي- ممدوح محمد الجنبيهي، أمن المعلومات الالكترونية، دار الفكر الجامعي، 206، ص 28.

[3] رشدي محمد علي محمد عيد علي، المرجع السابق، ص 74.

فهناك فرق بين الفرد الذي يدخل نظام حاسب بدون نية إجرامية وبين من يدخل بنية استخدام الحاسوب في اختلاس أموال خاصة بعميل في مؤسسة بنكية.

ونسرد المثال التالي عن الهاكرز، فقد ضايق الهاكرز الجيش الأمريكي عندما تصاعدت الأزمة الأخيرة في الخليج.[1] حيث أعلن نائب وزير الدفاع الأمريكي بأن الهاكرز استطاعوا الدخول إلى مناطق محظورة واستطاعوا تثبيت مفاتيح كي تمكنهم من الوصول للمعلومات في وقت لاحق.

بحيث أعلن مكتب التحقيق الفيدرالي بأن مخترقي أنظمة الكمبيوتر هم الأكثر خطورة على الولايات المتحدة، وأن أمريكا تواجه تهديدات كبيرة بسبب الهجوم على بنيتها الالكترونية. مما سبب خطأ أكبر حتى من أي مواجهة محتملة.

وقال رئيس المركز الوطني لحماية البنية التحتية في أمريكا وهو المخول إليه الحماية من التجسس الالكتروني، بأن خارقي أنظمة الكمبيوتر يرون في نظام دفاع حكومة الولايات المتحدة هو الإمتحان الأخير وأقصى تحدي لاختبار مهاراتهم، وأضاف بأن كثير من الحوادث كان السبب فيها هم الشباب الصغار وهؤلاء كان أثر اختراقهم تافه، ولكن حذر من الأعداء ذوو المهارات العالية لأن عملهم خطيراً.

وتأسيس مركز حماية التجسس الالكتروني خصيصاً كي يحقق في التهديدات الموجهة للبنية الأساسية الالكترونية، وهي بنية تحتية ذات حساسية هامة، حيث تشمل الاتصالات ومؤسسات المنافع العامة والشبكات المالية، وجميع هذه المؤسسات قابلة أن تكون ضحية تهديدات عن طريق الدخول إليها بالكمبيوتر وقال بأن العدو في هذه الحالة لا يحتاج للسفر آلاف الأميال حتى يهاجمنا أو يحمل أطنان القنابل ويغامر حتى يصل إلينا.[2]

[1] المؤلفان منير محمد الجنبيهي- ممدوح محمد الجنبيهي، المرجع السابق، ص 32- 33.

[2] منير محمد الجنبيهي- ممدوح محمد الجنبيهي، المرجع الاسبق، ص 34.

وبينت الإحصائيات أن أكبر 560 شركة تعتمد على الانترنت في أعمالها، وأن أكثر من نصفها أقروا بأنهم هوجموا بواسطة الهاكرز وأن أكثر من ثلاثة أرباع الذين هوجموا بواسطة الهاكرز قد هوجموا داخليا. ومن أمثلة الجرائم المعلوماتية التي ارتكبها ضغار نوابغ المعلوماتية الجريمة التالية:

ففي ألماني تمكن احد الطلبة الذي يبلغ من العمر 19 سنة، من نسخ وإفشاؤ بيانات حاسب آلي على نحو غير مصرح به، وأدى فعله هذا الغير مشروع إلى التسبب بخسارة هذه الصناعة في ألمانيا بمبلغ 23 ألف مارك ألماني واستفاد الطالب الجاني بمبلغ قدره 26 ألف مارك ألماني.[1]

وهناك أمثلة كثيرة عن اختراقات هؤلاء صغار نوابغ المعلوماتية لنظم المعلومات منها ما كشفت ومنها لا تزال غامضة.

ومن أشهر الجرائم التي ارتكبت في الولايات المتحدة الأمريكية جريمة اقترفها مراهق يبلغ من العمر 17 سنة، يدعى " دينيس موران" فهذه القضية تحولت إلى قضية رأي عام وذلك بسبب اختلافها عن الجرائم الأخرى فيما كبدته من خسائر. وأطلق على نفسه " دينيس موران " اسما حركياً هو "كوليو".

وقد قام هذا الأخير بشن سلسلة من الهجمات الالكترونية على مواقع مهمة أنشأتها الحكومة الأمريكية على شبكة الانترنت، ومنذ نهاية سنة 1999 وحتى بداية 2000 تمكن "كوليو" من أن يحول حياة المسؤولين عن هذه المواقع إلى الجحيم.[2]

فلقد هاجم موقع "Dare org" المسؤول عن مواجهة مخاطر الإدمان ونفد عمليات تخريبية عليها بحيث قام " كوليوا" باستغلال صورة منشورة على الموقع لفأر كان قد تعرض لتأثير نبات الماريجوانا المخدر وكتب أسفلها "ما أحلى المخدرات".

[1] د. المستشار عبد الفتاح بيومي حجازي، المرجع السابق، ص 90.

[2] د. أيمن عبد الحفيظ، المرجع السابق، ص 25.

ثم قام بنفس الشيء مرة أخرى وعلى نفس الموقع، حيث أدخل صورة لشخصية والت ديزني الشهيرة (دونالد داك) وهو يحقن نفسه بمادة مخدرة.

وجاء في تعليق للمسؤولين عن إدارة الموقع، بحيث صرحوا بأن "كوليو" حول موقع مكافحة الإدمان إلى موقع يشجع على تعاطي المخدرات. وهذا كله بفضل الصور والرسوم التي أدخلها على الموقع.

وشهدت سنة 1984 ما سمى بحرب الهاكرز العظمى، بحيث تم تكوين مجموعة من الهاكرز والهواة أطلقت على نفسها اسم "LOD" فهذه المجموعة تعد من أذكى المجموعات الموجودة في ذلك الوقت، وفي المقابل نشأت مجموعة أخرى كانت بزعامة شخص يدعى فيبر، وأطلق على مجموعته اسم "MOD"، وكانت هذه الأخيرة منافساً للمجموعة الأولى.

ومن أشهر الجرائم التي ارتكبت في الولايات المتحدة الأمريكية جريمة اقترفها مراهقا يبلغ من العمر 17 سنة، يدعى "دينيس موران". فهذه القضية تحولت إلى قضية رأي عام وذلك بسبب اختلافها عن الجرائم الأخرى فيما كبدته من خسائر. وأطلق على نفسه دينيس موران اسما حركيا هو "كوليو".

وقد قام هذا الأخير بشن سلسلة من الهجمات الإلكترونية على مواقع مهمة أنشأتها الحكومة الأمريكية على شبكة الأنترنت، ومنذ نهاية سنة 1999 وحتى بداية سنة 2000 تمكن "كوليو" من أن يحول حياة المسؤولين عن هذه المواقع إلى الجحيم.[1]

فلقد هاجم موقع "Dareorg" المسؤول عن مواجهة مخاطر الإدمان ونفذ عمليات تخريبية عليه بحيث قام "كوليو" باستغلال صورة منشورة على الموقوع لفأر كان قد تعغرض لتأثير نبات الماريجوانا المخدر وكتب أسفلها: "ما أحلى المخدرات".

[1] دكتور أيمن عبد الحفيظ، المرجع السابق، ص.25.

ثم قام بنفس الشيء مرة أخرى وعلى نفس الموقع، حيث أدخل صورة لشخصية والت ديزني الشهيرة (دونالد داك) وهو يحقن نفسه بمادة مخدرة.

وجاء في تعليق للمسؤولين عن إدارة الموقع، بحيث صرحوا بأن "كوليو" حول موقع مكافحة الإدمان إلى موقع يشجع على تعاطي المخدرات وهذا كله بفضل الصور والرسوم التي أدخلها على الموقع.

وشهدت سنة 1984 ما سمي بحرب الهاكرز العظمى، بحيث تم تكوين مجموعة من الهاكرز والهواة أطلقت على نفسها اسم "LOD" فهذه المجموعة تعد من أذكى المجموعات الموجودة في ذلك الوقت، وفي المقابل نشأت مجموعة أخرى كانت بزعامة شخص يدعى فيبر، وأطلق على مجموعته اسم "MOD"، وكانت هذه الأخيرة منافسا للمجموعة الأولى.

وفي بداية التسعينات اشتعلت الحرب بينهم وسميت حرب الهاكرز العظمى، وهذه الحرب كانت عبارة عن محاولات كل طرف من المجموعتين اختراق أجهزة الطرف الآخر.

واستمرت هذه الحرب قرابة 4 أعوام وانتهت بإلقاء القبض على رئيس مجموعة "MOD" والمسمى فيبر.

وبعد هذه الحادثة ظهرت مجموعات عديدة من الهاكرز.[1]

ونسرد مثال آخر عن الهاكرز، بحيث تمكنت مجموعة من طلبة المدارس العليا بالولايات المتحدة الأمريكية وتتراوح أعمارهم بين 15 و25 سنة يطلقون على أنفسهم اسم المجموعة "414"، باختراق أنظمة نحو 60 حاسبا عام 1983. ومن بينها: حاسبات وبنوك معلومات مختبر في "لوس أنجلس"، وأيضا مركز Salan Kottering لعلاج الأورام في نيويورك. وكذلك معهد ماساشوسيتي

[1] http://www.cpsr.org/cpsr/privavy/crime/denning.hackers.html/P:3.

للتقنية، وقاعدة ماك كليلان للقوات الجوية، وإدارة التليفونات بالنرويج، كل هذه الاختراقات تمت عن طريق استخدام موديمات وبعض المعلومات حول طرق الاتصال البصري.[1]

وأمامنا مشكلة، وهي التخوف من تحول الحدث الصغير من مجردها وصغير للأفعال غير المشروعة إلى محترف لأعمال السلب.

وهناك خطر آخر يجب الحذر منه، وهو استغلال المنظمات الغير المشوعة لهؤلاء الهواة، وذلك بتجنيدهم لصالحهم، وهنا يكون الخطر أكبر، ونكون بصدد مواجهة منظمات إجرامية ليس فقط هواة مخترقين للنظم والشبكات.

فأمام المشرع خطوة كبيرة ومختلفة، وهي خلق علاج لهؤلاء الصغار الهواة قبل معاقبتهم، لأن العقاب لا يكون دوما رادعا، فلذا يجب التوصل إلى علاج.

الهاكرز إرهابيون حسب التصنيف الأمريكي الجديد للإرهاب:[2]

حذرت جمعية الحريات المدنية من مشروع قانون أمريكي تقترحه الإدارة الأمريكية يعتبر المتسللين إلى البرامج الكمبيوترية، المعروفين بالهاكرز، إرهابيين، وقد أضاف مشروع القانون الجديد مخالفات التسلل إلى برامج الكمبيوتر إلى قائمة الجرائم الإرهابية، وقد تصل عقوبة هذه الجرائم إلى السجن مدة الحياة. ويقول شاري ستيل، مدير مؤسسة إليكترونك فرونتير، وهي جمعية تدافع عن الحريات المدنية في سان فرانسيسكو، إن اعتبار جرائم الكمبيوتر الصغيرة جرائم إرهابية لا يعتبر ردا مناسبا على الأحداث الأخيرة. وقد تقدم بمشروع القانون الجديد، الذي سيوسع من سلطات متابعة الإرهابيين ومعاقبتهم، وزير العدل الأمريكي جون آشكروفت، إثر الهجمات الإرهابية على نيويرك وواشنطن في الحادي عشر من سبتمبر/أيلول الجاري. وبالإضافة إلى جعل التسلل الكمبيوتري جريمة

[1] الدكتور المستشار عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الطبعة الأولى سنة 2006، مرجع سبق ذكره، ص.91.

[2] الجزيرة BBC أون لاين.

إرهابية، فإن القانون سيحدد عقوبات تصل إلى السجن مدة الحياة، ويوسع من صلاحيات الاحتجاز والمصادرة قبل الإدانة، بالإضافة إلى إشراك من يساعد المتسللين أو يؤويهم في الجريمة. حتى وإن كانت الأضرار الناتجة عن التسلل ضمن الحد الأدنى.

ويقول ستيل إنه يجب أن لا يعاقب التسلل، الذي لم يحدث ضررا كبيرا بالسجن بأي حال من الأحوال. ويطبق القانون بأثر رجعي على الجرائم الإرهابية، مما يعني أنه سيؤثر على المتسللين ومصممي برامج الفيروس السابقين، الذين لم يكن القانون ليعاقبهم بأكثر من تحذير أو عقوبة طفيفة، وتشعر جمعيات الحقوق المدنية بالقلق من أن مشروع القانون هذا ربما اقترح باستعجال ودون بحث تأثيراته على الأمن والحريات الشخصية، وتقول لورا ميرفي، من اتحاد جمعيات الحريات المدنية إن على الكونجرس أن يتخذ الإجراءات الكفيلة بحماية البلاد من الهجمات المستقبلية. وأضافت أن الأمريكيين يقيمون الحريات المدنية كثيرا وهي الآن أصبحت في خطر، ودعت الكونجرس إلى التثريب قليلا، وقد حذر المسؤولون والأكاديميون من أن التسلل التخريبي إلى الأنترنت سيكون جزءا من حرب خطيرة ضد الولايات المتحدة. وقال تقرير حديث لمعهد دراسات الأمن والتكنولوجيا أن معظم التسللات السابقة التي لها علاقة بالسياسة كانت تسللات تهدف الإزعاج وليس الضرر، وإن من غير المرجح أن تنتج مثل هذه التسللات عن عمل عسكري أمريكي. ويضيف التقرير أن الاحتمال قائم بأن يحصل تسلل مدمر ردا على أي عمل تقوم به الولايات المتحدة انتقاما من منفذي الهجوم الإرهابي في الحادي عشر من سبتمبر/أيلول الجاري، وإن مثل هذا التسلل الخطير لابد أن يزعزع شبكات المعلومات في الولايات المتحدة وحلفائها الأوروبيين ويقول مؤيدوا قانون مكافحة الإرهاب الجديد إن القانون لا يستهدف المتسللين الشباب.

2- الفئة الثانية: فئة المحترفين أو المخترقين Crakers

المحترفون في الجرائم المعلوماتية تتراوح أعمارهم من 25 إلى 45 سنة.[1]

ويقصد بهم فئة المخترقون ذوي النوايا الإجرامية في الإتلاف أو التخريب، باستخدام الفيروسات أو القنابل المنطقية، وهم يتميزون بأنهم من أصحاب التخصصات العالية، ولهم الهيمنة الكاملة على تقنيات الحاسب وشبكات المعلوماتية، وهم يمثلون التهديدات المباشرة للأنشطة والمصالح عبر شبكة الأنترنت.[2]

وهذا الصنف هو أكثر خطورة من الصنف الأول وقد يحدثون أضرارا كبيرة، وقد يؤلفون أندية لتبادل المعلومات فيما بينهم. فيفضل القراصنة العمل عادة في جماعات عن العمل الفردي، وغالبا ما يكون دافعهم لارتكاب الجريمة، إما الحصول على المال أو بغرض الشهرة أو إثبات تفوقهم العلمي ومدى ما يتمتعون به من ذكاء.[3]

فيرى الهاكرز أن رجال الشرطة والضبط القضائي بالنسبة لهم من فئة –الضعفاء–، لذلك يتعين تأصيل رجال الضبط القضائي وأداء العدالة لمواجهة مثل هذه النوعية من المجرمين.

فهذه الفئة تنعكس اعتداءاتهم وميولهم الإجرامي والرغبة في التخزين لأي دافع كان حيث يستخدمون برامج وتقنيات لاختراق الأنظمة والحصول على المعلومات التي يريدونها، ونسخها أو الإضافة عليها أو الحذف منها وقد تحولت أساليبهم إلى تصميم الفيروسات وذلك يشكل خطرا بالغا رغم عدم الاستفادة من تصميم الفيروس عدا حب التخريب أحيانا أو لأهداف شخصية فمنهم من يعمل في مجال الأنظمة المعلوماتية ويكون محل ثقة تجعل عملية ارتكابه للجريمة سهلا نظرا لعلاقة الوظيفة بخبراته ومهاراته ونظرا للثقة التي يتمتع بها، وقد يكون الدافع لذلك الانتقام من فرد أو منظمة وهذه العينية يسميهم البعض "فئة مجرمي المعلومات الحاقدين".

[1] الدكتور محمد علي العريان، المرجع السابق، ص.64.

[2] رشدي محمد علي محمد عيد علي، المرجع السابق، ص.74.

[3] شمسان ناجي صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الأنترنت، رسالة ماجستير، معهد البحوث والدراسات العربية.

كما أن هناك منظمات غير قانونية من هذه الفئة يقومون بعمليات مثل غسيل الأموال والتجارة في الأعضاء البشرية متلبسين بمواقع خاصة فيما يتناسب مع طبيعة أنشطتهم المتعددة عابرة الحدود وهذا نتيجة لضعف العقوبات التي تطبق على مرتكبي هذا النوع من الجرائم.[1]

بالإضافة إلى الفئتين السابقتين الهاكرز والكراكرز يمكن إضافة فئات أخرى وهم من فئة القراصنة "les pirates" :

أ- فئة المخادعون "Fraudeurs":

وهؤلاء يتمتعون بقدرات فنية عالية باعتبارهم عادة من الأخصائيين في المعلوماتية ومن أصحاب الكفاءات، وتنصب معظم جرائمهم على شبكات تحويل الأموال ويمكنهم التلاعب بحسابات المصارف أو فواتير الكهرباء والهاتف أو تزوير بطاقات الاعتماد أو ما شابه.[2]

ب- فئة الجواسيس "Espions":

يهدف هؤلاء إلى جمع المعلومات لمصلحة دولهم أو لمصلحة بعض الأشخاص أو الشركات التي تتنافس فيما بينها.

ثالثا: الأسباب الدافعة لارتكاب الجرائم المعلوماتية

تختلف الدوافع والبواعث إلى ارتكاب الجرائم المعلوماتية تبعا لطبيعة المجرم ومدى ثقافته وخبرته في مجال الحاسب الآلي لأن المتهم يرتكب جريمة بناءا على ما لديه من مهارة وخبرة.

فهدف المتهم ذو الخبرة في مجال البرمجة واستخدام شبكات الحاسب الآلي يختلف عن هدف المتهم الذي لا تتعدى خبرته مجرد تشغيل جهاز الحاسب الآلي هذا من جهة.

[1] http://kenanaonline.com/users/ahmedkordy/topics/99029/posts/323485.
الكاتب: عبد الله محمد آل عدينال، الاحتيال المعلوماتي.

[2] www.osamabahar.com

ومن جهة أخرى فإن المحترف لن يقدم على فعلته ما لم يوجد الدافع لتحقيق غرضه، وبسبب عدم كمال العقل البشري فإنه من المستحيل تجنب الخطأ أو منع وصول المجرمين إلى مواضيع هي عرضة للخطر واستغلال المهاجمين من الثغرات هي من أهم دوافع اختراق أنظمة الحواسيب وغيرها من التقنيات وكما إن انعدام الخبرة لدى المستخدمين يعد من أكبر الأسباب التي أفشت هذه الكارثة وأيا كان السبب من وراء هذه الجرائم إلا أنها تختلف دوافعها ومن أهمها:[1]

1- تحقيق المكسب المادي:

مرتكب الجرائم المعلوماتية يقوم بما لديه من خبرة ومهارة في المجال التكنولوجي بتوجيه هذه الإمكانيات نحو المؤسسات المالية لمحاولة تحقيق المكاسب المادية، وذلك إما بسرقة تلك الأموال أو بتحويلها لحسابه الشخصي داخل البنك، بحيث يستطيع المتهم بمجرد دخوله على أنظمة البنوك معرفة أرقام الحاسب وسرقتها أو تحويلها، ويتم كذلك عن طريق استخدام كارت الفيزا أو الماستركارت البيع والشراء عبر شبكة الاتصالات الدولية من خلال سرقة تلك الأرقام باستخدام شبكة المعلومات.[2]

بحيث أشارت مجلة "Sécurité Informatique" وهي مجلة متخصصة في الأمن المعلوماتي أن 43% من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال.

و23% من أجل سرقة معلومات و19%أفعال إتلاف و15%سرقة وقت الآلة أي الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية.

ويمكن توضيح مدى الأرباح المادية التي يحققها المجرم نتيجة لاقتراضه هذا النوع من الإجرام من خلال ما رواه هؤلاء المجرمين المحترفين في سجن كاليفورنيا، حيث قال: "لقد سرقت أكثر من نصف مليون دولار بفضل أجهزة حاسوب جهاز الضرائب في الولايات المتحدة الأمريكية وبإمكاني

[1] http://coeria.edu.sa/index.php/ar/assurance-awamess/articles/51-forensic-and-computer-crimes/987-tupes-of-electronic-crime-and-regulations-in-force-in-saudi-arabia.html.

[2] دكتور أيمن عبد الحفيظ، مرجع سبق ذكره، ص.18.

أن أكرر ذلك في أي وقت لقد كان شيئا سهلا فأنا أعرف أسلوب عمل جهاز الحاسوب للضرائب وقد وجدت ثغرات كثيرة في نظامه يمكن أن تمدني بمبالغ طائلة لو لم يكن سوء الحظ قد صادفني".[1]

2- إثبات الذات والرغبة في قهر النظام المعلوماتي:

في معظم الأحيان يكون الدافع لدى مرتكب الجرائم المعلوماتية هو الرغبة في إثبات الذات وتحقيق انتصار على تقنية الأنظمة المعلوماتية دون أن يكون لديهم نوايا آثمة، ويرجع ذلك إلى وجود عجز في التقنية التي تترك الفرصة لمشيدي برامج النظام المعلوماتي لارتكاب تلك الجرائم.[2]

إن مجرموا المعلوماتية يتملكهم شعور بالبحث عن القوة ويؤدي ارتكابهم للجرائم بواسطة الوسائل التقنية الحديثة إلى تعويضهم عن الإحساس بالدونية، ففي بعض الأحيان وجد أن مجرد إظهار شعور جنون العظمة هو الدافع لارتكاب فعل الغش المعلوماتي.

ومن جهة أخرى قد يكون الدافع وراء ارتكاب الجرائم المعلوماتية هو الرغبة في قهر الأنظمة الإلكترونية والتغلب عليها، بحيث يميل مرتكبوا هذه الجرائم إلى إظهار تفوقهم على وسائل التكنولوجيا الحديثة.

3- الانتقام:

دافع الانتقام من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب جريمة لأن دافع الانتقام غالبا ما يصدر من شخص يملك معلومات كبيرة عن المؤسسة التي يعمل بها، لأنه في أغلب

[1] الدكتورة نهلا عبد القادر المومني، مرجع سبق ذكره، ص.91.

[2] الدكتور أحمد خليفة الملط، مرجع سبق ذكره، ص.90.

الأحيان يكون أحد موظفيها، ويتيح هذا الدافع أي دافع الانتقام إما نتيجة لفصله من العمل، أو حرمانه من الترقية والحوافز... فهذه الأمور تجعله يقدم على ارتكاب جريمته.[1]

وندرج مثال في هذا الصدد، حيث قام موظف يعمل لدى إحدى شركات التأمين لكي يحتفظ بوظيفته التي سبق أن فصل منها بحجز وحدة التخزين المركزية الخاصة بالشركة كرهينة ووسيلة تهديد لرئيسه لإرجاعه للعمل وهو ما حدث بالفعل. أي بعد رحيله من العمل بعدة أشهر تم تدمير البيانات الخاصة بحسابات وديون المنشأة.[2]

4- ارتكاب الجرائم كوسيلة للتسلية والدعابة:

دافع المزاح والدعابة يعتبر من الدوافع التي تجعل الشخص يقوم بتصرفات وإن كان لا يقصد من ورائها إحداث جرائم وإنما بغرض التسلية والمزاح فقط. ولكن هذه التصرفات قد تنتج عنها نتائج ترقى إلى درجة الجريمة لأنه من الطبيعي أن الشخص الذي يقوم بمسح مجموعة من الملفات من جهاز شخص آخر، وكانت هذه الملفات تحتوي على معلومات مهمة فلا يمكن القول بأن هذا التصرف مجرد دابة، بل إن هذا التصرف في حقيقته هو جريمة إتلاف وتخريب متعمد.[3]

بالإضافة إلى هذه الدوافع هناك دوافع أخرى تدفع لارتكاب الجريمة المعلوماتية وهي كالآتي:

أ- التنافس السياسي والاقتصادي:

كذلك يمكن أن يكون دافعا إلى ارتكاب هذه الأفعال المجرمة، حيث أنه قام بعض القراصنة المتواجدين على الأراضي الروسية باختراق نظم حاسبات حكومية في الولايات المتحدة الأمريكية مدة

[1] الدكتور محمد علي العريان، مرجع سبق ذكره، ص.67.
[2] الدكتور أحمد خليفة الملط، مرجع سبق ذكره، ص.90.
[3] الدكتور أيمن عبد الحفيظ، مرجع سبق ذكره، ص.20.

عام كامل، وقاموا بسرقة معلومات غير سرية، ولكنها حساسة من أجهزة الحواسيب العسكرية الأمريكية.

ب- مناهضة العولمة:

كذلك ممكن أن تكون إحدى الدوافع لارتكاب هذا الفعل، بحيث تم اختراق النظام المعلوماتي للمنتدى الاقتصادي العالمي في دافوس بسويسرا، وتمت عملية سرقة معلومات سرية تتعلق بعدد من الشخصيات الثرية المؤثرة التي شاركت في المؤتمر وأرسلت إلى إحدى الصحف السويسرية.[1]

ج- التسابق القضائي والعسكري بين الدول:

يعد التسابق القضائي والعسكري بين الدول من إحدى الدوافع لارتكاب هذه الجريمة، حيث قام القراصنة بالإعارة على شبكات معلوماتية تابعة لوكالة القضاء ناسا ومواقع أسلحة ذرية تابعة لحكومة الولايات المتحدة الأمريكية. ومن جراء ذلك قام البنتاجون بإنشاء "مركز الحرب المعلوماتية" للدفاع عن الولايات المتحدة الأمريكية ضد القراصنة وتحديد وسائل الهجوم على شبكات حاسب الأعداء.[2]

وهناك مجموعات تطلق على نفسها اسم "مجموعات الكراهية" على الأنترنت هي ضد كل القيم الدينية والأخلاقية والاجتماعية السائدة في المجتمعات، حيث وجدت مواقع الإلحاد التي تطلب بإلغاء الدين والدولة والأسرة وتحرير الإنسان من تلك الأصفاد والقيود فهذه المجموعات يمكن أن ترتكب أفعالا إجرامية معلوماتية وتبدو وفقا لآرائهم ومعتقداتهم مشروعة وتهدف إلى تحسين العالم.

إذ أنه هناك دوافع كثيرة تكون دافع لارتكاب الجرائم المعلوماتية ليس من قبل الأفراد فقط بل من قبل الدول أيضا.

[1] http://news.bbc.co.uk/hi/arabic/news/newsied1153000/1153/24.stm.

[2] الدكتورة نهلا عب القادر المومني، مرجع سبق ذكره، ص.93.

المطلب الثالث: تصنيف الجرائم المعلوماتية

بداية نشير إلى أن الفقه قد انقسم في شأن تسمية هذه الجرائم، حيث ذهب البعض من الفقه إلى تسميتها بجرائم التعدي على وظائف النظام المعلوماتي، بينما فضل جانب آخر من الفقه تسميتها بالجرائم الموجهة ضد النظام المعلوماتي، وذهب جانب آخر إلى تسميتها صور الاعتداء على النظام المعلوماتي.

وهذا الاختلاف في التسمية أدى بطبيعة الحال إلى الاختلاف حول تقسيم الجرائم المعلوماتية، وذلك حسب الأساس والمعيار الذي يستند إليه التقسيم المعني.

فبعض الفقهاء قسمها إلى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته.

وبعضهم يصنفها ضمن فئات بالاستناد إلى الأسلوب المتبع في الجريمة، وآخرون يستندون إلى الدافع أو الباعث لارتكاب الجريمة، وغيرهم يؤسس تقسيمه على تعدد محل الاعتداء، وكذا تعدد الحق المعتدى عليه، فتوزع جرائم الكمبيوتر وفق هذا التقسيم إلى جرائم تقع على الأموال بواسطة الحاسوب، وجرائم تقع على الحياة الخاصة.

ويذهب بعض الفقهاء إلى أن السياسة التشريعية في مجال الأفعال المعتبرة جرائم معلوماتية يفترض أن تؤسس على أن المصلحة التي يحميها القانون هي الحق في المعلومات وفق توازن يراعي كفالة تدفقها وتنظيم معالجتها واستخدامها ونقلها، وعلى أن موضوع الجريمة المعلوماتية ومحل الاعتداء المباشر هو المعطيات بدلالتها التقنية الشاملة والحاسوب يلعب دور الأداة في الاعتداء. فيستهدف معطيات بذاتها، فيكون النظام الموجودة فيه هدفا للجريمة، أو تستهدف معطيات تمثل أموالا أو أصولا لجهة الاستيلاء على الأموال فيكون وسيلة لذلك.[1]

[1] الدكتورة نائلة عادل فريد، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، 2005، ص.34.

فمن الملاحظ أن هذه التقسيمات أو بعضها، لم تراعي بعض أو كل خصائص هذه الجرائم وموضوعها، والحق المعتدي عليه لدى وضعها لأساس أو معيار التقسيم، ونعرض لأهم هذه التقسيمات في النقاط التالية.

أولا: تقسيم الجريمة المعلوماتية بسب دور الكمبيوتر فيها

يذهب البعض إلى أن للكمبيوتر ثلاثة أدوار في مجال ارتكاب الجرائم المعلوماتية ودورا رئيسا في حقل اكتشافها، ونعرض لها على نحو ما يلي:

1- قد يكون الكمبيوتر هدفا للجريمة Target of an offense:

ويكون هذا في حالة الدخول غير المصرح به إلى النظام، أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها، وكما في حالة الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم.

والأفعال التي تتضمن سرقة للمعلومات تتخذ أشكال عديدة معتمدة على الطبيعة التقنية للنظام محل الاعتداء وكذلك على الوسيلة التقنية المتبعة لتحقيق الاعتداء، فالكمبيوترات مخازن للمعلومات الحساسة كالملفات المتعلقة بالحالة الجنائية والمعلومات العسكرية وخطط التسويق وغيرها، ولا يتوقف نشاط الاختراق على الملفات والأنظمة غير الحكومية بل يمتد إلى الأنظمة الخاصة التي تتضمن بيانات قيمة.

وتتضمن بعض طوائف هذا النمط كهدف أنشطة سرقة والاعتداء على الملكية الفكرية كسرقة الأسرار التجارية، وإعادة إنتاج ونسخ المصنفات المحمية وتحديدا برامج الحاسوب.[1]

2- قد يكون الكمبيوتر أداة الجريمة لارتكاب جرائم تقليدية:[2]

A tool in the commission of a traditional offense:

[1] الدكتور خالد ممدوح إبراهيم، مرجع سبق ذكره، ص.62.

[2] الدكتور عمرو عيسى القي، الجرائم المعلوماتية، جرائم الحاسب الآلي والأنترنت في مصر والدول العربية، المكتب الجامعي الحديث، 2006، ص.85.

فالحاسب الآلي هو دائما أداة الجريمة لأنه يمكن الشخص من الدخول على شبكة الأنترنت وقيامه بتنفيذ جريمته أيا كان نوعها بمعنى أن الحاسب الآلي هو الأداة الوحيدة لارتكاب أي جريمة من الجرائم التي ترتكب على شبكة الأنترنت.

ومثال ذلك حالة استغلال الكمبيوتر للاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو استخدام التقنية في عمليات التزييف والتزوير، أو استخدام التقنية في الاستيلاء على أرقام بطاقات ائتمان وإعادة استخدامها والاستيلاء على الأموال بواسطة ذلك، حتى أن الكمبيوتر كوسيلة قد يستخدم في جرائم القتل، كما في الدخول إلى قواعد البيانات الصحية والعلاجية وتحويرها أو تحوير عمل الأجهزة الطبية من خلال التلاعب ببرمجياتها، أو كما في إتباع الوسائل الإلكترونية للتأثير على عمل برمجيات التحكم في الطائرة أو السفينة بشكل يؤدي إلى تدميرها وقتل ركابها.

3- قد يكون الكمبيوتر بيئة الجريمة:

وقد يكون الكمبيوتر بيئة الجريمة، كما في حالة تخزين البرامج المقرصنة فيه أو في حالة استخدامه لنشر المواد غير القانونية أو استخدامه أداة تخزين، أو اتصال لصفقات ترويج المخدرات وأنشطة الشبكات الإباحية ونحوها.[1]

[1] د/ يونس عرب، جرائم الكمبيوتر والأنترنت، المعنى والخصائص والصور واستراتيجية المواجهة القانونية:
www.arablaw.org/download/cyber-crimes-general.doc

وطبعا يمكن للكمبيوتر أن يلعب أدوار أخرى كأن يستخدم أحد مخترقي نظم المعلومات (هاكرز) جهازه للتوصل دون تصريح إلى نظام مزود خدمات أنترنت (مثل نظام شبكة أمريكا أون لاين)، ومن ثم يستخدم الدخول غير القانوني لتوزيع برنامج مخزن في نظامه (أي نظام المخترق)، فهو ارتكب فعلا موجها نحو نظم المعلومات بوصفها هدفا للدخول غير المصرح به ثم استخدم نظم المعلومات لنشاط جرمي تقليدي (عرض وتوزيع المصنفات المقرصنة)، واستخدم جهازه كبيئة، أو مخزن للجريمة عندما قام بتوزيع برنامج مخزن في نظامه.[1]

4-أما من حيث دور الكمبيوتر في اكتشاف الجريمة:

فإن الكمبيوتر يستخدم الآن على نطاق واسع في التحقيق الاستدلالي لكافة الجرائم، عوضا عن أن جهات تنفيذ القانون تعتمد على النظم التقنية في إدارة المهام من خلال بناء قواعد البيانات ضمن جهاز إدارة العدالة والتطبيق القانوني.[2]

ومع تزايد نطاق جرائم الكمبيوتر، واعتماد مرتكبيها على وسائل التقنية المتجددة والمتطورة، فإنه أصبح لزاما استخدام نفس وسائل الجريمة المتطورة للكشف عنها، من هنا يلعب الكمبيوتر ذاته دورا رئيسيا في كشف جرائم الكمبيوتر وتتبع فاعليها بل وإبطال أثر الهجمات التدميرية لمخترقي النظم وتحديدا هجمات الفايروسات وإنكار الخدمة وقرصنة البرمجيات.[3]

كما يمكن أن يكون تقسيم الجرائم بحسب الدور الذي يلعبه الحاسب في الجريمة فقد يكون عاملا مساعدا في ارتكابها أي يكون دوره ثانويا فيها، وهناك حالات أخرى يكون فيها دور الحاسب مهما في ارتكابها إذ بدونه لا يمكن أن ترتكب الجريمة فيكون دوره فيها رئيسيا، وتكون الجريمة

[1] الدكتور أيمن عبد الله فكري، جرائم نظم المعلومات، رسالة دكتوراه، جامعة المنصورة، كلية الحقوق، 2005-2006، ص.87.

[2] الأستاذ أمير فرج يوسف، الجرائم المعلوماتية على شبكة الأنترنت، دار المطبوعات الجامعية، بدون تاريخ نشر، ص.108.

[3] د/ يونس عرب، جرائم الكمبيوتر والأنترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002، تنظيم المركز العربي للدراسات البحوث الجنائية، أبو ظبي 10-2002/02/12.
http://www.arablaw.org/download/cybercrimes-workpaper.doc

المعلوماتية وفقا لذلك هي كل نشاط إجرامي يؤدي فيه نظام الحاسب دورا لإتمامه على أن يكون هذا الدور على قدر من الأهمية، ولا يختلف الأمر سواء كان الحاسب الآلي أداة لإتمام الجريمة أو محلا لها.

ثانيا: تقسيم الجرائم المعلوماتية على أساس الجرائم الواقعة على أو باستخدام النظام المعلوماتي

الجريمة المعلوماتية تنقسم إلى نوعين، النوع الأول وتشمل الجرائم الموجهة ضد نظم المعلوماتية، أما النوع الثاني فتشمل مجموعة الجرائم المرتكبة عن طريق الاستعانة بنظم المعلوماتية، أي جرائم تقع على الأنترنت وجرائم تقع بواسطة الأنترنت، ونعرض هذين النوعين على النحو التالي:

1-النوع الأول: الجرائم الموجهة ضد نظم المعلوماتية (جرائم تقع على الأنترنت)

الجرائم التي تقع على الأنترنت هدف المجرم، وهي بذاتها المصلحة محل الاعتداء.[1]

فالجرائم الموجهة ضد النظام المعلوماتي قد تقع على المكونات المادية لنظام المعلومات le matériel، أو البرامج التي يحتوي عليها نظام المعلوماتية أو المعلومات المسجلة على نظام المعلوماتية.

أ- سرقة المال المعلوماتي:

أصبح لبرامج المعلومات قيمه غير تقليدية لاستخداماتها المتعددة في كافة المجالات الاجتماعية والاقتصادية فهذه القيمة المميزة لبرامج المعلومات تجعلها محلا للتداول، وهنا تبدو أهمية الأنترنت بصفته مصدر للمعلوماتية، مما أدى إلى ظهور قيمة اقتصادية جديدة وأموال جديدة عرفت بالأموال المعلوماتية، وصاحب ظهور هذا المال المعلوماتي جرائم جديدة عرفت بالجرائم المعلوماتية وهذه الجرائم يمكن تصورها من زاويتين:

[1] الدكتور أحمد خليفة الملط، المرجع السابق، ص.201.

الزاوية الأولى: تكون المعلوماتية أداة أو وسيلة للاعتداء.

الزاوية الثانية: تكون المعلوماتية موضوعا للاعتداء.

فالاتجاه الأول يستخدم الجاني المعلوماتية لتنفيذ جرائمه سواء تعلق منها بجرائم الاعتداء على الأشخاص أو الأموال كالسرقة أو النصب وخيانة الأمانة، أما الجرائم من الزاوية الثانية يكون المال المعلوماتي موضوعا لها.

ب- الدخول على المواقع المحجوبة (باستخدام البروكسي):

يحاول مستخدموا الأنترنت بواسطة بعض البرامج تجاوز المواقع المحجوبة والتي عادة ما تكون إما مواقع قومية أو سياسية، وقد يتم حجب بعض المواقع التي لا يفترض حجبها كبعض المواقع العلمية والتي تنشر إحصائيات عن الجرائم وكيفية حدوثها وارتكابها، أو حتى بعض المواقع العادية المخالفة للتقاليد والعادات الاجتماعية لتلك الدولة.

ج- جرائم الاختراقات:

يعتبر الهجوم على المواقع واختراقها على شبكة الإنترنت من الجرائم الشائعة في العالم ويشمل هذا القسم جرائم تدمير المواقع ، اختراق المواقع الرسمية والشخصية ، اختراق الأجهزة الشخصية ، اختراق البريد الإلكتروني للآخرين أو الاستيلاء عليه أو إغراقه ، والاستيلاء على اشتراكات الآخرين وأرقامهم السرية وإرسال الفيروسات .

- **الاقتحام أو التسلل:**

لكي تتم عملية الاقتحام لابد من برامج يتم تصميمها ليتيح للقائم بهذه العملية والذي يريد اختراق الحاسب الآلي لشخص أخر أن يتم ذلك الاختراق .

- **الإغراق بالرسائل:**

يلجأ بعض الأشخاص إلى إرسال مئات الرسائل إلى البريد الإلكتروني لشخص ما يقصد الاضرار به حيث يؤدى ذلك إلى ملء تلك المساحة خاصته وعدم إمكانية استقبال أي رسائل فضلا عن إمكانية انقطاع الخدمة ، حتى يتمكنوا من خلال تلك الأفعال بالأضرار بأجهزة الحاسبات الآلية دونما أي استفادة إلا إثبات تفوقهم في ذلك .[1]

- **الفيروسات:**

الفيروس هو أحد أنواع برامج الحاسب الآلي إلا أن الأوامر المكتوبة في هذا البرنامج تقتصر على أوامر تخريبية ضاره بالجهاز ومحتوياته يمكن عند كتابة كلمه أو أمر ما أو حتى مجرد فتح البرنامج الحامل لفيروس أو الرسالة البريدية المرسل معها الفيروس إصابة الجهاز به ومن ثم قيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به.

د- المواقع المعادية:

يكثر انتشار الكثير من المواقع الغير المرغوب فيها على شبكة الإنترنت فمصطلح المواقع المعادية هو مصطلح حديث بدأ استخدامه بعد هذا التطور التكنولوجي في مجال شبكة الإنترنت، فقام مصممو المواقع المعادية باستغلال التكنولوجيا لخدمة أغراضهم الشخصية.

- **المواقع السياسية المعادية:**

قد ينظر البعض إلى إنشاء تلك المواقع كظاهرة حضاريه تتماشى مع الديمقراطية والحرية الشخصية، ولكن الواقع غالبا ما يكون الغرض من وراء إنشاءها هو معارضة النظام السياسي القائم في بلد ما فيحاولون من خلال تلك المواقع نشر الأخبار الفاسدة التي تنشر الفرقة بين أفراد الشعب ونظامه السياسي القائم.

[1] الدكتور أحمد خليفة الملط، المرجع السابق، ص.202.

- **المواقع الدينية المعادية:**

ويكون الغرض من وراء إنشاءها الإساءة إلى دين من الأديان ونشر الأفكار السيئة عنه وحث الناس على الابتعاد عنه.

- **المواقع المعادية للأشخاص أو الجهات:**

وهى تشبه إلى حد كبير بالمواقع المخصصة للقذف، حيث تهدف أساسا لتشويه سمعة الشخص أو الجهة .

هـ- جرائم القرصنة:

يقصد بجرائم القرصنة هنا الاستخدام أو النسخ غير المشروع لنظم التشغيل أو لبرامج الحاسب الآلي المختلفة. ولقد تطورت وسائل القرصنة مع تطور التقنية ، ففي عصر الانترنت تطورت صور القرصنة ، واتسعت وأصبح من الشائع جداً العثور على المواقع بالانترنت خاصة لترويج البرامج المقرصنة مجاناً أو بمقابل مادي رمزي.[1]

وأدت قرصنة البرامج إلى خسائر مادية باهظة جداً وصلت في عام 1988 إلى 11 مليون دولار أمريكي في مجال البرمجيات وحدها .

- **جرائم التجسس الالكتروني:**[2]

في عصر المعلومات وبفعل وجود تقنيات عاليه التقدم فإن حدود الدولة مستباحة بأقمار التجسس والبث الفضائي، ولقد تحولت وسائل التجسس من الطرق التقليدية إلى الطرق الالكترونية خاصة مع استخدام الانترنت وانتشاره عالميا .

[1] الدكتور أحمد خليفة الملط، المرجع السابق، ص.203.

[2] د. محمد علي عمران، د. فيصل ذكي عبد الواحد، المدخل لدراسة القانون، الرسالة الدولية للطباعة والكمبيوتر، العام الجامعي 1999/1998، ص.52-53.

ولا يقتصر الخطر على محاولة اختراق الشبكات والمواقع على العابثين من مخترقي الأنظمة (HACKERS) بمخاطر هؤلاء محدودة وتقتصر غالباً على العبث أو إتلاف المحتويات والتي يمكن التغلب عليها باستعارة نسخة أخرى مخزنة ، أما الخطر الحقيقي فيكمن في عمليات التجسس التي تقوم بها الأجهزة الاستخبارية للحصول على أسرار ومعلومات الدولة ثم إفشائها لدولة أخرى تكون عادة معاديه، أو استغلالها بما يضر المصلحة الوطنية للدولة.

و- الإرهاب الإلكتروني:

في عصر الازدهار الالكتروني و في زمن قيام حكومات الكترونية ، تبدل نمط الحياة وتغيرت معه أشكال الأشياء وأنماطها ومنها ولا شك أنماط الجريمة والتي قد يحتفظ بعضها باسمها التقليدي مع تغيير جوهري أو بسيط في طرق ارتكابها ، ومن هذه الجرائم الحديثة في طرقها والقديمة في اسمها جريمة الإرهاب الالكتروني والتي أخذت أشكال حديثة تتماشي مع التطور التقني، ويتغير تطور الأساليب التي يحاول المفسدين الوصول بها إلى أهدافها فقد غدا الإرهاب الالكتروني هو السائد حاليا.

وأصبح اقتحام المواقع وتدميرها وتغيير محتوياتها والدخول على الشبكات والعبث بمحتوياتها بإزالتها أو بالاستيلاء عليها أو الدخول على شبكات الاتصالات أو شبكات المعلومات بهدف تعطيلها عن العمل أطول فترة ممكنة أو تدميرها نهائياً أصبح هو أسلوب الإرهاب حالياً في محاولة الوصول إلى أغراضهم.

2- النوع الثاني: الجرائم المرتكبة باستخدام النظام المعلوماتي

الجرائم التي تقع بواسطة الانترنت وبمعنى جرائم وسيلتها الانترنت ، وهى تلك الأفعال التي تتخذ من شبكة الانترنت وسيلة لارتكابها ، حيث تكون المصلحة المعتدى عليها قيمة ماديه أو أدبية أو اجتماعية تتجاوز حدود جهاز الكمبيوتر و شبكة الانترنت ومنها:

أ- الجرائم الجنسية والممارسات الغير أخلاقية:[1]

- **الجرائم غير الجنسية التي تستهدف الاشخاص**

Non-Sexual Crimes Against Persons

وتشمل القتل بالكمبيوتر Computer Murder، والتسبب بالوفاة جرائم الاهمال المرتبط بالكمبيوتر Negligent Computer Homicide، والتحريض على الانتحار Soliciting or Encouraging Suicide، والتحريض القصدي للقتل عبر الانترنت Intentional Internet Homicide Solicitationوالتحرش والمضايقة عبر وسائل الاتصال المؤتمتة Harassment via Computerized Communicationوالتهديد عبر وسائل الاتصال المؤتمتة Intimidation via Computerized Communicationوالاحداث المتعمد للضرر العاطفي او التسبب بضرر عاطفي عبر وسائل التقنية Malicious Infliction of Emotional Distress utilizing Computer Communicationو Reckless Infliction of Emotional Distress utilizing Computer Communication والملاحقة عبر الوسائل التقنية Stalking وانشطة اختلاس النظر او الاطلاع على البيانات الشخصية Online Voyeurism and Online Voyeurism Disclosure وقنابل البريد الالكتروني E-mail Bombing وانشطة ضخ البريد الالكتروني غير المطلوب او غير المرغوب به Spamming utilizing Computerized Communication وبث المعلومات المضللة او الزائفة Transmission of False Statements والانتهاك الشخصي لحرمة كمبيوتر (الدخول غير المصرح به) Personal trespass by computer.

- **طائفة الجرائم الجنسية** Sexual Crimes:[2]

[1] المرجع السابق، ص.54.

[2] المرجع السابق، ص.54.

وتشمل حضر وتحريض القاصرين على انشطة جنسية غير مشروعة Soliciting a Minor with a Computer for Unlawful Sexual Purposes وافساد القاصرين بأنشطة جنسية عبر الوسائل الالكترونية Corrupting a Minor with the use of a Computer for Unlawful Sexual Purposes. واغواء او محاولة اغواء القاصرين لارتكاب أنشطة جنسية غير مشروعة for Luring or Attempted Luring of a Minor by Computer Unlawful Sexual Purposes وتلقي أو نشر المعلومات عن القاصرين عبر الكمبيوتر من اجل انشطة جنسية غير مشروعة Receiving or Disseminating Information about a Minor by Computer for Unlawful Sexual Purposes والتحرش الجنسي بالقاصرين عبر الكمبيوتر والوسائل التقنية Sexually Harassing a minor by use of a Computer for Unlawful Sexual Purposes ونشر وتسهيل نشر واستضافة المواد الفاحشة عبر الانترنت بوجه عام وللقاصرين تحديدا Posting Obscene Material On The Internet. و Posting Or Receiving Obscene Material On The Internetو Trafficking In Obscene Material On The Internet و Sending Obscene Material To Minors Over The Internet و هتك العرض بالنظر عبر الانترنت Indecent Exposure On The Internetوتصوير او اظهار القاصرين ضمن أنشطة جنسية Conduct-- Depicting Minors Engaged In Sexually Explicit Pandering Obscenity Involving A Minor واستخدام الانترنت لترويج الدعارة بصورة قسرية او للاغواء او لنشر المواد الفاحشة التي تستهدف استغلال عوامل الضعف والانحراف لدى المستخدمUsing the Internet for Compelling Prostitution و Using the Internet for Pimping و Using the Internet for Soliciting و Using the Internet for Promoting Prostitution و الحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في أنشطة جنسية Unauthorized Appropriation of Identity,

Image, or Likeness for Unlawful Sexual Purposes؛ وبامعان النظر في هذه اللأوصاف نجد انها تجتمع جميعا تحت صورة واحدة هي استغلال الانترنت والكمبيوتر لترويج الدعارة او اثارة الفحشاء واستغلال اللأطفال والقصر في أنشطة جنسية غير مشروعة.

ب- الجرائم المالية:

- **جرائم السطو على أرقام البطاقات الائتمانية:**[1]

مع بداية استخدام البطاقات الائتمانية خلال شبكة الانترنت واكبت ظهور الكثير من المتسللين للسطو عليها بلا هوادة، فالبطاقات الائتمانية تعد نقوداً الكترونية والاستيلاء عليها يعد استيلاء على مال الغير. ومع وضع تفعيل مفهوم التجارة الالكترونية قامت العديد من شركات الأعمال إلى استخدام الانترنت والاستفادة من مزايا التجارة الالكترونية.

إن الاستيلاء على بطاقات الائتمان أمراً ليس بصعوبة مكان، فلصوص بطاقات الائتمان مثلاً يستطيعون الآن سرقة مئات الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الانترنت ومن ثم بيع هذه المعلومات للآخرين.ويتعدى الأمر المخاطر الأمنية التي يمكن أن تتعرض لها البطاقات الائتمانية الحالية فنحن الآن في بداية ثورة نقدية يطلق عليها اسم النقود الالكترونية والتي يتنبأ لها بأن تكون مكملة للنقود الورقية أو البلاستيكية ومن المتوقع أيضاً أن يزداد الاعتماد على هذا النوع الجديد والحديث من النقود أن تحوز الثقة التي تحوزها النقود التقليدية.

- **القمار عبر الانترنت:**

في الماضي كان لعب القمار يستلزم وجود اللاعبين معاً على طاولة واحدة ليتمكنوا من لعب القمار ، أما الآن ومع انتشار شبكة الانترنت على مستوى العالم فقد أصبح لعب القمار أسهل

[1] المستشار الدكتور محمد ياسر أبو الفتوح، خصائص وتصنيفات الجريمة المعلوماتية، محكمة استئناف القاهرة، مستشار مركز المعلومات ودعم واتخاذ القرار برئاسة مجلس الوزراء، 2008: http://www.F-law.net

وغدا التفاف اللاعبين على صفحة واحدة من صفحات الانترنت على مستوى العالم ومن أماكن متفرقة أسهل من ذي قبل . كما تنافست كثير من المواقع المتخصصة في ألعاب القمار لتزويد صفحات مواقعهم بكثير من البرامج نظراً لان اللاعبين بات بإمكانهم اللعب وكل في مسكنه وكثير ما تتداخل عملية غسيل الأموال في شكل يتم على شبكة الانترنت ولتكن مثلا مع أندية القمار المنتشرة ، الأمر الذي جعل مواقع الكازينوهات الافتراضية على الانترنت محل اشتباه ومراقبة من قبل السلطات الأمريكية ، وبالرغم من مشروعية أندية القمار في أمريكا ، إلا أن المشكلة القانونية التي تواجه أصحاب مواقع القمار الافتراضية على الانترنت أنها غير مصرح لها حتى الآن في أمريكا بعكس المنتشرة في لاس فيجاس.

- **تزوير البيانات:**

تعتبر جرائم تزوير البيانات من أكثر الجرائم شيوعاً من بين كافة أنواع الجرائم التي ترتكب سواء على شبكة الانترنت أو ضمن جرائم الحاسب الآلي نظرا لأنه لا تخلو جريمة من الجرائم إلا ويكون من بين تفاصيلها جريمة تزوير البيانات بشكل أو بأخر ، وتزوير البيانات يكون بالدخول على قاعدة البيانات الموجودة وتعديل تلك البيانات سواء بإلغاء بيانات موجودة بالفعل أو بإضافة بيانات لم تكن موجودة من قبل.[1]

ومما لا شك فيه أن البدء التدريجي في التحول إلى الحكومات الالكترونية سيزيد من فرص ارتكاب الجرائم حيث ستربط الكثير من الشركات والبنوك بالانترنت مما يسهل الدخول على تلك الأنظمة من محترفي اختراقها وتزوير البيانات لخدمة أهدافهم الإجرامية ، وجرائم التزوير ليست بالجرائم

[1] الدكتور أحمد خليفة الملط، المرجع السابق، ص.203.

الحديثة فإنه لا تخلوا ثمة أنظمة من قوانين واضحة لمكافحتها والتعامل معها جنائياً وقضائيا وتكفي التشريعات الحالية لتجريمها وتحديد العقوبة عليها[1].

- **الجرائم المنظمة:**

الهدف الأساسي للجريمة المنظمة في الأساس السعي للإفادة المادية ، أو تحقيق الأرباح ، من خلال مواصلة العمل بوسائل إجرامية ، ولذا كما تستعين الشركات العادية بشبكة الانترنت بحثاً عن فرص جديدة لتحقيق الأرباح، كذلك تفعل المنظمات الإجرامية ، وهى ليست اللاعبات الوحيدات في أسواق الأعمال غير المشروعة ،ولكنها تكون في أحيان كثيرة أهم وازكي اللاعبين علي الأقل بسبب تمتعها بقدرة اكبر على المنافسة التي يوفرها لها تمكنها من التهديد بأعمال العنف.

بالإضافة إلى ذلك قوة المنظمات الإجرامية في اكتشاف واستغلال فرص القيام بأعمال ومشاريع جديدة غير مشروعه في هذا السياق، توفر شبكه الانترنت والنمو المتواصل للتجارة الالكترونية مجالات هائلة جديدة لتحقيق أرباح غير مشروعه.

فخلال السنوات القليلة الماضية ازدادت حنكه ومهارة مجموعات الجريمة المنظمة و تجارة المخدرات، فمثلا اتبعت المنظمات الكولومبية لتجارة المخدرات الممارسات التي تقوم بها الشركات العادية بتنويع الأسواق والمنتجات واستغلت أسواقا جديدة في أوروبا الغربية ودول الاتحاد السوفييتي السابق وأخذت المنظمات الإجرامية و تجار المخدرات تزيد من توظيف مختصين ماليين لإدارة شئون غسيل الأموال[2].

- **تجارة المخدرات عبر الانترنت:**

[1] المرجع نفسه، ص.203.

[2] الدكتور أحمد خليفة الملط، المرجع نفسه.

في عصر الانترنت ظهرت مخاوف جديدة من مواقع السوء – المواقع المنتشرة على الانترنت والتي لا تتعلق بالترويج للمخدرات وتشويق النشء لاستخدامها بل تتعداه إلى كيفية زراعة وصناعة المخدرات بكافة أصنافها وأنواعها وبأبسط الوسائل المتاحة منذ عامين .

- **غسيل الأموال:**[1]

اختلف الكثير في تعريف غسيل الأموال ، وكان أول استعمال قانوني لها عام 1931 اثر محاكمة لأحد زعماء المافيا في أمريكا قضي فيها مصادرة أموال قيل أن مصدرها من الاتجار غير المشروع بالمخدرات ، وقد يكون التعريف الأشمل هو انه أي عملية من شأنها إخفاء المصدر غير المشروع الذي اكتسبت منه الأموال.

وقد ساعدت شبكة الانترنت الذين يقومون بعمليات غسيل الأموال بتوافر عدة مميزات منها السرعة الشديدة وتخطي الحواجز الحدودية بين الدول وتفادى القوانين التي قد تضعها بعض الدول وتعيق نشاطهم وكذلك تشفير عملياتهم مما يعطيها قدر كبير من السرية . وتأكيد لذلك يشير التقرير الذي أعدته الأمم المتحدة وصندوق النقد الدولي إلى ان 28.5 مليار دولار من الأموال القذرة تطير سنويا عبر الانترنت لتخترق حدود 67 دولة لغسلها.

ج- قيادة الجماعات الإرهابية عن بعد:[2]

ويكون ذلك من خلال شبكة الانترنت حيث تقوم بعض الجماعات أو الأفراد في صورة منظمة ببث الأفكار المتطرفة سواء كانت سياسية أو عنصرية أو دينية ، وذات اتجاه اقتصادي والتي تسيطر على عقول الأفراد وتفسد عقائدهم وتخريب اتجاهاتهم ومدى إقناعهم بما هم فيه واستغلال معاناتهم ، في تحقيق أهداف خاصة تتعارض مع مصلحة المجتمع .

[1] د. نائلة عادل محمد فريد، جرائم الحاسب الاقتصادية ودراسة نظرية وتطبيقية، دار النهضة العربية، ط2004، ص.93.

[2] د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتب الآلات الحديثة، أسبوط 1994، ص.41-42.

د- السطو على أموال البنوك:[1]

أصبحت البنوك والمصارف هي هدف لمحترفي التلاعب واختراق شبكات الانترنت والذين يتلاعبون في كشوف حسابات العملاء ونقل الأرصدة من حساب لآخر وقد تكون بصورة ثانية كإضافة بضعة أرقام أو أصفار إلى رقم ما في هذا الحساب.جاءت ثورة المعلومات في النصف الثاني من القرن العشرين لكي تفرض على العالم تحديات كثيرة ولدها التطور العلمي والثورة الهائلة في مجال التكنولوجيا والمعلومات والاتصالات وصناعة الالكترونيات والتعامل مع نظم متقدمة للخبرة والذكاء الاصطناعي وظهور الانترنت. فبالرغم من الإيجابيات الكثيرة للانترنت إلا انه مع مرور الوقت بدأت السلبيات في الظهور فكشفت الاختبارات والحوادث عن ظهور نوع جديد من الجرائم هو الجرائم المعلوماتية الناتجة عن جرائم الحاسب الآلي والانترنت والتي غيرت مفهوم الجريمة العادية لتصبح اشد تأثيرا وأسرع انتشارا وأكثر تنوعاً وأصعب ضبطاً لمرتكبيها حيث أن إقامة الدليل عليهم يكاد يكون معدوماً .ومع وجود هذا العجز التشريعي جعل مواجهة هذه الجرائم أشبه بالمستحيل مع الأخذ في الاعتبار تحديات الجريمة عابرة الحدود والقوميات.

الجرائم المعلوماتية و التي تعددت صورها وأنماطها على كافة المستويات الاقتصادية والاجتماعية والأمنية والأخلاقية وسواء كانت هذه الجرائم واقعة على الانترنت أو واقعة بواسطة الحاسب الآلي فإن لها جوانب سلبية خطيرة تهدد امن وسلامة النظام الاجتماعي داخل المجتمع حيث تعددت صورها وأنماطها على كافة المستويات الاقتصادية والاجتماعية والأخلاقية وهى كأحد الأنماط الإجرامية المستحدثة تتسم بالغموض حيث يصعب إثباتها والتحقيق فيها مما يضع مسئولية كبيرة على رجال الشرطة والأمن والإدارات المعنية كأداة مكافحة جرائم الحاسب الآلي والانترنت ، وبصفه عامة يجب أن ينظر المشرع إلى تحديث قوانين العقوبات الخاصة بهذه النوعية من الجرائم وان يضع قانوناً

[1] المرجع نفسه، ص.42.

للانترنت يجرم الأفعال غير المشروعة ويعاقب مرتكبيها ، وسن قوانين لحماية الملكية الفكرية على المستوى الإقليمي والعالمي.

الفصل الثاني

الاعتداءات على المعلومات والحماية الموفرة لها

تطور تقنيات المعلوماتية ادى كما ذكرنا الى تطور و سائل الاجرام وهذا مادفع بالشارع الى التدخل وتصنيف هذه الجرائم وتقسيمها حسب الوسائل المستخدمة فيها وسن تشريعات تجرمها وتامين الحماية لاصحاب هذه المعلومات وهذا ماسوف نراه في هذا الفصل.

المبحث الأول: الحماية الجنائية للمعلومات وأهميتها

بما أن المعلومة تمثل قيمة أو ثروة اقتصادية كبرى، استوجب ذلك توفير حماية جنائية خاصة بها.

فما المقصود بالحماية الجنائية للمعلومات؟ وفيما تكمن هذه الحماية؟

هذا ما سوف نتعرض له في هذا المبحث وذلك على النحو التالي:

- المطلب الأول: ضرورة الحماية الجنائية للمعلومات
- المطلب الثاني: الحماية الجنائية للمعلومات في النظم المقارنة

المطلب الأول:ضرورة الحماية الجنائية للمعلومات

تجد المعلومة ذاتها في القيمة المعنوية التي تحتويها، وهي بهذا المعنى تحولت من مجرد المعرفة إلى التعامل بالمعرفة، وكان نتيجة لذلك التحول أن أصبح هناك الآن ما يعرف بالمال المعلوماتي le Bien Informatique، الذي يصلح أن يكون محلا للحقوق وتحمل التبعية.

فالمعلومة أصبحت تقوم ماليا، وهي بالتالي تدخل في عداد الأموال الاقتصادية وقد تكون المعلومة شخصية، وإفشائها يهدد الحياة الخاصة من جوانب متعددة. ونظرا للتطور السريع في التكنولوجيا وتقنيات المعلومات التي تمثلت في ظهور شبكة الأنترنت، أظهرت الدراسات الجنائية عدم كفاية النصوص التقليدية، في تطبيقها على الجرائم المستحدثة، في ظل التطور الهائل في أنظمة معالجة المعلومات ونقلها عبر الشبكات، وباتت الحاجة ضرورية لاستحداث قواعد قانونية جديرة لمواجهة هذه الجرائم المستحدثة.[1]

[1] الدكتور أحمد خليفة الملط، مرجع سبق ذكره، ص.109-110.

فالحماية الجنائية للمعلومات يستلزم عند تقريرها مراعاة التحول الجديد الذي أحدثته ثورة المعلومات في خصائصها لا سيما في مسألة التأثير المتطور لها. وهو أمر لا يمكن استدراكه كاملا إلا عند التعامل بالمعلومة في إطار المعالجة الآلية لها.[1]

ويجب أن تستند الحماية للمعلومات على منطق التعامل التشريعي في إطار قانون المعلوماتية.

فلقد وفرت هذه التكنولوجيا في مجال الإتصالات الإلكترونية إمكانية تحقق التواصل الإنساني وإنجاز المعاملات في سهولة ويسر، وأتاح إستخدامها حسن تقديم خدمات الرعاية الصحية وتنمية الملكية الفكرية، وغيرها من مجالات . وتعد شبكات المعلومات ونظم التبادل الإلكتروني للبيانات تطبيقا للإستخدام التكنولوجي الحديث في مجال الإتصالات ونقل المعلومات وهي تختلف بذلك كثيرا عن غيرها من الوسائل التقليدية للاتصال والإعلام ، وهذا الإختلاف يؤدي إلى أمرين:الأول هو تعدد أوجه إستعمالات هذه الوسائل وإتساعها، والثاني هو الحاجة إلى تنظيم قانوني يضع الإطار لهذه الإستعمالات، غير أن هذه التكنولوجيا قد يساء إستعمالها وأن يهدد إستخدامها السلامة العامة والمصلحة الوطنية، فإذا كانت وسائل الإتصال الإلكتروني الحديثة تتيح إنجاز المعاملات المالية بشكل سريع وموثوق به أيا كان مكان المتعاملين؛ فإن إستعمال هذه الوسائل لا يخلو من مخاطر، فقد يستغل بعض المجرمين هذه الوسائل في إرتكاب جرائمهم بطريق الإحتيال أو المساس بخصوصية هؤلاء المتعاملين وسرية معاملاتهم .وإذا كان التقدم التقني قد حاول مكافحة الجرائم في مجال الإتصالات ولجأ إلى تشفيرها بما يحفظ سريتها، فإن هذه الإجراءات – مع ذلك – قد أفضت إلى إستغلال الجناة لهذه الإجراءات في إرتكاب جرائمهم بإستخدام وسائل إتصال يصعب إختراقها أو الوقوف على محتواها، وهو ما يعني أن التقدم التقني قد أمد المجرمين بوسائل بالغة القوة والفاعليةفى ارتكاب جرائمهم.

[1] د. حسام الدين الأهواني، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني، مجلة العلوم الاقتصادية، كلية الحقوق، جامعة عين شمس، بحث مقدم إلى مؤتمر القانون والحاسب الآلي في الكويت، نوفمبر 1989، ص.142.

فمن ناحية فإن المعلومات الالكترونية تتصل بطائفة مهمة من النظم الإدارية والتجارية والمالية التي تمتد لتشمل الدولة والأفراد على حد سواء، وتعتبر من الأدوات المهمة في تنفيذ فكرة "الحكومة الإلكترونية"، التي تقدم خدماتها إلى الأفراد والهيئات العامة والخاصة، ومرتبطة بنشاط الهيئات التي تعمل في مجال البنوك والتأمين والخدمات الطبية وغيرها، فهذه الهيئات تؤدي عملها بالإعتماد على هذه المعلومات .

والحماية الجنائية للمعلومات هى السبيل لتحقيق التجارة الدولية أهدافها، وإنجاز المعاملات وإبرام التصرفات والصفقات التي تقتضيها فكرة التجارة الإلكترونية .ومن شأن كفالة حماية المعلومات على شبكة الانترنت أن يفضي إلى سهولة المعاملات التجارية وسرعة إنجازها وإلى توفير النفقات.

المطلب الثاني: الحماية الجنائية للمعلومات في النظم المقارنة

لقد أثار إحصاء تقنية المعلومات تحديات كبيرة بالنسبة لقانون العقوبات في كل أنظمته القانونية، وسبب ذلك القيمة المتزايدة للمعلومات بالنسبة للاقتصاد والمجتمع والسياسة.

ونظرا لأن قانون العقوبات حتى فترة قريبة لم يكن يعرف إلا حماية الأشياء المادية والمرئية، إلا أنه مؤخرا وللأهمية المتزايدة للمعلومات وتقنياتها ظهرت الحماية الجنائية لها وللقيم المعنوية الأخرى.

فحدثت الموجة الأولى من التعديلات في السبعينات والثمانينات من القرن الماضي في العديد من الأنظمة القانونية الغربية. وهذه التعديلات تتعلق بالحياة الخاصة، وهذه التشريعات كانت بمثابة رد فعل إزاء التهديدات المستحدثة للحياة الخاصة.[1]

ففي بداية الثمانينات، أصدرت العديد من الدول قوانين لمكافحة الإجرام الاقتصادي الخاصة بتقنية المعلومات والتي تشتمل على تجريم الولوج غير المسموح به إلى النظام التقني للمعلومات.

[1] د. رشدي محمد علي محمد عيد علي، مرجع سبق ذكره، ص.79.

وبعدها ظهرت تشريعات بغرض توفير حماية أفضل للملكية الذهنية في مجال تقنية المعلومات.

وقد استبعدت برامج تقنية المعلومات من الحماية عن طريق قانون براءات الاختراع، وصدرت قوانين أخرى لحماية البرامج.

أولا:حماية المعلومات على المستوى الدولي:

تختلف خطة التشريعات المقارنة في موضع النص على الحماية الجنائية وتتوزع إلى اتجاهاين :

الأول يرى إصدار قانون يعاقب فيه على جرائم الكمبيوتر بصورها المختلفة ، وتقترن هذه الخطة في تجريم هذه الأفعال بإصدار تشريعات تنص على صورة معينة مثلا "السجلات والتوقيع الإلكتروني" ومن أمثلة التشريعات التي تبنت هذه الخطة تشريعات الولايات المتحدة الأمريكية.

والإتجاه الثاني من التشريعات يذهب إلى إدخال تعديلات على النصوص التشريعية القائمة على نحو يؤدي إلى إستيعابها الصور المستحدثة من الجرائم الإلكترونية ، ثم تفرد هذه الخطة التشريعية قوانين خاصة ببعض الموضوعات مثل الإتصالات والتوقيع الإلكتروني والتي تتضمن نصوصا تتصل بتجريم الاعتداء على المستند الإلكتروني .ومن امثلة التشريعات التي تبنت هذه الخطة الأخيرة القانون الألماني والفرنسي.

1- تشريعات الولايات المتحدة الأمريكية:

أولا: على المستوى الإتحادي: إعتبر الشارع الأمريكي جرائم الكمبيوتر والجرائم الملحقة بها من الجرائم الإتحادية، ويرجع ذلك إلى قانون سنة 1984 الذي أقره الكونجرس بشأن تجريم الإتصال غير المرخص به، والغش وإساءة إستعمال الكمبيوتر. ومنذ صدور هذا التشريع تزايدت نصوصه

وتوسعت أحكامه حتى تتسنى مواجهة الصور المستحدثة من جرائم الكمبيوتر. وقد أدى الإتساع الضخم لشبكات المعلومات وعدم مركزية النشاط المتصل بالكمبيوتر إلى وجود صعوبة بالغة في تنظيم هذا النشاط.[1] ومع تزايد إستخدام الكمبيوتر وتطور تقنياته ظهرت نماذج جديدة من السلوك الضار أدت إلى تطور التشريع على نحو مواز لها، وقد تمخض هذا التطور عن صدور عدة تعديلات منها قانون إساءة إستعمال الكمبيوتر لسنة 1994. وبالإضافة إلى القوانين سالفة الذكر فقد أصدر الشارع الأمريكي في 30 يونيه سنة 2000 قانونا اتحاديا "للتوقيع الإلكتروني العالمي والتجارة الوطنية" أجاز بموجبه قبول وإستخدام التوقيع والسجلات الإلكترونية في التعاملات التجارية الدولية وبين الولايات.

وقد أبقى هذا القانون الإتحادي على كافة التشريعات الصادرة من الولايات للتوقيع والسجلات الإلكترونية، غير أنه في حال عدم صدور مثل هذه التشريعات فإن القانون الإتحادي للتوقيع الإلكتروني هو الذي يطبق. وهو ما يعني أن الغطاء التشريعي للمستندات الإلكترونية يمتد إلى كافة الولايات الأمريكية، حتى ولو لم تصدر قانونا خاصا به.

وقد سبق القانون الإتحادي للتوقيع الإلكتروني جهودا تشريعية لإقرار التوقيع والسجلات الإلكترونية ومساواتها بالمستندات الكتابية، ومن هذه الجهود:القواعد الإتحادية للتوقيع والسجلات الإلكترونية الصادرة في 20 مارس سنة 1997والتي وضعت لتطبيقها في مجال شركات الأجهزة والقانون الإتحادي للغذاء والدواء ومستحضرات التجميل وقانون الخدمة الصحية العامة[2].

وتعود الجهود التشريعية للتوقيع والسجلات الإلكترونية إلى ما طالب به ممثلو الصناعات الصيدلانية في سنة 1991 عن رغبتهم في إستخدام البدائل الإلكترونية مثل تلك المحررة بخط اليد. وكان تبرير ذلك ما تحققه هذه الوسائل وخاصة في مجال حفظ السجلات من أهمية كبيرة لشركات

[1]Computer viruses: Information age vulnerability and the technopath, Amercan criminal Law Review, Vol. 27, 1990, P.525.
[2]ABA Section Creates First Digital Signature Guidelines To Aid In Security of The Internet, 1996.

التصنيع الصيدلاني. وقد أثمرت هذه الدعوة عن تشكيل مجموعة عمل تتحدد مهمتها في تنمية سياسة قبول التوقيع الإلكتروني من الهيئات. وقد وضعت مجموعة العمل تقريرا في يوليه سنة 1992 إقتصرت فيه على إلقاء الضوء على القواعد المتصلة بالتوقيع الإلكتروني؛ غير أنها في 31 أغسطس 1994 أصدرت تقريرا وضعت فيه القواعد المتعلقة بالسجلات الإلكترونية. كما وضعت قواعد للتوقيع والسجلات الإلكترونية صدرت في 20 مارس سنة 1997 لتطبيق على شركات الأجهزة. كما صدر نموذج لقانون المعاملات الإلكترونية الموحد، وهو نموذج إختياري، وذلك بهدف توحيد القواعد التي تتصل بالمعاملات التجارية الإلكترونية بين تشريعات الولايات. وإلى جانب هذه التشريع فإن هناك بعض التشريعات التي يكفل الحماية الجنائية للبيانات المخزنة إلكترونيا تضمنتها تشريعات إتحادية منها ما ينص عليه الفصل 119 من القسم الأول من تقنين الولايات المتحدة سالف الذكر والذي يحمل عنوان "إعتراض وسائل الإتصالات السلكية والإلكترونية والشفهية[1]."

أصدرت الكثير من الولايات الأمريكية تشريعات تتضمن وضع تنظيم للسجلات والتوقيع الإلكتروني. ويعد أول تشريع يصدر في هذا الموضوع هو "قانون المعاملات الإلكترونية الموحد" الذي أصدرته ولاية كاليفورنيا في 16 سبتمبر سنة 1999 والذي دخل إلى حيز النفاذ في أول يناير سنة 2000. وقانون المعاملات الإلكترونية الموحد الذي أصدرته ولاية نورث كارولينا والذي دخل حيز النفاذ في الأول أكتوبر سنة 2000.

وقد أصدرت ولاية نيويورك تشريعا في 28 سبتمبر سنة 1999 للسجلات والتوقيع الإلكتروني. وكان هدف هذا التشريع هو تنظيم وتشجيع التعامل بالسجلات الإلكترونية وقبول التوقيع الإلكتروني في التعاملات التجارية. وقد كلف الشارع في ولاية نيويورك مكتب تقنيات الولاية بوضع تقرير يتضمن وضع تنظيم ودليل عمل لأفضل السبل لإنشاء وإستخدام وتخزين والمحافظة على التوقيع والسجلات الإلكترونية (المادة الثالثة من الفصل الرابع من هذا القانون .(وقد أصدرت ولاية

[1]Computer viruses: Information age vulnerability and the technopath, Amercan criminal Law Review, Vol. 27, 1990, P.525.

كونتيكتكت قانونا للمعاملات الإلكترونية في فبراير سنة 2002ودخل حيز النفاذ في الأول من أكتوبر في ذات السنة. كما أصدرت ولاية بنسلفانيا قانونا مماثلا في 16 ديسمبر سنة 1999.

2- تشريعات فرنسا

-القانون الفرنسي:نص الشارع الفرنسي على تجريم الإعتداء على أنظمة معالجة البيانات، وذلك بموجب الفصل الثالث من الباب الثاني من قانون العقوبات ومن ضمن الجرائم التي تضمنها هذا الفصل إدخال أو مسح أو تغيير معلومات بطرق الغش (المادة 323-3)كما نص الشارع الفرنسي على تجريم عدة أفعال تقع ضد المصالح العليا للدولة وذلك إذا انصبت على المعلومات أو البيانات التي تم معالجتها إلكترونيا (المواد 411-6 إلى 411-10) وإلى جوار هذه النصوص الخاصة الواردة في قانون العقوبات فإن الشارع الفرنسي قد نص على بعض الجوانب المتصلة بالمستند الإلكتروني في قوانين متفرقة أهمها:قانون الإثبات والتوقيع الإلكتروني الصادر في 13 مارس سنة 2000/ ولائحته الصادرة في 30 مارس سنة 2001 .والذي أقر فيه الشارع الفرنسي الأخذ بالدليل الإلكتروني في الإثبات والتوقيع الإلكتروني ووضع له الضوابط التي تكفل صحته . ومن التشريعات الأخرى التي تتضمن جانبا من الحماية المقررة للمستند الإلكتروني قانون حرية الإتصالات الذي صدر في سبتمبر سنة 1986 وعدل بقانون أول أغسطس سنة 2000.

3- القانون الألماني:

تدخل الشارع الألماني بقانون 15 مايو سنة 1986 والذي عدل بمقتضاه قانون العقوبات بأن اضاف إليه المادة 202 (أ)، والتي جرم بها فعل التجسس على المعلومات المخزنة . وقد وردت هذه المادة في الباب الخاص بجرائم الإعتداء على الحياة الخاصة والسر اللذين جمعهما الشارع الألماني

في باب واحد، وعلة ذلك الإرتباط الوثيق بين فكرة السر وبين الحياة الخاصة، وأن عناصرهما تتحدد في حماية سرية المحادثات وحماية سرية المراسلات ، وحماية الأسرار الخاصة للأفراد[1].

كما أصدر الشارع الألماني قانونا للتوقيع الإلكتروني دخل حيز النفاذ في أول نوفمبر سنة 1997، وقد نص الشارع الألماني في هذا القانون على قواعد التوقيع الإلكتروني مثل تعريف الإصطلاحات الواردة في التشريع وتحديد السلطة المختصة بتطبيقه، والقواعد المتعلقة بمقدمي خدمة التوثيق والسلامة الفنية وفي الرابع نظم قواعد الإشراف وضوابطه كما نص كذلك على القواعد الخاصة بالمسؤولية والجزاءات الموقعة . وقد اصدر الشارع الالماني كذلك قانون المعلومات وخدمات الإتصالات ، والذي دخل حيز النفاذ في أول أغسطس سنة 1997.

ثانيا:حماية المعلومات على المستوى العربي او الاقليمي:

لم تكن الدول العربية غائبة عن النقاشات، التي كانت تدور داخل أروقة الأمم المتحدة حول مدى تأثير تطور التكنولوجيا الحديثة للإعلام على حقوق الإنسان وحرياته. ويعتبر انعقاد مؤتمر الأمم المتحدة الأول لحقوق الإنسان في طهران عام 1968 أكبر شاهد على ذلك. خلاله بدأت الدول العربية تعي خطورة وأهمية انتشار هذه التكنولوجيا، خاصة حينما ستنفلت من يد الدولة فتصبح متاحة للأفراد والمؤسسات يستخدمونها كما شاءوا. وقد أكدت قضية "واتركيت" في الولايات المتحدة الأمريكية لدى هذه الدول خطورة استخدام الآلات الدقيقة من طرف الأفراد أو من طرف بعض المؤسسات غير الأمنية والغير عسكرية، في التلصص، والتصنت، وكشف أسرار الهيئات والمؤسسات وحتى الدول[2]. في السابق كانت هذه الآلات حكرا على أجهزة المخابرات، بينما اليوم يمكن الحصول عليها من طرف أي كان، واستخدامها لشتى الأغراض، من كشف أسرار الدولة إلى كشف أسرار الأفراد والتعدي على حياتهم الخصوصية في أدق تفاصيلها.

[1]Verboteme Schriften im internet, Juristiche Rundschau, 1997, S496. Redbruch (Gustav).

[2]جميل عبد الباقي الصغير: القانون الجنائي والتكنولوجية الحديثة الكتاب الأول: الجرائم الناتجة عن استخدام الحاسب الآلي. دار النهضة العربية القاهرة 1992.

إذا كانت الدول العربية على علم ودراية بأهمية وخطورة هذه التقنيات الحديثة للاتصال الناتجة عن الثورة المعلوماتية فإنها مع ذلك تبقى كغيرها من الدول غير المنتجة لهذه التقنية، غير مبالية بانعكاساتها القانونية، تاركة في البداية أمر تدبير المشاكل الممكن أن تنتج عنها للقوانين القائمة التقليدية: مثل القانون الجنائي- وقانون الإعلام والاتصال والقانون التجاري، والقانون المدني.

فعلى المستوى الدولي شكل مؤتمر طهران 1968، لحظة تحول واهتمام بالتداعيات القانونية لتطور التكنولوجيا على مجال حقوق الإنسان. فتلى ذلك إصدار الأمم المتحدة لقرارات تشدد على هذا الأمر، وبالخصوص في سنة 1973 تزامنا مع قضية "واتركيت" وأعقب ذلك انطلاق تشريعات وقوانين حماية الخصوصية وحماية البيانات الشخصية، وتجدر الإشارة هنا على الخصوص إلى التشريع السويدي لسنة 1973[1].

لقد كانت هذه التطورات العلمية كبداية لتأكيد الجذور الأولى للفضاء الالكتروني، والفضاء التخيلي. ولربما أن ذلك ما حدا بالكاتب "وليام جيبسون" في سنة 1984 إلى تصور ظهور عالم افتراضي، ينشأ عن ترابط الأنظمة الكمبيوترية التي تعمل ضمن الشبكة العالمية، وتتم من خلاله أنواع متعددة من المعاملات مثل: البيع، والشراء، وتجارة الأسهم.فهل في ذلك تأثير على التفكير القانوني للانترنت؟

1- البحث حول إمكانية وجود قانون خاص بالأنترنت:

يبدو أن الأمر على عكس ما يتمناه كثير من القراصنة ومستغلي الفضاء الافتراضي من أجل ارتكاب جرائم السطو والسرقات، وجرائم التشهير، والمساس بالحياة الخصوصية للأفراد، فالانترنت ليس فضاء اللاقانون، وليس فضاءا تسوده الفوضى، تحت غطاء اعتباره مجالا للحرية المطلقة الشاملة، وليس عالما افتراضيا لا يحكمه أي ضابط، ومنفلت من أي وازع. إن هذا الأخير هو وسيلة لإرسال

[1] قانون حماية الكمبيوتر: بين تبادل المعلومات وحماية الابداعجريدة المساء: عدد 535 السبت/ الأحد 7/6 يونيو 2008.

واستقبال المعلومات والحصول عليها من مختلف أطراف المعمور وبسرعة مذهلة. كما يمكن القيام من خلاله بمعاملات متنوعة، كالتسويق، والاتصالات، والإعلانات، وإجراء التعاقد...[1]، وهذا ما اصطلح عليه بالفضاء التخيلي أو الفضاء الالكتروني. هكذا إنه بفعل المهام التي يقوم بها، والخدمات التي يقدمها بسهولة ويسر، وبحكم أهمية وخطورة المعاملات التي تجرى من خلاله، صار من المفروض أن ينظم من الناحية القانونية. وتوضع له ضوابط وقواعد تلجمه وتحكمه، ولأجل هذا الغرض ظهرت مدرسة التنظيم القانوني للانترنت التي تلح على عدم إهمال الجوانب القانونية للانترنت، خاصة في وقت صار التطور التكنولوجي في هذا المجال يطرح إشكالات وقضايا قانونية متنوعة ومعقدة، ومن نوع خاص[2]. وعلى هذا فإن المبادئ القانونية التقليدية قد لا تفي بالغرض عند تطبيقها على هذا المجال. تحت هذا الضغط فُرض على الدول المتقدمة، ودول العالم الثالث وضمنها الدول العربية صياغة ووضع قوانين يتم بموجبها تنظيم الفضاء الافتراضي. فإذا كان هاجس التنظيم القانوني للانترنت قد فرض نفسه على هذه الدول، فالأمر ازداد أهمية وإلحاحية في وقت أضحى فيه العالم بفعل هذه الوسيلة التكنولوجية عبارة عن قرية الكترونية صغيرة على حد تعبير "ماكلهون"، يمكن التجول في مختلف أرجاءها شرقا وغربا، شمالا وجنوبا، بفضل الانترنت.

2- الجهود الجماعية العربية لتقنين الانترنت

من المعلوم أن المشرع العربي على امتداد الوطن العربي من المشرق إلى المغرب، مسكون بنفس الهواجس، والمخاوف إزاء الانترنت، الذي يخترق الحدود، والسيادات بسلاسة ويسر لانظير لهما. وهكذا ولأجل مواجهة مخاطر هذا الوحش الالكتروني المخترق للحدود والسيادات، بادرت الدول

[1]Du droit et des libertés sur l'Internet rapport au premier ministre français. Paris- documentation française 2001 p : 12

[2]El houcine ennaciri : droit d'Internet au Maroc Mémoire de D.E.S.A faculté de droit - Rabat Agdal 2006 Du droit et des libertés sur l'Internet rapport au premier ministre français. Paris- documentation française 2001 p : 12

العربية على المستوى التشريعي إلى إصدار "قانون نموذجي" حول جرائم الانترنت" صدر عن مجلس وزراء الداخلية العرب على صورة مشروع، تمت المصادقة عليه في سنة 2004، وينص على[1]:

"... إن إرسال وتخزين المعلومات على الانترنت وإرسالها، وكذا المواد المنافية للأخلاق والنظام العام، والتي تتناقض مع مبادئ الدين والأسرة [العائلة] يعاقب عليها بالحبس حتى وإن ارتكبت هذه الجرائم من خارج الوطن".

وهناك بعض الدول العربية التي أصدرت قوانين لتنظيم الانترنيت قبل صدور "القانون العربي الموحد للانترنت"، غير أن ما هو مثير للنظر في جهود المشرع العربي في تعامله مع الانترنت، كونه لا يرى فيه إلا مجرد وسيلة إعلام واتصال، ولا شك أن ذلك قد يؤدي إلى التبخيس من قيمته ليتحول إلى مجرد أداة لنقل وبث الأخبار والمعلومات[2]، بينما هو قبل كل شيء بنية أساسية للمبادلات، والروابط والهويات وتداول، وتخزين المعلومات والمعرفة ...

لم يكن المشروع المقدم من طرف وزراء الداخلية العرب هو المرجعية الوحيدة التي تأثرت بها الدول العربية في سعيها إلى تنظيم الانترنت قانونيا، بل هناك تشريعات أوروبية وأمريكية سابقة على هذا المشروع، تركت بصماتها على قوانين الانترنت في الدول العربية. كما أن الاتفاقية الموضوعة في إطار النظام الإقليمي الأوروبي حول الانترنت: أي اتفاقية بودابيست سنة 2001 كانت هي الأخرى ذات تأثير ملموس على المشرع العربي.

هذه القوانين والاتفاقيات عبدت الطريق أمام الأقطار العربية لضبط وتقنين الانترنيت. فأصدرت حزمة من التشريعات بغرض تنظيم الفضاء الافتراضي. وهكذا على امتداد الوطن العربي، من مصر إلى المغرب، فالسعودية وتونس، والجزائر وليبيا، ولبنان وسوريا، والأردن والبحرين، والإمارات

[1] يونس عرب: التشريعات والقوانين المتعلقة بالانترنت في الدول العربية.
ورقة عمل: مقدمة إلى مؤتمر ومعرض التكنولوجيات المصرفية العربية والدولية- اتحاد المصارف العربية 28-29 تشرين الأول 2002 عمان الأردن.

[2] يونس عرب: التشريعات والقوانين المتعلقة بالانترنت في الدول العربية.
ورقة عمل: مقدمة إلى مؤتمر ومعرض التكنولوجيات المصرفية العربية والدولية- اتحاد المصارف العربية 28-29 تشرين الأول 2002 عمان الأردن

العربية المتحدة والسودان... وضعت قوانين لتنظيم الانترنت مصاغة بشكل مضبوط وبعناية دقيقة ومدروسة، من أجل خدمة أهداف الدولة، أكثر من حماية المجتمع. وتهدف هذه التشريعات إلى التحكم في الآثار الممكن أن تنشأ عن إطلاق العنان للانترنت وعدم ضبطه. وتضمنت مقتضيات كثيرة تيسر للدولة إمكانية اللجوء إلى حجبه. لقد أكد التقرير الذي تقدمت به الشبكة العربية للإعلام وحقوق الإنسان في سنة 2006 أن حجب المواقع أمر عادي ويتم اللجوء إليه بشكل متواتر في كل الدول العربية بما فيها تلك التي تدعي أنها أكثر انفتاحا كلبنان والمغرب.

3- الغرض الذي أدى إلى محاولة وضع قانون (قوانين) عربية للأنترنت

كان هناك نقاش واسع حول هل من الضروري وضع آليات قانونية لتنظيم الانترنت[1]؟ أم أن ماهو موجود وقائم حتى الآن من قوانين كاف ليحكم ما قد ينتج عن هذه الوسيلة التكنولوجية من تصرفات وأعمال، ومخالفات. أسفر هذا النقاش على ظهور اتجاهين[2].

أولهما: يرى أن الانترنت، لم ينتج بعد آثارا واضحة تقتضي التدخل المشروع لتنظيم المسائل المترتبة عنه.

الثاني: يرى أن الانترنت يسابق العصر وأن عدم الإسراع في تنظميه قاد إلى حدوث تأثيرات دون أن يكون ثمة قانون نهتدي به في الموقف من هذه التأثيرات.

وأيا كان الأمر فإن التعامل مع الانترنت يثير التساؤلات القانونية الآتية، وهي تساؤلات غير قاصرة على تشريعات الانترنت في الأقطار العربية فقط، بل هي عامة وتتعلق بالظاهرة القانونية للانترنت في عموميتها: وهذه التساؤلات هي[1]:

[1]PHILIPPE AIGRAIN : Au-delà du logiciel libre, le temps des biens communs : le monde diplomatique, Octobre 2005

[2]عمر محمد بن يونس: مشكلة قواعد البيانات، موسوعة التشريعات العربية ، دار الفكر الجامعي: الاسكندرية: 2004.

- هل إبرام العقود عبر الانترنت تتوفر فيه سلامة وصحة التعبير عن الإرادة كما هو الشأن في التعاقد الكتابي أو الشفاهي في مجلس العقد؟ وهل توقيع العقود والمراسلات اليكترونيا معادل لتوقيعها ورقيا؟
- هل رسائل البريد الالكترونية ذات قيمة معادلة للمراسلات الورقية؟
- هل الاعتداء على الأشخاص وعلى الأموال في البيئة الحقيقية يمكن تطبيق مفهومها على اعتداءات المجرم المعلوماتي؟
- كيف يمكن حماية الأسرار الشخصية، وبيانات الحياة الخاصة من اعتداءات المجرم المعلوماتي أو المتطفل دون تصريح أو إذن؟
- هل إغلاق المواقع أوحجبها، مثل المواقع ذات المحتوى غير المشروع في بعض النظم والمشروع في الأخرى، يعد تجاوزا في حق ديموقراطية العالم الافتراضي.
- هل النشر الالكتروني من قبيل النشر الصحفي الذي يحكمه قانون الإعلام والاتصال.[2]

ما ذا أنجزت الدول العربية على المستوى التشريعي انطلاقا من التساؤلات المومأ إليها من قوانين فيما يخص التجارة الالكترونية وفي التوقيع الالكتروني؟

إن التساؤل عما أنجز هنا تشريعيا على المستوى العربي غير قاصر على ما أنتج بشكل فردي من قبل كل قطر على حدة، ولو أن هذا هو الأهم، ولكن كذلك ما أنتج على المستوى الجماعي، أي في إطار النظام الإقليمي وفي ظل مؤسسة جامعة الدول العربية. لسنا في حاجة إلى التأكيد على أن الدول العربية مثلها مثل بقية الدول التي في نفس أوضاعها، تحاول جهدها ضبط ما يطرحه

---

[1] لمزيد من التدقيق في هذه الأسئلة يراجع: يونس عرب: مقال في جريدة المساء: عدد: 535/ السبت الأحد 2008/8/7 تحت عنوان: قانون الكمبيوتر... بين حرية تبادل المعلومات وحماية الإبداع.

ولمزيد من التدقيق يراجع: محمود عبده الدلالعة: الحماية الدولية والقانونية لتكنولوجيا المعلومات وبرامج الحاسب رسالة لنيل الدكتورة: كلية الحقوق الدار البيضاء 2002.

[2] علي كريمي: تطور قوانين الإعلام في الدول المغاربية

"ورقة مقدمة في الحلقة الدراسية المنظمة من طرف الإيسيسكو يونيو 2009 بطرابلس ليبيا"

استخدام الانترنت، وما يطرحه الاستخدام المتوالي والسريع لتكنولوجيا الإعلام قصد تنظيمها قانونيا. وتجدر الإشارة هنا إلى الجهود التي بدلت في هذا الاتجاه من طرف بعض الدول العربية وخاصة فيما يتعلق بمجال التجارة الالكترونية، والتوقيع الالكتروني.

يمكن أن نشير على سبل المثال لا الحصر إلى جهود كل من تونس، والمغرب، والأردن، والسعودية، والبحرين، والإمارات العربية، ومصر ولبنان، ودبي، وسوريا والسودان...

4- التنظيم القانوني: التجارة الالكترونية، والتعاقد والتوقيع الالكتروني[1]

اهتمت جل الدول العربية بهذا الموضوع خلال الفترة الممتدة ما بين 2000 و2009، ومن الناذر اليوم أن نجد خلو تشريع هذه الدول من قوانين تنظم التجارة الالكترونية والتوقيع الالكتروني. ولو شئنا سوق الأمثلة لتزاحمت أمامنا النماذج بما يفيض عن غرض هذه الورقة، ولغطت هذه الأمثلة كل دول المغرب العربي، والخليج العربي، والدول الأخرى. وهكذا ففي مملكة البحرين صدر قانون التجارة الالكترونية بتاريخ:14 سبتمبر 2002، كما صدر في الأردن القانون رقم 85 لسنة 2001، قانون المعاملات الالكتروني. وفي تونس صدر القانون عدد 83 لسنة 2000 الخاص بالمبادلات الالكترونية والمؤرخ في 9 غشت 2000. ويسرى نفس الشيء على المغرب، والجزائر وتونس وليبيا ولبنان والإمارات العربية المتحدة.فإذا كان استخدام الانترنت في الأغراض التجارية بدأ في الانتشار على الصعيد العالمي منذ 1992، فصار كمروج للسلع والخدمات. وبدأ رجال الأعمال وأصحاب المؤسسات والشركات التجارية في الإقبال على المواقع الخاصة بهذا الغرض، وأصبحوا يبرمون الصفقات

[1] علي كريمي: تطور قوانين الإعلام في الدول المغاربية، المرجع السابق.

عن طريق مراسلاتهم عبر البريد الالكتروني، كما صاروا يعرضون منتجاتهم وخدماتهم من خلال مواقع لهم على شبكة الانترنت[1].

ساهمت ثورة المعلومات والاتصالات في انتشار التجارة الالكترونية، ونتج عن الصفقات التي تتم عبر الانترنت، ظهور العقود الالكترونية كوسيلة قانونية جديدة، فصارت مثار جدال قانوني خصب. فاضطرت الكثير من المنظمات الإقليمية والدولية، وكثير من مشرعي الدول إلى الإقرار بهذا الواقع والاعتراف به، ومن ثمة، إجازة التعبير عن الإرادة التعاقدية عبر الوسائل الالكترونية. وهو ما يعني أن التقاء الإرادات اليكترونيا يكفي لإبرام العقد متى استوفى شروطه.

أقر القانون النموذجي للتجارة الالكترونية لسنة 1996 أن تبادل التعبير عن الإرادة من خلال تبادل البيانات الالكترونية في الأعمال التجارية حيث نصت المادة:11 منه على: "...في سياق إنشاء العقود، وما لم يتم اتفاق الطرفان على غير ذلك يجوز استخدام رسائل البيانات للتعبير عن العرض وقبول العرض، وعند استخدام رسالة البيانات في إنشاء العقد، لا يفقد ذلك العقد صحته أو قابليته للتنفيذ لمجرد استخدام رسالة بيانات لذلك الغرض".

كما أن قانون المعاملات الالكترونية الموحد لعام 1999 نص صراحة على أن أحكام التعاقد إلكترونيا مثل التعاقد كتابيا عندما قرر أن التسجيل الالكتروني يعادل المستند المكتوب خطيا[2].

وتقر اتفاقية الأمم المتحدة بشأن عقد البيع الدولي للبضائع في مادتها:10"... جواز التعاقد عن طريق وسائل الاتصال الفوري".

- لكن كيف تعاملت التشريعات العربية مع التعاقد الالكتروني؟ للجواب على هذا السؤال نستعرض بعضا من هذه التشريعات: وكمثال على ذلك: المادة:14 من قانون إمارة دبي

[1]Rachid BOUTI : les enjeux du commerce électronique pour les commerçants : cybers PME-PMI artisans on line, REMALD, sirie études, n°50, Mai-juin 2003.

[2]غزة على محمد الحسن: قانون الانترنت، شركة مطابع السودان للعملة: رقم الإيداع 404/2005

بشأن المعاملات والتجارة الالكترونية[1]وتنص على "... يجوز أن يتم التعاقد بين وسائط الكترونية مؤتمة متضمنة نظامي معلوماتي أو أكثر تكون معدة، ومبرمجة مسبقا للقيام بمثل هذه المهمات، ويتم التعاقد صحيحا ونافذا ومنتجا آثره القانونية على الرغم من عدم التدخل الشخصي أو المباشر لأي شخص طبيعي في عملية إبرام العقد في هذه الأنظمة".

وتأكيدا لمبدأ جواز التعاقد الالكتروني نصت المادة:7/1 من نفس القانون على:

" لاتفقد الرسالة الالكترونية آثارها القانوني أو قابليتها للتنفيذ لمجرد أنها جاءت في شكل الكتروني".

- أما المشرع الأردني فإنه أكد على "أن إبرام العقود الالكترونية بواسطة الرسالة الالكترونية يعتبر صحيحا عندما قرر في المادة 13 من قانون المعاملات الالكترونية رقم 85- لسنة 2001: "تعتبر الرسالة الالكترونية وسيلة من وسائل التعبير عن الإرادة المقبولة قانونيا لإبداء الإيجاب والقبول بقصد إنشاء التزام تعاقدي".

- وفي المغرب صدر قانون التوقيع الالكتروني بظهير رقم 1-07-129 الذي يقضي بتنفيذ القانون رقم 05-53 المتعلق بالتبادل الالكتروني للمعطيات القانونية التي يتم تبادلها بطريقة الكترونية.[2] يحدد القانون النظام المطبق على المعطيات القانونية التي يتم تبادلها بطريقة الكترونية، وعلى المعادلة بين الوثائق المحررة على الورق، وتلك المعدة على دعامة الكترونية وعلى التوقيع الالكتروني.

- ويشترط المشرع المغربي على أن تكون الوثيقة المحررة على دعامة الكترونية بنفس قوة الإثبات التي تتمتع بها الوثيقة المحررة على الورق شريطة أن يكون بالإمكان التعرف بصفة قانونية على

[1]وهو القانون رقم: 2 لسنة 2002.

[2]انظر الجريدة الرسمية رقم 5584 الصادرة يوم الخميس 6 دجنبر 2008.

الشخص الذي صدرت عنه، وان تكون معدة ومحفوظة وفق شروط من شأنها أن تضمن تماميتها، إضافة إلى أنه اشتراط أن يكون التوقيع الالكتروني مؤمّنا. ويعني بذلك أن يتم إنشاؤه وفق النصوص التنظيمية والتشريعية المعمول بها في هذا المجال (المادة 1-497-3-417).

- وأكدت المادة 6 من هذا القانون على أن التوقيع الالكتروني يجب أن يستوفي بعض الشروط[1].

- وفي الجزائر أصبح للكتابة في الشكل الالكتروني والتوقيع الالكتروني مكانا ضمن قواعد الإثبات في القانون المدني الجزائري من خلال نصي المادتين 323 مكررا و 327 فقرة 2 من ق.م.ج.

والمقصود بالكتابة في الشكل الالكتروني حسب هذا النص.ذاك التسلسل في الحروف أو الأوصاف أو الأرقام أو أية علاقة أو رموز ذات معنى مثل المعلومات والبيانات التي تحتويها الأقراص الصلبة أو المرنة، أو تلك التي تتم كتابتها بواسطة الكمبيوتر وإرسالها أو نشرها عبر الانترنت

كما أن المشرع التونسي في القانون رقم 83-2000 الخاص بتنظيم التجارة الالكترونية والتوقيع الالكتروني أقام التكافؤ بين المحررات الالكترونية والمحررات الورقية ولكنه قيد ذلك بشروط لتفادي الاستغلال غير المشروع للتوقيع الالكتروني، وأكد على ذلك في الفصل 5 من هذا القانون، وفي الفصل 6 منه.

عند مقارنة المشرع المغربي بالتونسي نجد أن المغربي هو الآخر يشترط أن يكون للوثيقة المحررة على دعامة الكترونية نفس القوة الاثباتية التي للوثيقة المحررة على الورق. لتأكيد ذلك أدخل تعديلات

[1] تنص المادة 6 على: " يمكن لكل من يرغب في إمضاء وثيقة الكترونية إحداث إمضائه الالكتروني بواسطة منظومة موثوق بها يتم ضبط مواصفاتها التقنية بقرار من الوزير المكلف بالاتصالات".

على قانون العقود والالتزامات المغربي همّ الفصول الآتية: [1-417 و 2-417 و 3-417]، ولكن ربط ذلك بشروط منها:

- أن يكون بالإمكان التعرف بصفة قانونية على الشخص الذي صدرت عنه الوثيقة المحررة بشكل الكتروني، ومحفوظة وفق شروط من شأنها ضمان تماميتها، ومدعمة للتوقيع الالكتروني.

وأقر المشرع على أن المحرر الالكتروني، يرقي إلى درجة الرسمية وذلك إذا وضع التوقيع على المحرر أمام موظف عمومي له صلاحية التوثيق.[1]

فإذا كانت التجارة الالكترونية والتعاقد والتوقيع الالكتروني من بين الأمور التي عمد المشرع العربي إلى الاهتمام بها بشكل معقول، فإن الجانب الأكثر أهمية الذي أولاه هذا الأخير عناية زائدة هو ما يتصل بمكافحة الجريمة الالكترونية.

5- المشرع العربي والجرائم الالكترونية

إذا كانت جرائم الانترنت جرائم متعددة ومتنوعة، ويستعصي حصرها بسهولة، فإن الأمر ذاته ينطبق على تعريفها، إلا أنه مع ذلك يمكن اعتبارها:

1-جميع الأفعال المخالفة للقانون والشريعة، والتي ترتكب بواسطة الانترنت.

2- هي الجرائم التي يتم ارتكابها، إذا قام شخص باستخدام معرفته بالانترنت بعمل غير مشروع قانونا، ومستخدما الحاسوب كموضوع للجريمة.

ورغم صعوبة ضبط وصعوبة مكافحة جرائم الانترنت على الصعيد العربي إلا أن هناك جهود جماعية وفردية في محاربة قراصنة الانترنت وإحالتهم قانونا على المحاكم. ولكن أيضا هذه الجهود فيها

[1] عمر نجوم: الحجية القانونية لوسائل الاتصال الحديثة: دراسة تحليلية في نظام الإثبات المدني. أطروحة لنيل الدكتوراه: كلية الحقوق الدارالبيضاء 2003-2004 ص 137.

ما هو مضاد لحرية التعبير ويمكن أن نذكر من بين الجهود الجماعية العربية، ما حصل من تعاون عربي في هذا الصدد بمناسبة انعقاد "مؤتمر وزراء الداخلية العرب في تونس سنة 2006". عندما قدم وزير الداخلية المصري اقتراحا بتوحيد الجهود العربية للعمل على استصدار قرار من مجلس الأمن بالتزام الدول التي تتبعها المؤسسات، والشركات العالمية الكبرى، التي تباشر إدارة واستقبال شبكات المعلومات والاتصال، بإغلاق المواقع التي تبث بيانات للأفكار والأيديولوجيات المتطرفة. قد قوبل هذا المطلب بمواجهة عنيفة من قبل المنظمات الحقوقية التي اعتبرت مثل هذا الإجراء ما هو إلا تقييد لحرية الرأي والتعبير.

كما تحركت مصر والسعودية مرة أخرى في مؤتمر وزراء الإعلام العرب 2008 "بتقديم مسودة مشروع مقترح لتشكيل لجنة عليا للإعلام الالكتروني"، وهو خطوة أخرى ظاهرها مكافحة الجرائم الالكترونية وباطنها هو تقييد حرية الرأي والتعبير، مستندين على أن الإعلام الالكتروني في الدول العربية يتسم بالخطورة ولا تحكمه أية معايير أو ضوابط مهنية واضحة يمكن الالتزام بها.

6- نماذج من القوانين الداخلية لمكافحة جرائم الانترنت عربيا

جل الدول العربية وضعت قوانين لمكافحة جريمة الانترنت، فعلى امتداد الوطن العربي من المحيط إلى الخليج، نجد ترسنة قانونية تنظم جرائم الانترنت[1].بدأت هذه الحركة في الظهور والانتشار منذ بداية الألفية الثالثة وعلى الأخص منذ منتصف العشرية الأولى منها، وعلى سبيل المثال ظهرت في معظم الدول العربية قوانين لمنع ومحاربة الإرهاب الذي أدخل في القوانين الجنائية، حيث تم التأكيد من خلالها على استخدام الانترنت في القضايا المتصلة بالإرهاب والتشديد عليها، والأمر هنا لا

[1] الصعيد العربي هناك دول قد أصدرت قوانين لمكافحة الجريمة الالكترونية، بينما أن دول أخرى عملت على سد الفراغ التشريعي الحاصل في مجموعة القانون الجنائي فيما يتعلق بتجريم الأفعال المرتبطة بتكنولوجيا المعلومات، ووضع العقوبات الملاءمة لها.
لمزيد من التوضيح : أنظر: محمود عبده الدلالعة: الحماية القانونية لتكنولوجيا المعلومات (برامج الحاسب الآلي). مرجع سابق

يقتصر على التشريع المغربي لسنة 2003 أو على التشريع التونسي والمصري، بل يهم جل تشريعات دول المنطقة.

إن ما كان سائدا في الأدبيات القانونية العربية الخاصة بالانترنت هو أن هناك فراغ قانوني على الصعيد العربي يحول دون تحجيم وكبح هذا الوحش الالكتروني، لكن هذا الاعتقاد صار اليوم غير ذي جدوى. ولتأكيد ذلك بالحجة والدليل القاطع سوف نحاول إيراد بعض نماذج القوانين العربية الخاصة بمكافحة ومحاربة الجرائم المعلوماتية مثل القانون السوداني سنة 2006، وكذلك قانون الإمارات العربية المتحدة، أي القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات. وقانون المملكة العربية السعودية المتعلق: بنظام مكافحة جرائم المعلوماتية، الصادر بالمرسوم الملكي رقم:17 بتاريخ 1428/3/8.

إذا كان من واجب المشرع أن ينتج نصوصا قانونية تؤطر الظواهر الاجتماعية الجديدة، فإن من واجبه كذلك أن تكون القواعد التي يصوغها جد واضحة وخالية من الغموض، حتى لا تكون محل تفسير خاطئ أو مغمض من طرف السلطة التنفيذية[1]، ولعل المثال الذي يمكن سوقه هنا، ما يتردد في كل التشريعات العربية الخاصة بمكافحة جريمة الانترنت، بحيث لا يخلو أي قانون منها. وتتكرر فيه بنفس الغموض، ويتعلق الأمر بالنظام العام والأمن العام والأخلاق العامة. إن هذه الألفاظ عامة وفضفاضة وتحتمل مختلف أوجه التأويل، بل إن مفهوم النظام العام قد يتسع ويضيق تبعا للظرفية السياسية التي يمر بها البلد. فمفهوم النظام العام عندما تكون الدولة في حرب، أو بها اضطرابات اجتماعية هو غير مفهوم النظام العام في حالة الاستقرار والهدوء.

[1]Samia MIHOUB : « la question le l'Internet arabe ou quand les états se trompent de cible, http://www.africultures.com/php/index.php?nav=article&no=7494.

وما نلاحظه فيما يخص التشريع العربي للانترنت هو الطابع الموحد والمشترك لنصوصه. إن هذه الأخيرة تكاد تكون مصاغة وبنفس الكيفية ونفس النمط، ويتضح ذلك في تشريعات الانترنيت في جميع الدول العربية تقريبا دون أدنى تمييز بينها.

ويمكن أن نجمل الجرائم التي وردت في هذه التشريعات على النحو الآتي:

أ- جرائم نظم ووسائط شبكات المعلومات:

كدخول المواقع وأنظمة المعلومات المملوكة للغير- التصنت أو التقاط أو اعتراض الرسائل – دخول المواقع وأنظمة المعلومات من موظف سام- جريمة دخول المواقع عمدا قصد الحصول على معلومات أوبيانات أمنية- إعاقة أو تشويش أو تعطيل الوصول للخدمة.

ب- الجرائم الواقعة على الأموال والبيانات والاتصالات بالتهديد والابتزاز:

- الاحتيال أو انتحال الشخصية أو صفة غير صحيحة- الحصول على أرقام أو بيانات بطاقات الائتمان- الانتفاع دون وجه حق بخدمة الاتصال.

ج- جرائم النظام العام والآداب العامة:

- الإخلال بالنظام العام والآداب- إنشاء أو نشر مواقع بقصد ترويج أفكار وبرامج مخالفة للنظام العام الآداب- انتهاك المعتقدات الدينية أو حرمة الحياة الخاصة- الإساءة إلى السمعة.

د- جرائم الإرهاب والملكية الفكرية:

- إنشاء أو نشر مواقع للجماعات الإرهابية- جريمة نشر المصنفات الفكرية.[1]

[1]Samia MIHOUB, op. cit.

هـ- جرائم الاتجار في الجنس البشري والدعارة والمخدرات وغسل الأموال- الاتجار أو الترويج للمخدرات أو المؤثرات العقلية- غسل الأموال.

و- الجرائم المتعلقة بأمن الدولة وسلامتها الداخلية والخارجية.

إن التمعن في قراءة النصوص المنظمة لجرائم الانترنت في التشريعات العربية تكشف عن حقيقة متواترة في جل هذه التشريعات، ألا وهي اهتمامها الكبير عند تنظيم الانترنت وضبطه، بجعل حماية الدولة وأمنها كهدف أسمى من طرف المشرع قبل حماية أمن المواطن، وهذه مسألة واضحة على مستوى النصوص. ومن أهم الأمور التي أولتها هذه التشريعات أهمية قصوى إلى جانب أمن الدولة الحفاظ على النظام العام الذي يتواتر فيها بنفس الصيغ والمعنى. ففي التشريع السعودي نجد مثلا المادة:6 المقطع "أ" منها ينص على تجريم "إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية أو الآداب العامة، أو الحياة الخاصة..."

- أما التشريع السوداني فقد خصص فصلا كاملا لجرائم النظام العام والآداب والإخلال بهما. وهو الفصل الرابع وخاصة المادة:14 منه.
- أما التشريع الإماراتي رقم 2 لسنة 2006 "في شأن مكافحة جرائم تقنية المعلومات" فنجد المادة:20 منه تنص على: "كل من أنشأ موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لأية مجموعة تدعو لتسهيل وترويج برامج وأفكار من شأنها الإخلال بالنظام العام والآداب العامة يعاقب بالحبس مدة لا تزيد على خمس سنوات".

ومن بين الأمور التي ركزت عليها التشريعات العربية المتعلقة بالجرائم الالكترونية وتتردد وباستمرار فيها مسألة حماية القيم الدينية والعائلية، ومنع البورنوغرافية. فالتشريع الإماراتي كان أكثر وضوحا فيما يخص الإساءة إلى الدين الإسلامي وإلى الديانات السماوية الأخرى، وهذا ما تؤكده المادة 15 منه- وأردف في المادة الموالية أي المادة:16 التأكيد على ما يلي:" كل من اعتدى على أي

من المبادئ أو القيم الأسرية أو نشر أخبارا أو وصورا تتصل بحرمة الحياة الخاصة أو العقلية للأفراد، ولو كانت صحيحة عن طريق شبكة المعلومات أو إحدى وسائل تقنية المعلومات يعاقب بالحبس مدة لا تقل عن سنة، وبالغرامة التي لا تقل عن خمسين ألف درهم، أو بإحدى هاتين العقوبتين".[1]

– والملاحظ هنا، هو كون التشريع العربي للانترنت ركز كل اهتماماته على ما من شأنه أن يجعل حماية الدول، أسمى هدف من أهدافه، وأكبر هاجس من هواجسه وفي نفس الآن التركيز على النظام العام. بينما أن حماية المواطن لم يدقق فيها بالصورة المطلوبة والمرجوة. وهذه القاعدة تسري على جل التشريعات المنظمة لجرائم الانترنت في الدول العربية[2].

ومن المعلوم أن حماية الأمن الرقمي يمكن أن يحيل على مفاهيم متعددة تتراوح مابين حماية الأشخاص، وحماية المجموعات وغيرها.

من هنا نتساءل لماذا لم تهتم هذه التشريعات بحماية المجموعات الاثنية والدينية، والثقافية... لماذا لم تشدد أكثر على حقوق المرأة وعلى دعارة الأطفال وعلى الأحقاد العرقية؟ إن الأمور المشار إليها لا يمكن أن تبقى مهملة، إن لم يكن من كل قوانين الدول العربية فعلى الأقل في بعض هذه القوانين. فإذا كانت الدول العربية تغالي كثيرا في مراقبة الانترنت، فإنها في نفس الآن تغيب عنها بنفس الصرامة والحدة مراقبة جرائم الدعارة و دعارة الأطفال، وجرائم العنصرية، التي تنتشر بشكل حر على فضاء الانترنت المفتوح[3].

– فإذا كانت هذه الدول تلجأ باستمرار إلى محاكمة ومعاقبة مستخدمي الانترنت عندما يتعلق الأمر بارتكاب بعض الجرائم، فإنها ومن واجبها كذلك أن تبدل جهودها من أجل القيام بحملات تحسيسية للحماية من المخاطر التي يمكن أن تصادف القاصرين ومختلف مستعملي الانترنت. لقد كان من نتائج غياب التحسيس ما كشف عنه تقرير: مركز حرية الإعلام للشرق

[1]Samia MIHOUB : la question le l'Internet arabe où quand les états se trompent de cible.
[2]Samia MIHOUB : op.cit.
[3]مالك خدام: جرائم الحاسب والانترنت... ارتفاع معدل استغلال الأطفال جنسيا جريدة الثورة: الاثنين 2005/3/7

الأوسط وشمال إفريقيا في تقريره الشهير حول "جرائم الانترنت ضد الأطفال في المغرب"[1]، عندما أوضح المخاطر التي تهدد الأطفال واستغلالهم على شبكة الانترنت، وذلك في غياب أية مقاربة جدية وحقيقية تتبناها هذه الدول بغية حماية الأطفال من المحتويات المشتملة على الخلاعة والدعارة المتداولة باستمرار على شبكة الانترنت.

إن الحافز المهيمن على ممارسات الدول العربية التشريعية في مجال تنظيم الانترنت محكوم بالهم السياسي وهاجس الأمن العام والنظام العام بمضمونه السياسي، ولعل ذلك ما يستشف من تقرير "برنامج الأمم المتحدة للتنمية البشرية في الوطن العربي لسنة 2004" الذي يوضح عند حديثه على قيم الحرية، والتعددية وحقوق الإنسان، كيف أن المشرع يضع نصوصا جنائية وغير جنائية، تقيد الحريات العامة، وتعتبر حرية الصحافة المكتوبة والسمعية البصرية، وممارسة حرية التعبير كنشاطات مزعجة ينبغي تحجيمها[2].

وعلى العموم يمكن القول إن الدول العربية لم يعمم فيها بعد وبشكل كافي، إصدار قوانين خاصة بجرائم الانترنت، باستثناء بعض النماذج المشار إليها مثل الإمارات العربية المتحدة، وتونس، والسودان ويبدو اليوم أن هناك لدى هذه الدول شعور عميق بتنظيم الجرائم المرتكبة عن طريق الانترنت، وهي تحضر مشاريع قوانين في هذا الاتجاه. ويعود سبب الاهتمام بتنظيم جرائم الانترنت إلى كون القانون الجنائي التقليدي غير قادر على استيعاب الجرائم الالكترونية الحديثة النشأة والتي ظهرت لأول مرة كمصطلح في استراليا عام 1988.

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

[1] مركز حرية الإعلام بالشرق الأوسط وشمال إفريقيا: القاصرون وجرائم الانترنت في المغرب سبتمبر 2006.

[2] Nouri LAJMI : « la liberté de l'information à l'ère du cyberespace », Revue Tunisienne de la communcation n° 37-38, Janvier/ décembre 2001

العربية، على غرار ما حصل في النظام الإقليمي الأوروبي، لما وضعت الاتفاقية الأوروبية "حول جرائم الانترنت المرخص بها من قبل اللجنة الأوروبية ب "بودابيست في 23 نوفمبر 2001، والتي يمكن اعتبارها من بين التشريعات الأكثر تطورا، حيث عرفت تسع جرائم مجتمعة في أربع فئات هي:[1]

- الجرائم التي تمس حرية الحاسوب وسلامته.
- سوء النية المقصود في استعمال الحاسوب (مثل جريمة التزوير أو الاحتيال المرتبطة بالحاسوب).
- الجرائم المرتبطة بمختلف قوانين النشر والترويج
- الجرائم المتعلقة بالجنس (أي الجرائم التي لها علاقة بالدعارة وبالاعتداء الجنسي على الأطفال).

ومن المعلوم أن الاتفاقية العربية لمكافحة جريمة الانترنت عند وضعها قد تتضمن ما يعبر عن الخصوصية العربية الإسلامية للمجتمعات العربية شريطة أن تكون تلك الخصوصية إضافة جديدة في مجال حقوق الإنسان، وليس نقصا لما هو متعارف عليه عالميا في هذا المجال.

ولعل مؤتمر الأمم المتحدة الثاني لحقوق الإنسان في فيينا عام 1992 قد فصّل كثيرا في هذا الموضوع، موضوع الخصوصية.[2]

- ويدفعنا موضوع الخصوصية إلى طرح حق الخصوصية وحماية البيانات الشخصية وكيف تم التعامل معها على مستوى التشريعات العربية المنظمة للانترنت، باعتبارها حقا من حقوق الإنسان الأساسية والجوهرية.

ي_تشريعات القانون الجزائرى

[1]Conseil de l'Europe : « convention sur la cybercriminalité », Budapest, 23 Novembre 2001. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

[2]محمد أحمد: حقوق الإنسان بين الخصوصية والعالمية، رسالة لنيل دبلوم الدراسات العليا المعمقة: كلية الحقوق الدار البيضاء 2003

صادق مجلس الأمة الجزائرى يوم الأربعاء / 8 يوليو الحالى / 2009 بالاجماع على مشروع القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ويتضمن القانون 19 مادة موزعة على 6 فصول و هو ثمرة عامين من التحضير والدراسة والتحليل والمقارنة مع أحدث القوانين وقامت بإعداده نخبة من رجال القانون بمشاركة خبراء و مهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المعنية.

كما يتضمن القانون أحكاما خاصة بالمراقبة الإلكترونية التي لايجوز إجراؤها إلا بإذن من السلطة القضائية المختصة و في حالات تم تحديدها وهي الأفعال الموصوفة بجرائم الإرهاب والتخريب و الجرائم الماسة بأمن الدولة أو حالة توفر معلومات عن اعتداء محتمل يهدد منظومة من المنظومات المعلوماتية لمؤسسات الدولة أو الدفاع الوطني أو النظام العام.

وينص القانون على انشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال و مكافحته تتولى تنشيط و تنسيق عمليات الوقاية من الجرائم المعلوماتية ومساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم.

وتتكفل اللجنة أيضا بتبادل المعلومات مع نظيراتها في الخارج، علما بأن القانون أكد على مبدأ التعاون الدولي من منطلق المعاملة بالمثل.

قانون رقم 09-04مؤرخ في 14شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها[1].

[1] ج.ر.ج.ج.د.ش: رقم 47.

المبحث الثاني:أشكال الاعتداءات على المعلومة

يقصد بالحماية المباشرة للمعلومات على شبكة الأنترنت هو حماية المعلومات بطريقة مباشرة من أي اعتداء، وذلك بتحريم أفعال الاعتداء المختلفة التي توجه ضدها وذلك بالنظر إلى جرائم السلوك والنتيجة.

ولذلك سوف نتناول هذا المبحث في ثلاثة مطالب كالتالي:

- المطلب الأول: الاعتداء على حقوق الملكية الفكرية بطريقة الأنترنت
- المطلب الثاني: الاعتداء على البيانات الشخصية والخصوصية المعلوماتية بطريق الأنترنت
- المطلب الثالث: الاعتداء على القيمة الاقتصادية والأمنية للمعلومات بطريق الأنترنت

المطلب الاول: الاعتداء على حقوق الملكية الفكرية بطريق الانترنت.

يواجه المؤلف دائما التزامان متناقضان هما: الرغبة في الشهرة التي تشجعه على نشر مصنفه، ورغبته في الاعتراف به كمؤلف وحيد للمصنف والذي قد يدفعه إلى عدم نشره والاحتفاظ به.

ورغم أن المؤلف قد نجح على مر العصور في أن يوقف بين هذين الالتزامين، فإن ذلك كان ضد رغبة السلطات العامة في الدول بصفة عامة، نظرا لأن المصنف له أهمية اجتماعية نقاش بقدرته على إثراء الثقافة الوطنية.

إذن فإن السلطات العامة تسعى إلى إحداث توازن في سلطات المؤلف على مؤلفه حتى تحافظ على ازدهار الفن مع ضمان مستوى كاف من الحماية للمؤلفين يتمثل في الحماية القضائية والاعتراف بالحقوق المادية والأدبية لهم على مصنفاتهم لتشجيع الابتكار وتقنيات نشر المصنف متعددة ومتطورة بشأن إمكانية لنسخ أو إعادة استخدام المصنف.

وسوف نتناول في هذا المطلب نقطتين:

- أولا: محل الحماية الجنائية في الاعتداء على حقوق الملكية الفكرية
- ثانيا: الاعتداء على حقوق المؤلف في التشريع المقارن

أولا: محل الحماية الجنائية في الاعتداء على حقوق الملكية الفكرية

أيا كان شكل المصنف، طالما أنه يتميز بطابع ابتكاري يكون هو محل الحماية الجنائية، وما زال القانون لا يحمي الفكرة المجردة ولكنه يشترط أن يكون لهذه الفكرة واقع مادي ملموس وهو المصنف، فالمصنف قد تشمله الحماية الجنائية كمؤلف أو لكونه برمجية حاسوب Softwar، أو أي شكل آخر من أشكال المصنفات التي عرفتها القوانين في مختلف دول العالم وفقا للتطورات التقنية في مجال النشر، مثل المصنفات السمعية البصرية التي يعبر عنها بالصوت، أو الصوت والصورة معا، وفنون الرسم والديكور والأفلام السينمائية والموسيقى، وكذلك مصنفات الوسائط المتعددة، ومصنفات قواعد البيانات التي أضيفت في القانون الفرنسي الصادر في أول يوليو 1998. الذي حدد بشكل واضح إمكانية حماية قواعد البيانات بواسطة حق المؤلف. حيث تضمنت نصوص مواده أن: "مؤلفي المقتطفات لمصنفات أو بيانات مختلفة مثل قواعد البيانات يتمتعون بحماية حقوق المؤلف".

كما نص أيضا في المادة 140 من قانون الملكية الفكرية المصري الجديد على أنه: "يتمتع بحماية هذا القانون حقوق المؤلفين على مصنفاتهم الأدبية والفنية، وبوجه خاص المصنفات الآتية... قواعد البيانات سواء كانت مقروءة من الحاسب الآلي أو من غيره".[1]

فالحماية الجنائية لحقوق الملكية الفكرية تنص على حماية المصنف مهما اختلفت وتعددت أشكاله في التشريعات المقارنة.

[1] المذكرة الإيضاحية للقانون رقم 354 لسنة 1954م الصادر بشأن حماية حقوق المؤلف في مصر والذي ألغي، وتم العمل بالقانون رقم 82 لسنة 2002 بشأن حماية الملكية الفكرية.

ومن الملاحظ أن التشريعات المقارنة لم تحدد مفهوم أو مصطلح مصنف، ولذلك سوف نعرض لمفهوم المصنف وأبوة المؤلف لمصنفه كالآتي:

1- مفهوم المصنف:

لكي تتوافر الحماية الجنائية والقانونية للمصنف، يجب أن يتوافر في هذا الأخير، شرط الابتكار فهو إبداع فكري وليس شيئا ماديا، ولكنه لا يكتسب الحماية إلا إذا تم التعبير عنه بشكل مادي وتسجيله لدى الجهات المختصة، وإيداع نسخ منه سواءا كانت مؤلفات أو برمجيات أو قواعد بيانات، وكذلك مخطوطة بيانية لموضوع الاختراع المراد تسجيله، أو مجسم للعلامة التجارية والرسومات المراد تسجيلها لدى الجهة التي تمنحها الدولة اختصاصها بذلك.

حيث نصت المادة 138/ فقرة أولى من القانون الخاص بحماية الملكية الفكرية في مصر رقم 82 سنة 2002 على أن المصنف هو: "كل عمل مبتكر أدبي أو فني أو علمي أيا كان نوعه أو طريقة التعبير عنه أو أهميته أو الغرض من تصنيفه".

ويشتمل المصنف على اسم المؤلف وعنوانه ومادته أو موضوعه، وأن أي اعتداء على اسم المؤلف أو عنوانه أو مادة المؤلف إنما يمثل اعتداءا على حقوق الملكية الفكرية للمؤلف، وهو ما قررته التشريعات المقاربة.

وذلك ما جاء في المادة 112 فقرة 4 من قانون الملكية الفكرية الفرنسي، حيث اهتم هذا القانون بعنوان المصنف الأدبي بنصها على أن "عنوان المصنف الأدبي، ...، مشمولا بالحماية مثل المصنف ذاته، ولا يمكن لأحد استخدام هذا العنوان لإعداد مصنف من ذات النوع، حتى ولو لم يكن المصنف غير مشمول بالحماية كما هو مقرر في المواد من 123/ف1 إلى 123/ف3، مما يجعل ذلك قابل للالتباس".[1]

[1] CP/fr.art.L.112/4.

وفي الواقع العملي، يلاحظ أن الاعتداءات قد تتم ضد مادة المصنف، ولذلك نجد أن الإشارة إلى حماية حقوق المؤلف، إنما هي إشارة إلى حماية مادة المصنف في المقام الأول، والواقع أن الحماية القانونية يجب أن تمتد إلى الأركان الأخرى، كعنوان المصنف، واسم المؤلف لكونها أمورا لازمة في تكوينه طالما توافر فيها عنصر الابتكار.

ولقد ثار مشكل حول مدى مشروعية نشر المقالات الصحفية التي يقوم بتحريرها الصحفي للجريدة التي يعمل بها على W.W.W. (الأنترنت) بدون إذن صحفي، وهل يمكن اعتبار هذه المقالات الصحفية من ضمن المصنفات الأدبية المبتكرة، ومن ثم تتمتع بالحماية القانونية؟

في الواقع، لا توجد صعوبة في أن تكون الكتابات الصحفية من المصنفات الأدبية المبتكرة، وبالتالي فإنها تتمتع بالحماية القانونية والجنائية. لأن الصحفي هو مؤلف هذه المقالات وبالتالي تتمتع بالحماية بهذه الصفة طالما أن المقال ممهور باسم مؤلفه، من جهة، ومن جهة أخرى له طابع الابتكار. وهذا ما أكدت عليه المادة 14 من قانون حماية حق المؤلف المصري رقم 354 لسنة 1954 المعدل بالقانون رقم 82 لسنة 2002 حيث جاء في نص المادة:

"لا يجوز للصحف أو النشرات الدورية أن تنقل المقالات العلمية أو الأدبية أو الفنية أو الروايات المسلسلة والقصص الصغيرة التي تنشر في الصحف والنشرات الدورية الأخرى دون موافقة مؤلفيها".

إذن هذه المادة تحفظ الحق الأدبي للمؤلف، وبالتالي لابد من الحصول على موافقة الصحفي على ترقيم مقالاته ووضعها على موقع من مواقع شبكة الأنترنت.[1]

2- أبوة المؤلف لمصنفه:

[1] رشدي محمد علي محمد عيد علي، مرجع سبق ذكره، ص116-117.

ويقصد بأبوة المؤلف لمصنفه، هو أن ينسب هذا المصنف إلى مؤلفه، فالمؤلف له الحق وحده في أن ينسب إليه مصنفه، وله حق استغلاله ماديا ولا يجوز لغيره مباشرة هذا الحق دون إذن سابق منه أو ممن يخلفه، وله أن ينزل عن حق الاستغلال هذا بما يشمل مضمونه من الحق في النشر وفي الاشتقاق من المصنف الأصلي.

ويترتب على هذا الحق أنه لا يكون للغير أن ينسخ أو يتناول المصنف المتروك من صاحبه لأنه يظل منسوبا إلى صاحبه وحده.

ثانيا: الاعتداء على حقوق المؤلف في التشريع المقارن

1-على مستوى الدولي:

المشرع المقارن اهتم بتجريم الاعتداء على حقوق المؤلف وبصفة خاصة، تجريم نسخ المصنفات بدون الحصول على إذن من مؤلفها، وذلك نظرا لازدياد المشروعات الإجرامية على حقوق الملكية الفكرية. ونتيجة لذلك ظهرت المحاولات الإقليمية والدولية.

فعلى المستوى الدولي وضع المشرع الدولي اتفاقية الجات GATT/WTO بحيث نصت المادة 61 من هذه الاتفاقية على أنه:[1]

"تلتزم الدول الأعضاء بفرض تطبيق الإجراءات والعقوبات الجنائية كحد أدنى في حالات التقليد العمدي للعلامات التجارية المسجلة، وانتحال حقوق المؤلف على نطاق تجاري، وتشمل الجزاءات التي يجوز فرضها الحبس أو الغرامة المالية أو أيهما بما يكفي لتوفير الردع الذي يتناسب مع مستوى العقوبات المطبقة فيما يتعلق بالجرائم ذات الخطورة المماثلة، وفي الحالات الملائمة تشمل الجزاءات التي يجوز فرضها أيضا حجز السلع المخالفة وأية مواد ومعدات تستخدم بصورة رئيسية في ارتكاب الجريمة

[1] د. أبو العلا علي النمر، الحماية الوطنية للملكية الفكرية، بحث مقدم إلى الندوة العلمية عن التراخيص في مجال الملكية الفكرية وتوسية المنازعات الناشئة عنها، القاهرة في 1998/03/10، دار النهضة العربية، القاهرة، 1998، ص.150.

ومصادرها وإتلافها، ويجوز للبلدان الأعضاء فرض تطبيق الإجراءات والعقوبات الجنائية في حالات أخرى من حالات التعدي على حقوق الملكية الفكرية، سيما حين التعدي عمدا وعلى النطاق التجاري".

وكذلك جاء في المؤتمر الدبلوماسي للمنظمة العالمية للملكية الأدبية والفكرية "WIPO" الويبو المنعقد في جنيف في شهر ديسمبر 1996، أن عملت المنظمة على تطوير اتفاقية برن المتعلقة بحقوق المؤلف، حيث وضعت حماية كبيرة للأعمال الفنية والتمثيلية والإنتاجية للتسجيلات الصوتية وذلك عن طريق إعداد اتفاقية خاصة بحق المؤلف، والثانية خاصة بالأداء والتسجيل الصوتي. وقد عرفت هاتين الاتفاقيتين باتفاقيتي الأنترنت، وقد أشير فيهما إلى مصطلح إدارة حقوق النسخ، وهذا المصطلح يشير إلى المعلومات التي تعرف بالمصنف والمؤلف ومالك الحق في المصنف أو معلومات عن المصطلحات وشروط استعمال المصنف، وأي أرقام أو شفرات تبين هذه المعلومات عندما تكون أي من هذه البيانات ملحقة بنسخة من المصنف أو أو تبرز موصولة في حركة اتصال المصنف بالعامة.

وهذا ما نصت عليه المادتين 12 فقرة 2 من اتفاقية حقوق النسخ والمادة 19 فقرة 2 من اتفاقية العرض والفونوجرام. وقد تضمنت الاتفاقيتين المشار إليهما بعض النصوص التي تحرم الدخول إلى شبكة الأنترنت بقصد العدوان على المصنفات، ونشير إلى الاتفاقية الأوروبية للجريمة الافتراضية التي جرم فيها العدوان على حقوق المؤلف والحقوق المجاورة.

2-على المستوى الإقليمي:[1]

أما على المستوى الإقليمي، فسنذكر بعض التشريعات المقارنة التي عالجت هذا الموضوع وعلى رأسها التشريع المصري، والتشريع الفرنسي، والتشريع الجزائري.

أ- حقوق المؤلف في التشريع المصري:

[1] د. رشدي محمد علي محمد عيد علي، مرجع سبق ذكره، ص.122.

أول قانون صدر بشأن حماية حقوق المؤلف برقم 354 لسنة 1954، المعدل بالقوانين 14 لسنة 1968م. 34 لسنة 1975. ثم تم تعديله بالقانون رقم 38 لسنة 1992، ثم عدل بالقانون رقم 29 لسنة 1994م ثم صدر القانون الجديد في حقوق الملكية الفكرية برقم 82 لسنة 2002.[1]

حيث بين المشرع في المادة 47 من القانون رقم 354 لسنة 1954م العدوان على حقوق المؤلف.[2]

ومن أبرز صور العدوان على حقوق المؤلف، أن قرر المشرع في المواد 5،6،7 من القانون المذكور بعض الحقوق التي يملكها المؤلف وحده دون غيره. وهي كالتالي:

حيث نصت المادة 5 على أنه: "للمؤلف وحده الحق في تقرير نشر مصنفه وفي تعيين طريقة هذا النشر، وله الحق وحده في استخدام مصنفه ماليا، ولا يجوز لغيره مباشرة هذا الحق إلا بعد الحصول على إذن كتابي من صاحب الحق في الاستغلال المالي للمصنف الأصلي أو خلفائه، ويتضمن الإذن طريقة ونوع ومدة الاستغلال".

إذن يستخلص من نص المادة المذكورة أنه أي اعتداء على أي من الحقوق المذكورة في المادة وهي الحق في تقرير نشر المصنف وفي تحديد طريقة النشر، والحق في استغلال مصنفه ماليا، يعد عدوانا على حقوق المؤلف، ولا يجوز لغيره مباشرة الحق في استغلاله بأي صورة بدون الحصول على إذن كتابي سابق من المؤلف حال حياته أو من ورثته بعد وفاته.

وكذلك جاء نص المادة 6 من القانون المذكور على أنه "يتضمن حق المؤلف في الاستغلال أولا: نقل المصنف إلى الجمهور مباشرة بأي طريقة، وخاصة بأحد الصور الآتية: التلاوة العلنية أو التوقيع الموسيقي أو التمثيل المسرحي أو العرض العلني أو الإذاعة اللاسلكية للكلام أو الصوت أو

[1] الوقائع المصرية، (العدد 49 مكرر/غير اعتيادي) في 24 يونيو، سنة 1954م.

[2] د. عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، الطبعة الثانية، 2007، ص.72-73.

للصور أو العروض بواسطة الفانوس السحري أو السينما أو نقل الإذاعة اللاسلكية بواسطة مكبر الصوت أو لوحة التليفزيون بعد وضعها في مكان عام. ثانيا: نقل المصنف إلى الجمهور بطريقة غير مباشرة بنسخ صورة منه تكون في متناول الجمهور، سواء تم ذلك بطريقة الطباعة أو الرسم أو الحفر أو التصوير أو الصب في قوالب أو التسجيل أو النسخ أو التثبيت على اسطوانات أو أشرطة مسموعة أو مرئية أو بأي طريقة أخرى".

وما يستخلص من نص المادة حق المؤلف في استغلال مصنفه مع ذكر صور هذا الاستغلال، وسردت بأنه يمكن نقل المصنف للجمهور بطريقة مباشرة أو غير مباشرة، وأوضحت المادة صور النقل المباشر والغير المباشر من تلاوة علنية... ونسخ صورة من المصنف أيا كان نوعه للجمهور...إلخ.

وكذلك جاء نص المادة 7 من القانون 354 لسنة 1954م بشأن حقوق المؤلف على أنه: "المؤلف وحدة إدخال ما يرى من التعديل أو التحوير على مصنفه، وله الحق في ترجمته إلى لغة أخرى، ولا يجوز لغيره أن يباشر شيئا من ذلك، أو أن يباشر صورة أخرى من الصور المنصوص عليها في المادة الثالثة، إلا بإذن كتابي منه أو ممن يخلفه، ويتم تداول المصنف بعنوانه الأصلي أو ترجمته المطابقة له، ولا يجوز تعديل هذا العنوان أو تغييره إلا بموافقة كتابية من المؤلف أو ممن يخلفه".[1]

فمن مطالعة المادة السابعة، نلاحظ أن للمؤلف وحده الحق في إدخال أي تعديل أو تحوير على مصنفه وكل تعديل أو تحوير أو ترجمة للمصنف دون موافقة مسبقة فإن ذلك يعد جريمة وفقا للمادة 47 من هذا القانون.

وقد أكدت المادة الثالثة من هذا القانون على الحماية، حيث جاء في نص المادة أنه: "يتمتع بالحماية من قام بترجمة المصنف إلى لغة أخرى، أو بتحويله من لون من ألوان الأدب أو الفنون أو العلوم إلى لون آخر، أو من قام بتخليصه أو بتعديله أو بشرحه أو بالتعليق عليه بأي صورة تظهره في

[1] راجع المذكرة الإيضاحية للقانون رقم 354 لسنة 1954م بإصدار قانون حماية حق المؤلف.

شكل جديد، وذلك مع عدم الإخلال بحقوق مؤلف المصنف الأصلي، على أن حقوق المصنف الفوتوغرافي لا يترتب عليها منع الغير من التقاط صور جديدة للشيء المصور، ولو أخذت هذه الصور الجديدة من ذات المكان، وبصفة عامة في ذات الظروف التي أخذت فيها الصورة الأولى".

وبالإضافة إلى ذلك تطرق المشرع المصري إلى حالة جلب المصنفات المنشورة في الخارج إلى مصر بقصد الاستغلال، حيث نصت المادة 2/47 من القانون رقم 354 لسنة 1954، الصادر بشأن حماية حق المؤلف الملغى على أنه: "... من أدخل في مصر بقصد الاستغلال دون إذن من المؤلف أو من يقوم مقامه، مصنفا منشورا في الخارج مما تشمله الحماية التي تفرضها أحكام هذا القانون".[1]

حيث يظهر من هذا النص أن إدخال المصنفات المنشورة خارج مصر إلى مصر بقصد التداول والاستغلال، يجب أن يكون من حق المؤلف الذي له الحق في تقرير نشره واستغلاله بأية طريقة، ولا يكون لغيره مباشرة هذا الحق دون الحصول على إذن كتابي سابق من المؤلف حال حياته، أو ممن يخلفه بعد وفاته.

وكذلك جاء المشرع المصري بنص صريح حول تجريم تداول المصنفات المقلدة: وذلك في المادة 3/47 والتي نصت على: "من باع أو عرض للبيع أو للتداول أو للإيجار مصنفا مقلدا مع علمه بالتقليد".

كما نصت الفقرة الرابعة من نفس المادة المذكورة: "من قلد في مصر منشورا في الخارج، أو باعه أو عرضه للبيع أو للتداول أو للإيجار أو صدره أو شحنه من الخارج مع علمه بتقليده، وتتعدد العقوبة بتعدد المصنفات محل الجريمة".

[1] أنظر عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني، الجزء الثامن، حق الملكية، الطبعو الثانية (نادي القضاة)، 1991، ص.354.

إذن الفقرة 3 تعرضت لحالة المصنف المقلد داخل البلاد، أما الفقرة 4 فقد تعرضت للمصنف المنشور خارج البلاد ويتمثل الركن المادي لهذه الجرائم في البيع والعرض للبيع أو للتداول أو الإيجار لمصنف مقلد وذلك دون اشتراط مشاركة البائع في التقليد. ويتبين أن القصد الجنائي في هذه الجريمة هو القصد العمدي الذي يتطلب توافر العلم من الجاني وقت ارتكاب الجريمة بأن المصنف مقلد وتتجه إرادته نحو بيع المصنف.

وقد صدر القانون رقم 82 لسنة 2002م بشأن حقوق الملكية الفكرية الجديد والذي تضمن الباب الثالث منه حقوق المؤلف والحقوق المجاورة في المواد 138 إلى 188، وقد جاء هذا القانون متوافقا مع ما جاء في اتفاقية الجات.

ولقد وضع المشرع المصري في المادة 181من القانون 2002/82، صور العدوان على حقوق المؤلف مع العقوبات المقررة لها.

حيث نصت هذه المادة على: "مع عدم الإخلال بأية عقوبة أشد في قانون آخر، يعاقب بالحبس مدة لا تقل عن شهر وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرة آلاف جنيه، أو بإحدى هاتين العقوبتين، كل من ارتكب الأفعال الآتية:

أولا: بيع أو تأجير مصنف أو تسجيل صوتي أو برنامج إذاعي محمي طبقا لأحكام هذا القانون، أو طرحه للتداول بأية صورة من الصور بدون إذن كتابي مسبق ومن المؤلف أو صاحب الحقوق المجاورة.

ثانيا: تقليد مصنف أو تسجيل صوتي أو برنامج إذاعي أو بيعه أو عرضه للبيع أو للتداول أو للإيجار مع علمه بتقليده...

وتتعدد العقوبات بتعدد المصنفات أو التسجيلات أو البرامج الإذاعية أو الأداءات محل الجريمة...إلخ.

ويلاحظ أن المشرع في القانون الجديد لم يخرج على الأحكام العامة المقررة في القانون رقم 354 لسنة 1954، وأوضح من خلال هذه المادة الاعتداءات المختلفة التي تتم على حقوق المؤلف.

ب- حقوق المؤلف في التشريع الفرنسي:[1]

المشرع الفرنسي اعترف للمؤلف بحقوق مطلقة في مواجهة الغير، وذلك في قانون الملكية الفكرية الصادر في مارس 1957م، في المواد 111 فقرة أولى والمواد 122 فقرة 2 و3.

كما نص المشرع الفرنسي في المادة 335 فقرة 2 من قانون العقوبات الفرنسي الجديد على جريمة التقليد أو الاستنساخ، حيث قرر المعاقبة بالحبس سنتين وغرامة مليون فرنك لكل من استنسخ كتب أو ألحان موسيقية أو ر سم أو رسم ألوان، ويسري ذلك أيضا على كل ما يمكن إعادة طباعته كليا أو جزئيا، وتسري هذه العقوبات على كل من جلب أو صدر مثل هذه المواد المستنسخة.

وكذلك توسع المشرع الفرنسي في المادة 335 الفقرة 3 من قانون العقوبات الجديد في مدلول العدوان بالتقليد، حيث قررت المعاقبة على بث أو نشر أو استنساخ أي مصنف فكري بأية وسيلة، لأنه يمثل عدوانا على حق المؤلف.

ويلاحظ أن المادة 122 فقرة 25 من قانون الملكية الفرنسي تعرضت لبث المصنفات عبر W.W.W. "الأنترنت".

ج- حقوق المؤلف في القانون الجزائري:

ما زالت حقوق المؤلف إلى يومنا هذا عرضة للسطو والاعتداء منذ نشأته وكانت ردود الفرد والجماعة في بادئ الأمر تجاه هذه الظاهرة مقتصرة على الاستنكار الأخلاقي والنفور الأدبي ومع بداية هذا العصر الحديث انتقلت إلى مرحلة الحماية القانونية المنظمة وقد كان موقف المشرع الجزائري

[1] د. رشدي محمد علي محمد عيد علي، مرجع سبق ذكره، ص.128.

من ذلك صريحا من خلال الأمر رقم 05/03 مؤرخ في جمادى الأولى عام 1424 الموافق لـ19 يوليو سنة 2003 بخصوص حق المؤلف والحقوق المجاورة.[1]

ولقد جاء هذا الأمر كالآتي:

إن رئيس الجمهورية، بناء على الدستور، لاسيما المواد 38 و 122 و124 منه،

- و بمقتضى الأمر رقم 66-154 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 و المتضمن قانون الإجراءات المدنية، المعدل و المتمم،
- و بمقتضى الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 و المتضمن قانون الإجراءات الجزائية، المعدل و المتمم،
- و بمقتضى الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 و المتضمن قانون العقوبات، المعدل و المتمم،
- و بمقتضى الأمر رقم 73-26 المؤرخ في 4 جمادى الأولى عام 1393 الموافق 5 يونيو سنة 1973 والمتضمن انضمام الجزائر إلى الاتفاقية العالمية الخاصة بحق التأليف لسنة 1952 والمراجعة في باريس في 24 يوليو سنة 1971،
- وبمقتضى الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 و المتضمن ق.م، المعدل و المتمم،
- وبمقتضى الأمر رقم 75-59 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 و المتضمن القانون التجاري، المعدل و المتمم،
- وبمقتضى القانون رقم 84-11 المؤرخ في 09 رمضان عام 1404 الموافق09 يونيو سنة 1984 و المتضمن قانون الأسرة،

[1] مجلة الموسوعة القضائية الجزائرية، موسوعة الفكر القانوني، العدد الثالث، ص.67.

- وبمقتضى القانون رقم 90-22 المؤرخ في 27 محرم عام 1411 الموافق18 غشت سنة 1990 و المتعلق بالسجل التجاري،المعدل و المتمم،
- و بمقتضى الأمر رقم 96-16 المؤرخ في 16 صفر عام 1417 الموافق 02 يوليو سنة 1996 والمتعلق بالإيداع القانوني،
- وبمقتضى الأمر رقم 97-10 المؤرخ في 27 شوال عام 1417 الموافق 6 مارس سنة 1997 والمتعلق بحقوق المؤلف و الحقوق المجاورة،
- وبمقتضى الأمر رقم 03-03 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003 و المتعلق بالمنافسة،
- و بمقتضى المرسوم الرئاسي رقم 97-341 المؤرخ في 11 جمادى الأولى عام 1418 الموافق 13 سبتمبر سنة 1997 و المتضمن انضمام الجمهورية الديمقراطية الشعبية، مع التحفظ، إلى اتفاقية برن لحماية المصنفات الأدبية و الفنية المؤرخة في 9 سبتمبر سنة 1886 والمتممة بباريس في 4 مايو 1896 و المعدلة ببرلين في 13 نوفمبر سنة 1908 و المتممة ببرن في 20 مارس سنة 1914 و المعدلة بروما في 2 يونيو سنة 1928، و بر وكسل في 26 يونيو سنة 1948، واستوكهولم في 14 يوليو سنة 1967، و باريس في 24 يوليو سنة 1971 والمعدلة في 28 سبتمبر سنة 1979،

و بعد الاستماع إلى مجلس الوزراء، يصدر الأمر الآتي نصه:

أحكام تمهيدية

المادة الأولى: يهدف هذا الأمر إلى التعريف بحقوق المؤلف و الحقوق المجاورة، و كذا المصنفات الأدبية أو الفنية المحمية و تحديد العقوبات الناجمة عن المساس بتلك الحقوق.

المادة 2: تضمن أحكام هذا الأمر حماية حقوق:

- مؤلف المصنفات الأدبية أو الفنية،فنان الأداء أو العازف، و منتج التسجيلات السمعية أو السمعية البصرية، و هيئات البث الإذاعي السمعي أو السمعي البصري.
- القواعد الخاصة بالتسيير الجماعي للحقوق و حماية مصنفات التراث الثقافي التقليدي والمصنفات الوطنية للملك العام.[1]

الباب الأول

حماية المصنفات و حقوق المؤلف

الفصل الأول

المصنفات المحمية

المادة 3: يمنح كل صاحب إبداع أصلي لمصنف أدبي أو فني الحقوق المنصوص عليها في هذا الأمر.

تمنح الحماية مهما يكن نوع المصنف و نمط تعبيره و درجة استحقاقه ووجهته، بمجرد إيداع المصنف سواء أكان المصنف مثبتا أم لا بأية دعامة تسمح بإبلاغه إلى الجمهور.

المادة 4: تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يأتي:

أ) المصنفات الأدبية المكتوبة مثل: المحاولات الأدبية، و البحوث العلمية والتقنية، والروايات، والقصص، و القصائد الشعرية، و برامج الحاسوب، والمصنفات الشفوية مثل المحاضرات والخطب و المواعظ و باقي المصنفات التي تماثلها،

ب) كل مصنفات المسرح والمصنفات الدرامية، والدرامية الموسيقية والإيقاعية، والتمثيليات الإيمائية،

ج) المصنفات الموسيقية، المغناة أو الصامتة،

[1] مجلة الموسوعة القضائية الجزائرية، مرجع سبق ذكره، ص.68.

د) المصنفات السينمائية و المصنفات السمعية البصرية الأخرى سواء كانت مصحوبة بأصوات أو بدونها،

هـ) مصنفات الفنون التشكيلية و الفنون التطبيقية مثل:الرسم، و الرسم الزيتي، والنحت، والنقش، والطباعة الحجرية و فن الزرابي،

و) الرسوم، والرسوم التخطيطية، والمخططات والنماذج الهندسية المصغرة للفن و الهندسة المعمارية و المنشآت التقنية،

ز) الرسوم البيانية و الخرائط و الرسوم المتعلقة بالطوبوغرافيا أو الجغرافيا أو العلوم،

ح) المصنفات التصويرية والمصنفات المعبر عنها بأسلوب يماثل التصوير،

ط) مبتكرات الألبسة للأزياء و الوشاح.[1]

المادة 5: تعتبر أيضا مصنفات محمية الأعمال الآتية:

- أعمال الترجمة و الاقتباس، و التوزيعات الموسيقية، و المراجعات التحريرية، و باقي التحويرات الأصلية للمصنفات الأدبية أو الفنية،
- المجموعات و المختارات من المصنفات، مجموعات من مصنفات التراث الثقافي التقليدي وقواعد البيانات سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى، و التي تتأتى أصالتها من انتقاء موادها أو تربيتها.

تكفل الحماية لمؤلف المصنفات المشتقة دون المساس بحقوق مؤلفي المصنفات الأصلية.

المادة 6: يحظى عنوان المصنف، إذا اتسم بالأصلية، بالحماية الممنوحة للمصنف ذاته.

[1] مجلة الموسوعة القضائية الجزائرية، مرجع سبق ذكره، ص.69.

المادة 7: لا تكفل الحماية للأفكار و المفاهيم و المبادئ و المناهج و الأساليب و إجراءات العمل و أنماطه المرتبطة بإبداع المصنفات الفكرية بحد ذاتها، إلا بالكيفية التي تدرج بها، أو تهيكل، أو ترتب في المصنف المحمي، و في التعبير الشكلي المستقل عن وصفتها أو تفسيرها أو توضيحها.

المادة 8: تستفيد مصنفات التراث الثقافي التقليدي و المصنفات الوطنية التي تقع في عداد الملك العام حماية خاصة كما هو منصوص عليها في أحكام هذا الأمر.

تتكون مصنفات التراث الثقافي التقليدي من:[1]

- مصنفات الموسيقى الكلاسيكية التقليدية،
- المصنفات الموسيقية و الأغاني الشعبية:
- الأشكال التعبيرية الشعبية المنتجة و المترعرعة و المرسخة في أوساط المجموعة الوطنية و التي لها ميزات الثقافة التقليدية للوطن،
- النوادر و الأشعار و الرقصات و العروض الشعبية،
- مصنفات الفنون الشعبية مثل: الرسم و الرسم الزيتي و النقش و النحت و الخزف والفسيفساء:
- المصنوعات على مادة معدنية و خشبية و الحلي،والسلالة، وأشغال الإبرة، و منسوج الزرابي والمنسوجات.

تتكون المصنفات الوطنية التي تقع في عداد الملك العام من المصنفات الأدبية أو الفنية التي انقضت مدة حماية حقوقها المادية لفائدة مؤلفها و ذوي الحقوق وفقا لأحكام هذا الأمر.

المادة 9: يمكن أن تستعمل استعمالا حرا مصنفات الدولة، الموضوعة بطريقة شرعية في متناول الجمهور لأغراض لا تدر الربح مع مراعاة سلامة المصنف و بيان مصدره،

[1] مجلة الموسوعة القضائية الجزائرية، مرجع سبق ذكره، ص.69.

يقصد بمصنفات الدولة، في مفهوم هذه المادة، المصنفات التي تنتجها و تنشرها مختلف مؤسسات الدولة و الجماعات المحلية و المؤسسات العمومية ذات الطابع الإداري.

المادة 10: تبقى المصنفات التي آلت إلى الدولة عن طريق التبرع أو بالإرث خاضعة لنظام الحماية القانونية الذي كان مطبقا عليها قبل الأيلولة المذكورة دون المساس بالأحكام المتعلقة بالمواريث و الهبات،

المادة 11: لا تكفل الحماية المقررة لحقوق المؤلف المنصوص عليها في هذا الأمر للقوانين والتنظيمات و القرارات و العقود الإدارية الصادرة عن مؤسسات الدولة،و الجماعات المحلية،و قرارات العدالة،و الترجمة الرسمية لهذه النصوص.[1]

الفصل الثاني

المؤلف و قرينة ملكية الحقوق

المادة 12: يعتبر مؤلف مصنف أدبي أو فني في مفهوم هذا الأمر الشخص الطبيعي الذي أبدعه.

يمكن اعتبار الشخص المعنوي مؤلفا في الحالات المنصوص عليها في هذا الأمر،

المادة 13: يعتبر مالك حقوق المؤلف،ما لم يثبت خلاف ذلك، الشخص الطبيعي أو المعنوي الذي يصرح بالمصنف باسمه أو يضعه بطريقة مشروعة في متناول الجمهور،أو يقدم تصريحا باسمه لدى الديوان الوطني لحقوق المؤلف و الحقوق المجاورة، المنصوص عليه في المادة 131 من هذا الأمر.

إذا نشر المصنف باسم مؤلفه، فإن الشخص الذي يضعه بطريقة مشروعة في متناول الجمهور يعد ممثل لمالك الحقوق، ما لم يثبت خلاف ذلك.

[1] مجلة الموسوعة القضائية الجزائرية، مرجع سبق ذكره، ص.70.

إذا نشر المصنف المجهول الهوية دون الإشارة إلى هوية من يضعه في متناول الجمهور،فإن ممارسة الحقوق يتولاها الديوان الوطني لحقوق المؤلف و الحقوق المجاورة إلى أن يتم التعرف على هوية مالك الحقوق.

المادة 14: المصنف المركب هو المصنف الذي يدمج فيه بالإدراج أو التقريب أو التحوير الفكري مصنف أو عناصر مصنفات أصلية دون مشاركة مؤلف المصنف الأصلي أو عناصر المصنف المدرجة فيه.

يمتلك الحقوق عل "المصنف المركب" الشخص الذي يبدع المصنف مع مراعاة حقوق مؤلف المصنف الأصلي.[1]

المادة15: يكون المصنف "مشتركا" إذا شارك في إبداعه أو إنجازه عدة مؤلفين.

لا يمكن الكشف عن المصنف "المشترك" إلا ضمن الشروط المتفق عليها بين مالكي الحقوق،

تعود حقوق المصنف إلى جميع مؤلفيه و تمارس هذه الحقوق وفق الشروط المتفق عليها فيما بينهم، و إذا لم يتم الاتفاق، تطبق الأحكام المتعلقة بحالة الشيوع.

لا يمكن أي مساهم في المصنف المشترك أن يعارض استغلال المصنف في الشكل المتفق عليه إلا بمبرر.

يسمح لكل مؤلف مصنف مشترك باستغلال الجزء الذي ساهم في المصنف الذي تم الكشف عنه، ما لم يلحق ضررا باستغلال المصنف ككل مع مراعاة وجوب ذكر المصدر و يعد باطلا كل شروط مخالف لذلك.

[1] مجلة الموسوعة القضائية، مرجع سبق ذكره، ص.71.

المادة 16: يعتبر مصنفا سمعيا بصريا المصنف الذي يساهم في إبداعه الفكري بصفة مباشرة كل شخص طبيعي.

يعد على الخصوص مشاركا في المصنف السمعي البصري الأشخاص الآتي ذكرهم:

- مؤلف السيناريو،
- مؤلف الاقتباس،
- مؤلف الحوار أو النص الناطق،
- المخرج،
- مؤلف المصنف الأصلي إذا كان المصنف السمعي البصري مقتبسا من مصنف أصلي،
- مؤلف التلحين الموسيقي مع كلمات أو بدونها تنجز خصيصا للمصنف السمعي البصري،
- الرسام الرئيسي أو الرسامون الرئيسيون إذا تعلق الأمر برسم متحرك،[1]

المادة 17: يعتبر مصنف إذاعيا المصنف الذي يبدعه مؤلف مصنف أدبي أو موسيقي بغرض البث الإذاعي السمعي.

يعتبر مساهما في المصنف الإذاعي كل شخص طبيعي يشارك مباشرة في الإبداع الفكري للمصنف.

المادة 18: يعتبر مصنفا"جماعيا" المصنف الذي يشارك في إبداعه عدة مؤلفين، بمبادرة شخص طبيعي أو معنوي و إشرافه ينشره باسمه

لا تمنح المساهمة في المصنف الجماعي حقا مميزا لكل واحد من المشاركين في مجمل المصنف المنجز.

[1] مجلة الموسوعة القضائية، مرجع سبق ذكره، ص.71.

تعود حقوق مؤلف المصنف الجماعي إلى الشخص الطبيعي أو المعنوي الذي بادر بإنتاج مصنف و إنجازه و نشره باسمه، ما لم يكن ثمة شرط مخالف.

المادة 19: إذا تم إبداع مصنف في إطار عقد أو علاقة عمل، يتولى المستخدم ملكية حقوق المؤلف لاستغلال المصنف في إطار الغرض الذي أنجز من أجله، ما لم يكن ثمة شرط مخالف.

المادة 20: إذا تم إبداع مصنف في إطار عقد مقاولة يتولى الشخص الذي طلب إنجازه ملكية حقوق المؤلف في إطار الغرض الذي أنجز من أجله، ما لم يكن ثمة شرط مخالف.

الباب الثاني

الحقوق المحمية

المادة 21: يتمتع المؤلف بحقوق معنوية و مادية على المصنف الذي أبدعه تكون الحقوق المعنوية غير قابلة للتصرف فيها و لا للتقادم و لا يمكن التخلي عنها.

تمارس الحقوق المادية من قبل المؤلف شخصا أو من يمثله أو أي مالك آخر للحقوق بمفهوم هذا الأمر.[1]

الفصل الأول

الحقوق المعنوية و ممارستها

[1] مجلة الموسوعة القضائية، مرجع سبق ذكره، ص.72.

المادة 22: يتمتع المؤلف بحق الكشف عن المصنف الصادر باسمه الخاص أو تحت اسم مستعار و يمكنه تحويل هذا الحق للغير.

يعود الكشف عن المصنف بعد وفاة مؤلفه إلى ورثته ما لم تكن هناك وصية خاصة.

تفصل الجهة القضائية التي يختارها المبادر بكشف المصنف في حالة وقوع نزاع بين الورثة.

يمكن الوزير المكلف بالثقافة أو من يمثله أو بطلب من الغير إخطار الجهة القضائية للفصل في مسألة الكشف عن المصنف إذا رفض الورثة الكشف عنه و كان هذا المصنف يشكل أهمية بالنسبة للمجموعة الوطنية.

يمكن الوزير المكلف بالثقافة أو من يمثله أن يخطر الجهة القضائية المختصة للحصول على الإذن بالكشف عن المصنف إذا لم يكن للمؤلف ورثة.

المادة 23: يحق لمؤلف المصنف اشترط ذكر اسمه العائلي أو المستعار في شكله المألوف و كذا على دعائم المصنف الملائمة.

كما يمكنه اشتراط ذكر اسمه العائلي أو الإسم المستعار فيما يخص جميع أشكال الإبلاغ العابرة للمصنف إذا كانت الأعراف و أخلاقيات المهنية تسمح بذلك.[1]

المادة 24: يمكن المؤلف الذي يرى أن مصنفه لم يعد مطابقا لقناعته أن يوقف صنع دعامة إبلاغ المصنف إلى الجمهور بممارسة حقه في التوبة أو أن يسحب المصنف الذي سبق نشره من جهة الإبلاغ للجمهور عن طريق ممارسة حقه في السحب.

غير أنه لا يمكن المؤلف ممارسة هذا الحق إلا بعد دفع تعويض عادل عن الأضرار التي يلحقها عمله هذا بمستفيدي الحقوق المتنازل عنها.

[1] مجلة الموسوعة القضائية، مرجع سبق ذكره، ص.73.

المادة 25: يحق للمؤلف اشتراط احترام سلامة مصنفه و الاعتراض على أي تعديل يدخل عليه أو تشويهه أو إفساده إذا كان ذلك من شأنه المساس بسمعته كمؤلف أو بشرفة أو بمصالحه المشروعة.

المادة 26: تمارس الحقوق المنصوص عليها في المادتين 23و25 من هذا الأمر، من قبل ورثة مؤلف المصنف بعد وفاته أو من طرف كل شخص طبيعي أو معنوي أسندت له هذه الحقوق بمقتضى وصية.

إذا وقع نزاع بين ورثة مؤلف المصنف،تفصل الجهة القضائية بإخطار من صاحب المصلحة المبادر في الحقوق المشار إليها في الفقرة السابقة.

يمكن الديوان الوطني لحقوق المؤلف و الحقوق المجاورة أن يمارس الحقوق المنصوص عليها في الفقرة الأولى من هذه المادة بما يضمن الاستعمال الأمثل لحقوق المؤلف إذا لم يكن لهذا الأخير ورثة.[1]

و من استقراء الأمر 10/97 المعدل والمتمم بالأمر 05/03 المتعلق بحق المؤلف والحقوق المجاورة نستخلص ما يلي:[2]

1- أنه وسع قائمة المؤلفات المحمية حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية (م4 الأمر 10/97) والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي والتي تمكن من القيام بنشاط علمي أو أي نشاط من نوع آخر أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بآلة وتترجم باندفاعات الكترونية بالحاسوب، أما قواعد البيانات فهي عبارة عن مجموعة المصنفات والأساليب والقواعد كما يمكن أن تشمل الوثائق المتعلقة بسير ومعالجة المعطيات (م 5 الأمر 10/97).

[1] مجلة الموسوعة القضائية الجزائرية، مرجع سبق ذكره، ص.74.

[2] أ. قارة أمال: الجريمة المعلوماتية، رسالة ماجستير، جامعة الجزائر، كلية الحقوق، بن عكنون، الاختصاص القانون الجنائي والعلوم الجنائية، 2005، ص.139.

2- أن مدة الحماية تحدد من 25 سنة إلى 50 سنة بعد وفاة المبدع تماشيا مع اتفاقية بارن BERNE التي حددت كمدة دنيا للحماية 50 سنة ،وبالتالي هذه المدة تشمل حتى مصنفات الإعلام الآلي[1] (المادة 58 من الأمر 05/03).

3- تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما مؤلفي المصنفات المعلوماتية (المادة 153 من الأمر 05/03 تقابل المادة 151 الأمر 10/97)، إذ في السابق تجريم الاعتداءات على الملكية تناولته المواد 590-394 من قانون العقوبات لكنها أخرجت منه بموجب الأمر 10/97.

تجدر الإشارة إلى أن هذه المستجدات التي اعتمدها المشرع الجزائري من خلال الأمرين 10/97 و05/03 تعود لأسباب أهمها أن من شروط الانضمام إلى المنظمة العالمية للتجارة هو المصادقة على اتفاقية بارن وهو ما فعلته الجزائر بموجب المرسوم الرئاسي 341/97[2] إضافة إلى تبني أحكام اتفاق جوانب الملكية الفكرية المتعلق بالتجارة الواقع بين المنظمة الدولية للملكية الفكرية والمنظمة العالمية للتجارة (أبرم في 1994/04/15 وساري المفعول منذ 1995/01/01).

ولقد نصت المادة 10 منه على أن برامج الإعلام الآلي سواء كانت في صورة برنامج مصدر أو الصورة المنقوشة فهي محمية على أساس أنها مصنفات أدبية (المادة 10 من الاتفاق).[3]

كما أن الاتفاقية حول الإجرام المعلوماتي نصت على تجريم الاعتداءات على حقوق المؤلف والحقوق المجاورة تطبيقا لأحكام اتفاق جوانب الملكية إذا ارتكبت هذه الاعتداءات عن طريق نظام المعلوماتي في نطاق تجاري.

[1] المادة 07 من اتفاقية بارن مدة الحماية التي تمنحها الاتفاقية تشمل مدة حياة المؤلف و 50 سنة بعد الوفاة (في هذا الصدد انظر المادة 12 من اتفاق جوانب الملكية الفكرية المتعلق بالتجارة).

[2] المرسوم الرئاسي رقم 341/97 (97/09/13) المتضمن انضمام الجزائر مع التحفظ إلى اتفاقية برن لحماية المصنفات الأدبية والفنية المؤرخة في 1896/06/09 والمتممة في باريس في 1896/05/04 والمعدلة في 1979/09/28 (ج.ر. مؤرخة في 97/09/14).

[3] المادة 10 من اتفاق جوانب الملكية الفكرية المتعلق بالتجارة.

كما أشارت معاهدة الويبو بشأن حق المؤلف (اتفاقية الانترنت) المؤرخة في 1996/06/20 في مادتيها 4-5 على ما يلي: تتمتع برامج الحاسوب بالحماية باعتبارها مصنفات أدبية بمعنى المادة 2 من اتفاقية برن، وتطبق تلك الحماية على برامج الحاسوب أيا كانت طريقة التعبير عنها أو شكلها. أما المادة 5 منه فلقد نصت على أن" مجموعات البيانات أو المواد الأخرى تتمتع بالحماية بصفتها هذه أيا كان شكلها إذا كانت تعتبر ابتكارات فنية بسبب اختيار محتوياتها أو ترتيبها ولا تشمل هذه الحماية البيانات أو المواد في حد ذاتها".[1]

وتجدر الإشارة إلى أن المادة 5 من الأمر 05/03 قد عدلت تسمية مجموعات المعلومات البسيطة التي كانت واردة في المادة 5 من الأمر 10/97 وعوضت بمصطلح قاعدة البيانات وهذه الأخيرة تعتبر مصنفات أدبية مشتقة.

4 -تسري الحماية على مصنفات الجزائريين سواء نشرت هذه المصنفات في الجزائر أو الخارج أخذا بالمعيار الشخصي؛ أما بالنسبة لمؤلفات الأجانب فنفرق بين المؤلفات التي لم يسبق لها أن نشرت و التي تنشر للمرة الأولى في الجزائر ،و هي تتمتع بنفس الحماية التي تتمتع بها مؤلفات الجزائريين و هذا معيار اقليمي .

أما مؤلفات الأجانب التي نشرت في الخارج من قبل فانها لا تتمتع بالحماية الا على اساس المعاملة بالمثل.

وعليه ضرورة تنسيق الجزائر مع باقي الدول فيما يتعلق بالمصنفات المعلوماتية نظرا لكثرة تداولها ،و اعتمادا على المذكرة الايضاحية للنصوص النموذجية التي وضعتها المنظمة العالمية للملكية الفكرية التي تقتصر الحماية علا واقعة النقل المادي للبرامج بل نصت صراحة على صلاحية النقل

[1] معاهدة الويبو بشأن حق المؤلف (اتفاقية الأنترنت) المؤرخة في 1996/06/20، المادة 4 والمادة 5.

المعنوي لها عن طريق شبكات الحاسب التي ترتبط العديد من الدول و يطلق عليها شبكات الانترنت.

5-عادة ما تكون المصنفات المعلوماتية عبارة عن مصنفات يتعدد مؤلفوها المساهمون في ايداعها و هي عبارة عن مصنفات مشتركة أو جماعية خاصة تلك المبرمجة من قبل مؤسسات ضخمة بمساهمة عدة اختصاصيين محللين و مبرمجين.

وبالنسبة للمشرع الجزائري نص على المصنف المشترك للأشخاص الطبيعية المشاركة في انجازه (المادة 16) .لكن نظرا لكون عملية الاستثمار الاقتصادي الذي يتطلب انجاز المصنفات المعلوماتية مرتفع جدا في بعض الحالات ،أو بالاعتماد على هذه الأسس و لضمان الاستقلال الكافي لهذا المصنف كان من الأجدر أن يأخذ المشرع الجزائري بما سارت عليه الدول الانجلوساكسونية التي تمنح للمنتج صفة المؤلف و لا تمنحها لغيره من المشاركين تجنبا لمشكلة اعتراض المؤلفين لاستغلال المصنف كان من الأجدر في هذا الاطار أن يضع المشرع نصا خاصا بالمصنفات المشتركة في مجال الاعلام الآلي كما هو الحال بالنسبة للمصنفات السمعية البصرية[1].

و عليه و رغم اعتراف المشرع الجزائري لبرامج الاعلام اللآلي و قواعد البيانات بصفة المصنف المحمي الا أنه لا يخفى علينا أن الحماية الجزائية للبرامج من خلال حق المؤلف تنصب بصفة أساسية على شكل البرنامج أو مضمونه الابتكاري فقط دون أن تغطي تلك الحماية كل مضمون البرنامج ،و لهذا السبب كان البحث عن نوع آخر من الحماية ينضم الى الحماية السابقة من الحماية الجزائية لهذه البرامج في مثل هذه الحالات أمرا ضروريا،و لذلك فلا مفر من ضرورة اللجوء الى استحداث نصوص تجريمية خاصة بالمعلوماتية.

[1] د_أحمد السمدان –النظام القانوني لحماية برامج الحاسب الآلي-مجلة الحقوق-الكويت- العدد4 ،سنة 1987،ص51،11

المطلب الثاني: الاعتداء على البيانات الشخصية والخصوصية المعلوماتية بطريق الانترنت

المعاملات التجارية أصبحت تتم عبر الواقع الافتراضي cyberspace، وذلك من خلال التعامل عبر شبكة الأنترنت، كما أن الأخيرة أصبحت تمثل جميع المعاملات بين البشر، ولكن في الواقع الافتراضي أو الخيالي، وأن من شأن ذلك العالم الخيالي جمع المعلومات المتعلقة بالحياة الخاصة للأشخاص، وتحويلها إلى بيان تفصيلي عن مركزه المالي وهواياته واهتماماته وكافة المسائل الأخرى المتعلقة بحياته الشخصية، وباتت الخصوصية في غير مأمن أو معزل عن الآخرين، وقد ظهرت وسائل تقنية لمواجهة خطر انتهاك الخصوصية، وذلك عن طريق استخدام طرق التشفير الآمنة.[1]

ولكن تطور تقنيات المعلومات المتلاحق من ضمن خصائصه تخزين واسترجاع وتحليل كميات هائل من البيانات والمعلومات ذات الخاصة الشخصية عن طريق الحاسبات الآلية في المؤسسات والشركات والوكالات الحكومية، بل ويمكن نقل هذه المعلومات عبر البلاد والدول في كافة أنحاء العالم المادي...

وبالتالي فإن ذلك يكشف بوضوح التهديد الكبير للخصوصية والبيانات الشخصية. واستخدام الحاسب الآلي في جمع ومعالجة البيانات الشخصية المتصلة بالحياة الخاصة للأفراد ساعد على إيجاد بنوك المعلومات Data Bank، التي تمثل تطورا تقنيا هائلا في مجال تحليل واسترجاع المعلومات. وكذلك اتجهت معظم دول العالم بمختلف مؤسساتها وهيئاتها إلى إنشاء قواعد بيانات في كافة المجالات، مما أتاح الفرصة لجمع وتخزين ومعالجة البيانات الشخصية لأغراض متعددة، ونتيجة لظهور شبكة الأنترنت تغيرت البيئة التي تتم عبرها رحلة البيانات المتبادلة، وذلك يرجع إلى أن جمع

[1] رشدي محمد علي محمد عيد علي، مرجع سبق ذكره، ص.173.

البيانات أصبح أكثر سهولة وأكثر ملائمة، بالتفاعل مع تقنيات الحاسب الآلي عن طريق إتاحة وسائل تبادل المعلومات عبر شبكة الأنترنت.[1]

والمتمثلة في برمجيات التصفح ودخول المواقع والبريد الإلكتروني للمشتركين Email، فضلا عن أن بروتوكول شبكة الحاسب الآلي والخدمات الأخرى يعملان من نقطة إلى نقطة أخرى مرتبطة، بالإضافة إلى قيام محتوى البيانات ويسمى "IP"بالتعريف بهوية المرسل والمرسل إليه أو مستلم البيانات المنقولة، كما توجد مجموعات الأخبار، وغرف الدردشة والتي يكون معظمها مفتوحا أمام المستخدمين. فهي تحتوي على بيانات شخصية يمكن تخزينها آليا على العديد من الحاسبات بدون تدخل أو تعديل من المستخدم.

كما أن الموردين يهتمون بمعرفة وتوثيق هوية المستخدمين عن طريق تخزين البيانات الشخصية واستخدامها في أغراض أخرى. وفي بيئة الأنترنت، تستخدم العديد من الوسائل التقنية لتتبع المعلومات الشخصية للمشتركين، ومن أشهرها رسائل كوكيز cookies وهذه الرسائل تنتقل إلى نظام المستخدم بمجرد ولوجه إلى أحد المواقع عبر شبكة الأنترنت، وتتمكن من تسجيل بعض البيانات الشخصية الخاصة به. وعلى الرغم من أن بداية هذه الرسائل كانت مشروعة، وكانت تستخدمها الشركات والمؤسسات التجارية في أنشطتها الخاصة بالدعاية عن طريق إرسال بريد إلكتروني من هذه الشركات في إطار نشاط الدعاية.

فبالرغم من هذه الفائدة، إلا أنها ومع تطورها أصبحت من أخطر الوسائل تهدد الحياة الخاصة للأفراد عبر شبكة الأنترنت، لأنها أصبحت وسيلة لملاحقة واقتفاء أثر المستخدمين وجمع المعلومات عنهم وتحليلها لأهداف الإعلان والدراسات التسويقية على الخط.

وفي دراستنا لهذا الموضوع سوف نتناول نقطتين على التفصيل الآتي:

[1]See the center for democracy and technology's snoop demonstration at: http://snoop.cdt.org/for an example of the information that can be easily captured by sites on the world wide web.

1- حماية الخصوصية المعلوماتية في القانون المقارن

2- حماية الخصوصية المعلوماتية في بعض التشريعات العربية

أولا: حماية الخصوصية المعلوماتية في القانون المقارن:

نظرا لما يمثله كلا من القانونين الفرنسي والأمريكي من انتمائهما لنظامين قانونيين مختلفين سنتناول كلا منهما من خلال كيفية حماية الخصوصية المعلوماتية كلا على حدى.

1- حماية الخصوصية المعلوماتية في القانون الجنائي الفرنسي:[1]

يتطلب القانون الفرنسي المسمى بنظم المعالجة الرقمية والحرية Informatique Et Liberté الصادر في 6 يناير 1978 عند معالجة أية بيانات اسمية شخصية من قبل أشخاص القانون الخاص وجوب إخطار اللجنة القومية للمعلوماتية والحريات، ويتطلب الأمر الحصول على تصريح سابق إذا كان من يقوم بجمع المعلومات من أشخاص القانون العام أو من أشخاص القانون الخاص الذين يعملون لمصلحة الدولة.[2]

وإذا أراد القائمون على موقع من مواقع الأنترنت التعامل مع البيانات الشخصية فيتعين عليهم قبل البدء في هذا الأمر إخطار اللجنة القومية للمعلوماتية والحريات، وذلك لأن نشر مثل هذه المعلومات على مواقع الأنترنت يجعلها عرضة للانتهاك ووقوع الأفعال غير المشروعة عليها مثل الالتقاط غير المسموح به والتزييف والاستيلاء والتلاعب بها. ولذلك تشترط اللجنة إخطار الأشخاص

[1] André Holleaux, « la loi de 6 Janvier 1978 sur l'informatique et liberté » rev, Adm. 1978. N°181, P.31-40 et N°182, P.160-165.

[2] http://internet –juridique.net/chroniques/sitejuridique.html

بمخاطر وضع بياناتهم الشخصية على المواقع وتعطى لهم الحق في الاعتراض على البيانات المنشورة عنهم ولهم حق الإطلاع عليها والتصحيح والاعتراض ومحو البيانات لأسباب مشروعة.

ويرى جانب من الفقه أن القضاء قد أسهم كثيرا في تحديد مفهوم البيانات الاسمية التي يوفر لها هذا القانون الحماية فقد اعتبر أن من البيانات التي يشملها هذا القانون بالحماية رقم التليفون ولكنه لم يعتبر باسم الشخص وعنوانه ضمن البيانات الاسمية، كما قرر أن البيانات التي تتعلق بالمعلومات الخاصة بجنسية سكان عقار وأفكارهم الفلسفية هي من البيانات الاسمية التي يحميها القانون.

ورغبة من اللجنة القومية للمعلوماتية والحريات في تيسير الإجراءات قامت بوضع توجيهات عامة بحيث يكتفي بإخطار مبسط للجنة إذا تعلق الأمر ببيانات لا تتسم بالخطورة، أما إذا تعلق الأمر ببيانات على قدر من الحساسية (كالتي تتعلق بالعرف والآراء السياسية والفلسفية والدينية أو المتعلقة بالانتماءات النقابية أو بأخلاق الشخص). فيتعين الحصول على موافقة صريحة من صاحب الشأن وذلك وفقا لما نصت عليه المادة 31 والتي تم تضمينها بالمادة 226-19 من قانون العقوبات. وقد تم إدانة أحد الأشخاص وفقا لهذا القانون لقيامه بوضع صورة عارية لصديقته على موقع على الأنترنت.

هذا من جهة القواعد الإجرائية العامة لحماية البيانات الإسمية في قانون 1978م. وأما عن الحماية الجنائية لحرمة الحياة الخاصة في ق.ع.ف الحديث: فالمشرع الفرنسي في قانون العقوبات الحديث بشأن حماية الحياة الخاصة كفل الحماية للحياة الخاصة بالمواد 226 فقرة أولى، 226 فقرة ثانية، 226 فقرة ثامنة.

وتتعلق المادة الأولى بتجريم التقاط أو تسجيل أو نقل الكلام الصادر بصورة خاصة أو سرية بدون موافقة المجني عليه، وكذلك تجريمه لالتقاط أو تسجيل أو نقل صورة شخص من مكان خاص

دون رضاء منه، وتتعلق المادة الثانية بجريمة حفظ أو إعلان أو استعمال تسجيل أو مستند تم الحصول عليه بأحد الأفعال المشار إليها بالمادة 226 فقرة أولى.

أما المادة الأخيرة فتتعلق بعمل مونتاج لصوت أو صورة لشخص بدون رضاه والمشرع الفرنسي لم يعدل في صياغة المواد كما كانت واردة في قانون العقوبات القديم والمتعلقة بحماية الحياة سواء فيما يتعلق بالجريمة الأولى وهي جريمة التقاط أو تسجيل أو نقلا لكلام صادر بصورة خاصة وسرية دون موافقة المجني والمنصوص عليها بالمادة 226 فقرة أولى.[1]

وأما عن الحماية الجنائية للبيانات الاسمية في القانون الجنائي الفرنسي فيتعلق الأمر هنا بالجرائم التي نص عليها المشرع بالقانون 1978 وتعديلاته [2] والمتعلق بالمعلوماتية والحريات، والتي أكد عليها القانون الجنائي الفرنسي الحديث بعد أن أجري عليها بغض التعديلات وأزال عنها الغموض المتعلق بها، وقد أراد المشرع الفرنسي أن يؤكد على حماية حقوق وحريات المواطنين في مواجهة مخاطر وتطورات تكنولوجيا المعلومات.

ولم يحاول المشرع الفرنسي عند قيامه بوضع القانون الجنائي الحديث أن يقوم بتغيير روح قانون 1978 أو أن يقوم بتقليص سلطات اللجنة القومية للمعلوماتية والحريات، وقد تضمن التشريع الجنائي الفرنسي الحديث المواد 41-44 من قانون 1978 في الفصل الخاص بحماية الشخصية وتناول الجرائم المتعلقة بالبيانات الاسمية والأحكام الخاصة بالعقاب في المواد 16/226 إلى 24/226 والمادة 31/226 من قانون العقوبات الحديث مع إجرائه لبعض التعديلات في هذه الجرائم، والأفعال التي تناولها ق.ع.ف الحديث والمتعلقة بحماية البيانات الشخصية مثل:

- عدم اتخاذ الإجراءات الأولية لمعالجة البيانات م226-16...إلخ

[1] هذه النصوص موجودة بالموقع التالي:

http://www.legifrance.gouv.fr/waspad/uncode?code=cpenalll.rcv.

[2] قانون المعالجة الآلية للمعطيات – ملفات المعطيات والحريات الفردية رقم 17-78 تاريخ 1978/01/6.

The act on Data processing, Data Files and individual liberties N°17-78 (1978).

2- حماية الخصوصية المعلوماتية في القانون الجنائي الأمريكي:

لقد أقرت الولايات المتحدة الأمريكية ثماني ولايات منها على الأقل ضمانات دستورية صريحة للخصوصية الشخصية، كما تضمن العديد من قوانين الولايات النص على قوانين تحمي الحق في الخصوصية إلا أن هذه الحماية غالبا ما تتسم بالغموض والطموح، بالإضافة إلى أنها عندما تتعارض مع القانون الاتحادي فإن السيادة تكون للقانون الاتحادي، وهو الأمر الذي يحد ومن أثرها في حماية الخصوصية.

وإن سياسة المشرع الولائي الأمريكي تأخذ أبعادا متفاوتة فيما بينها فبينما ينص بعضهم على الحماية الدستورية للخصوصية نجد بعضهم الآخر يضعها في نطاق الحماية القانونية ولهذا فقد تشكل مجموعات أعمل لوضع مفاهيم ومبادئ للخصوصية في القانون الأمريكي كان من أبرزها ما صدر من مبادئ عامة لجميع المشاركين في المجال المعلوماتي، والتي صدرت في يونيو 1995 فمنها ما يتعلق بجميع المشاركين في المجال المعلوماتي، وأخرى لمستخدمي المعلومات الشخصية، وأخرى للأفراد الذين يقدمون المعلومات الشخصية.[1]

بالنسبة للفئة الأولى تتسم بثلاثة مبادئ وهي:[2]

- مبدأ خصوصية المعلومات ويعني الحصول على المعلومات الشخصية، وكشفها واستخدامها بطرق تحترم خصوصية الفرد.
- مبدأ سلامة المعلومات ينبغي عدم تغيير أو إتلاف المعلومات الشخصية بصورة غير ملائمة
- مبدأ جودة المعلومات ينبغي أن تكون المعلومات الشخصية دقيقة، وفي الوقت الملائم، ومناسبة للغرض التي تقدم وتستخدم من أجله

[1] أيمن عبد الله فكري، جرائم نظم، المعلومات، رسالة دكتوراه، جامعة المنصورة كلية الحقوق، 2005-2006، ص.538-539.
[2] أيمن عبد الله فكري، جرائم نظم، المعلومات، رسالة دكتوراه، مرجع سبق ذكره، ص.538 وما يليها.

أما بالنسبة لمبادئ الفئة الثانية وهي الخاصة بمستخدمي المعلومات فقد حددت مجموعة العمل خمسة مبادئ وهي:

- مبادئ الامتلاك فينبغي لمستخدمي المعلومات تقييم التأثير على الخصوصية لتقرير ما إذا كان يتم امتلاك أو كشف أو استخدام المعلومات الشخصية، وكذلك الحصول على أو الاحتفاظ بالمعلومات في صورة معقولة تدعم الأنشطة التجارية أو المستهدفة.
- مبدأ الإخطار والذي يلزم مستخدمي المعلومات الذين يقومون بجمع المعلومات الشخصية بصورة مباشرة عن الفرد تقديم معلومات كافية ومناسبة عن لماذا يقومون بجمع المعلومات وما هو الهدف أو الغرض من جمعها، وما هي الخطوات والإجراءات التي ستتخذ لحماية سريتها وسلامتها ودقتها، ونتائج تقديم و حجب المعلومات.
- مبدأ الحماية فينبغي على مستخدمي المعلومات استخدام ضوابط فنية وإدارية مناسبة لحماية سرية وسلامة المعلومات الشخصية.
- مبدأ العدالة والذي يجب فيه على مستخدمي المعلومات الشخصية عدم استخدام المعلومات الشخصية بطرق لا تتفق مع فهم الفرد للكيفية التي تستخدم بها، ما لم يكن هناك مصلحة عامة اضطرارية لمثل هذا الاستخدام.
- مبدأ التوعية والذي يجب على مستخدمي المعلومات القيام بتوعية العملاء والجمهور بكيفية المحافظة على خصوصية المعلومات.

والمجموعة الأخيرة من المبادئ تتعلق بالأفراد الذين يقدمون المعلومات وتتضمن ثلاثة مبادئ هي:

1. مبدأ الوعي والذي ينبغي فيه على الأفراد أن يحصل على معلومات كافية ومناسبة عن لماذا يتم جمع المعلومات، ما الذي يتوقع أن تستخدم المعلومات من أجله، ما هي الخطوات التي ستتخذ

لحماية المعلومات من حيث السرية والسلامة والنوعية، نتائج تقديم أو حجب المعلومات، وأي حقوق أخرى.

2. مبدأ التمكين فيكون الأفراد من خلال تطبيق هذا المبدأ على علم بكيفية حماية خصوصيتهم بأن تتوافر لديهم وسيلة للحصول على معلوماتهم الشخصية، وسيلة لتصحيح معلوماتهم الشخصية غير الدقيقة أو غير الصحيحة، الفرصة لاستخدام ضوابط فنية مناسبة مثل التشفير لحماية سرية الاتصالات والمعاملات.

3. مبدأ العدالة فيكون لدى الأفراد وسيلة يتم اللجوء إليها لحماية معلوماتهم الشخصية في حالة الاستخدام غير المشروع لها أو الإفشاء غير القانوني.[1]

ثانيا:الحماية الجنائية للخصوصية المعلوماتية في التشريعات العربية:

سوف نتناول في هذه النقطة الحماية الجنائية للخصوصية المعلوماتية في التشريع المصري سواء من حيث ما ورد به من نصوص قانونية في القانون الجنائي التقليدي وكذلك من حيث ما صدر عنه من تشريعات حديثة تتعلق بحماية الخصوصية المعلوماتية من جوانب مختلفة.

الحماية الجنائية للخصوصية المعلوماتية في التشريع المصري:

الحديث عن حماية حرية الحياة الخاصة من التعدي بالوسائل المعلوماتية يقتضي البحث في النصوص التقليدية التي تكفل هذه الحماية في ظل عدم وجود قانون عقابي متكامل لمواجهة جرائم الكومبيوتر والأنترنت، وفيما يتعلق بقانون العقوبات المصري فقد وردت المواد 309 مكرر (أ) و310 في شأن حماي الحياة الخاصة.

[1]http://www.iitf.nist.gov

فالمادتان 309 مكرر و309 مكرر (أ) يتعلقان بحماية حرمة الحياة الخاصة وذلك فيما يتعلق بحظر تسجيل الصوت والصورة بطريق غير مشروع، وفي غير الأحوال المصرح بها قانونا، وتجرم كذلك فعل إفشاء هذه الأسرار وإذاعتها بأي طريقة أو المساعدة في هذه الأفعال أو التهديد بالقيام بها.

حيث جاء نص المادة 309 مكررا من ق.ع.م: "يعاقب بالحبس مدة لا تزيد عن سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونا أو بغير رضاء المجني عليه:[1]

أ- استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون.

ب- التقط أو نقل بجهاز من الأجهزة أيا كان نوعه، صورة شخص في مكان خاص فإذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء اجتماع أو على مسمع أو مرأى من الحاضرين في ذلك الاجتماع، فإن رضاء هؤلاء يكون مفترضا. ويعاقب بالحبس الموظف العام الذي يرتكب أحد الأفعال المبنية بهذه المادة اعتمادا على سلطة وظيفته.

ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عليه، كما يحكم بمحو التسجيلات المتحصلة من الجريمة أو إعدادها".

وجاء في نص المادة 309 مكررا (أ) على أنه: "يعاقب بالحبس كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلا أو مستندا متحصلا عليه بإحدى الطرق المبينة بالمادة السابقة أو كان ذلك بغير رضاء صاحب الشأن.[2]

[1] المادة 309 مكررا، ق.ع.م، من قانون 58 لسنة 1937.

[2] المادة 309 مكررا (أ)، ق.ع.م،من قانون 58 لسنة 1937.

ويعاقب بالسجن مد لا تزيد على خمس سنوات كل من هدد بإفشاء أمر من الأمور التي تم الحصول عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الامتناع عنه، ويعاقب بالسجن الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادا على سلطة وظيفته.

ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عنها، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها".

وأما نص المادة 310 من قانون العقوبات فإنه يجرم إفشاء السر الذي وصل إلى علم أصحاب المهن أو الحرف رغم أنهم مؤتمنون على هذه الأسرار.[1]

وكذلك تضمنت المادتان 21و22 من قانون الصحافة المصري رقم 1996/96 أحكاما مماثلة للمادتين 309 مكرر، 309 مكرر (أ) من قانون العقوبات.

فالمادة 21 من القانون المذكور تنص على أنه: "لا يجوز للصحفي أو غيره أن يتعرض للحياة الخاصة للمواطنين، كما لا يجوز له أن يتناول مسلك المشتغل بالعمل العام أو ذوي الصفة النيابية العامة أو المكلف بخدمة عامة إلا إذا كان التناول وثيق الصلة بأعمالهم ومستهدفا المصلحة العامة".

أما المادة 22 فقد عاقبت من يخالف أحكام المادة 21 بالحبس الذي لا تزيد مدته عن سنة والغرامة التي لا تقل عن خمسة آلاف جنيه ولا تزيد عن عشرة آلاف جنيه أو بواحدة من هاتين العقوبتين".

إذا نرى أن المادتين 309 مكررا، 309 مكرر (أ)، من قانون العقوبات قصد فيهما المشرع المصري حماية حرمة الحياة الخاصة للمواطن.

[1] المستشار الدكتور عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الطبعة الأولى 2006، ص.664-665.

ولم يذكر في الدستور المصري أو في قانون العقوبات أي تعريف للحياة الخاصة. كما لم يرد ذات التعريف في قانون سلطة الصحافة رقم 96 لسنة 1996 رغم أن المشرع استعمل تعبيرات قريبة منها "حرمة الحياة الخاصة" ولم يستخدم تعبير الخصوصية أو حق الخصوصية، وقد كان ذلك هو مسلك المشرع الفرنسي الذي لم يتعرض لتعريف الحياة سواء في قانون الصحافة الصادر في 29 يوليو 1981 وتعديله في 6 مايو 1994، أو في القانون الصادر في 17 يوليو 1970 رغم أن الهدف من صدور القانون الأخير كان هو حماية الحياة الخاصة.

المطلب الثالث: الاعتداء على القيمة الاقتصادية و الامنية للمعلومات بطريق الانترنت

لقد شهد العصر الحالي تغييرا كبيرا في القيم الاقتصادية للأشياء بسبب ثورة المعلوماتية، وانتقلت المعلومات من مجرد أفكار إلى قيمة اقتصادية كبرى، مثل القيم الاقتصادية التي ظهرت في بدايات الثورة الصناعية.

والمعلومة قد تكون سياسية أو أمنية أو علمية أو اقتصادية، فهي لها تصنيفات كثيرة. وفي الواقع أن قيمة المعلومة مرتبطة بها دوما ولكن يلاحظ أن ظهور أهمية هذه القيمة قد ارتبط باتصال المعلومة بشبكات الاتصال ودخولها نظام المعالجة الآلية للبيانات، وهو الأمر الذي جعل دولا كثيرة تهتم برصد أهمية القيم الاقتصادية للمعلومات، وهناك المعلومات السرية أو الوثائق السرية التي تتعلق بالمصلحة العليا للدولة، وكذلك هناك المعلومات التجارية أو الاقتصادية السرية.[1]

وبالنظر إلى أن كل معلومة سرية أصبحت ذات قيمة اقتصادية نظرا لعامل الكتمان فيها، وحصرها في مظهر المنع من التداول، وبالتالي فإن منطق الترويج لها اصبح يعتمد المنطق الاقتصادي في تحديد سعرها. دون النظر إلى طبيعة المعلومة وفيما إذا كانت تجارية أو اقتصادية أو سياسية أو

[1] رشدي محمد علي محمد عيد علي، مرجع سبق ذكره، ص.284.

أمنية...، فكل معلومة لها طابع السرية ويحظر القانون تداولها، ويكون لها في سوق المعلومات قيمة اقتصادية فهي تعد ذات قيمة اقتصادية.

وفي الواقع، لا يوجد نظام قانوني واحد لحماية المعلومات السرية في القوانين المقارنة، واختلفت النظم القانونية فيما بينها بشأن كيفية حماية المعلومات السرية، حيث نجد أن المشرع الأمريكي قد أصدر قانون التجسس الاقتصادي عام 1996، وتضمن هذا القانون حماية الأسرار التجارية وأفرد نصوصا لبيان أشكال الاعتداء على الأسرار التجارية، كما وضعت اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية وهي "اتفاقية تريبس" نظاما لحماية المعلومات السرية أطلقت عليه "المعلومات غير المفصح عنها undisclosed information" وأدخلته في عداد الملكية الفكرية، وتحظر التشريعات المقارنة على الغير الحصول على الأسرار التجارية باستخدام أساليب وممارسات غير مشروعة.[1]

وحماية الأسرار التجارية تختلف عن حماية نظام براءة الاختراع، لأن حماية الأسرار التجارية تخضع لشروط معينة تختلف عن شروط حماية براءة الاختراع.

والتجسس المعلوماتي من المجالات الخصبة للجريمة المعلوماتية، ويعد واحدا من الجرائم التي تساعد على ارتكابها الحاسبات الآلية، ويشمل التجسس المعلوماتي أنماطا متعددة من الجرائم قد تتعلق بأسرار الدولة في العديد من المجالات أو المعلومات التجارية والصناعية.

ويلاحظ أن التصنيف السياسي للمعلومات من الناحية الأمنية يطلق عليها الوثائق الرسمية للدولة. كما أن المعلومات السرية الاقتصادية والتجارية لها مفاهيم تتعلق بالمعلومات التي ترتبط بالاقتصاد القومي من حقائق وبيانات فضلا عن أنه هناك شروط يجب أن تتوافر في المعلومات حتى

[1] رشدي محمد علي محمد عيد علي، مرجع سبق ذكره، ص.285.

يمكن حمايتها جنائيا. بالإضافة إلى أن الحماية الجنائية للأسرار التجارية لم تتفق التشريعات على نظام قانوني معين لحمايتها.

وعن مفهوم المعلومات محل الحماية، يجب التطرق إلى مفهوم نقطتين:

أولا:مفهوم الوثائق السرية:

كما سلف الذكر أن هذه الوثائق تتعلق بالأمن القومي والسياسة العليا للدولة. ففي مصر صدر قرار رئيس الجمهورية رقم 472 لسنة 1979 المتعلق بكيفية المحافظة على الوثائق الرسمية للدولة وطريقة نشر هذه الوثائق واستخدامها.[1]

فلقد أحاط المشرع المصري الوثائق والمستندات والمكاتبات التي تتعلق بالسياسة العليا للدولة والأمن القومي بالسرية، على أن تستمر مدة الخطر 50 عاما كحد أقصى تبدأ من تاريخ صدور الوثيقة وبمجرد إقرار سريتها، وتكون عملية إقرار سرية هذه الوثائق والمستندات بتدوين عبارات السرية وحظر الإطلاع عليها من غير ذوي الاختصاص والتداول.

وبالتالي، فإن انتهاك هذا الحظر عن طريق الإطلاع على هذه الوثائق ونشرها على شبكة الأنترنت يكون من شأنه تعريض السياسة العليا للدولة والأمن القومي للخطر.

وجاء في نص المادة 1030 (أ) (3) من القانون الفدرالي لجرائم الحاسب الآلي لعام 1984 في الولايات المتحدة الأمريكية، حيث تعاقب هذه المادة كل من يقوم بالدخول غير المصرح به إلى نظام الحساب الآلي، ويقوم بإنشاء معلومات توجد داخل هذا الحاسب، متى كان يستعمل بواسطة

[1] الجريدة الرسمية العدد 48 في 1979/11/29، موسوعة التشريعات العربية، الجزء 46 مكرر، مصر، ثقافة وقانون.

حكومة الولايات المتحدة الأمريكية أو لمصلحتها، وترتب على هذا السلوك الإصرار بهذا الاستعما: إلا أن هذا النص لم يؤخذ به عند التعديلات المتلاحقة التي طرأت على هذا القانون.[1]

ثانيا:مفهوم المعلومات الاقتصادية والتجارية محل الحماية:

ويقصد بالمعلومات الاقتصادية محل الحماية هي تلك المعلومات التي تتعلق بالاقتصاد القومي من حقائق وبيانات وأخبار تتعلق بالأمن الاقتصادي في الدولة، ويدخل في ذلك التدابير السرية التي تتخذها الدولة للإفلات سرا من حصار اقتصادي مفروض عليها.

وقد عرف السر التجاري أو الاقتصادي في مدونة المسؤولية عن الفعل الضار في الولايات المتحدة الأمريكية عام 1939 بأنه "أي وصف أو تصميم أو أسلوب أو مجموعة من المعلومات... مما يتم استخدامه في الحركة الاقتصادية، فتعطي لصاحبها فرصة الحصول على ميزة نسبية في مواجهة منافسيه الذين لم يسبق لهم استعمالها.[2]

ثالثا:الشروط الواجب توافرها في المعلومات محل الحماية:

نصت المادة 39 فقرة 3 من اتفاقية التريبس على الشروط العامة لحماية المعلومات غير المفصح عنها، وهي شروط تتفق بوجه عام مع شروط حماية الأسرار التجارية في القانون الأمريكي،

[1] د. نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، مرجع سبق ذكره، ص.276.

[2] د. حسام الدين عبد الغني الصغير، حماية المعلومات غير المكشوف عنها بناءا على اتفاق تريبس، ورقة عمل مقدمة إلى الندوة الوطنية المشتركة بين الويبو واتحاد المحامين العرب عن الملكية الفكرية للمحامين، تنظمها المنظمة العالمية للملكية الفكرية (الويبو)، اتحاد المحامين العرب بالتعاون مع حكومة مملكة البحرين ونقابة محامي البحرين، المنامة، من 23 إلى 25 يناير 2003 -wipo-alm/bah/03doc7

وهذه الشروط هي أن تكون هذه المعلومات سرية كما سلف الذكر، وأن يكون لها قيمة تجارية أي أن تكون المعلومة نافعة ومفيدة في مجال نشاط المشروع، لأن هذه الفائدة هي التي تعطيها قيمة اقتصادية في مجال النشاط، وهذه القيمة تتضح أيضا إذا كانت المعلومات السرية تعطي لصاحبها ميزة نسبية في مجال نشاطه في مواجهة منافسيه.واما ثالث شرط وهو الاخير,هو ان يتخذ حائز المعلومات التدابير الجدية للمحافظة على سريتها.اي لكي يمكن حماية المعلومات السرية التجارية جنائيا,يجب ان يكون صاحب هذه المعلومات قد اتخذ من الاجراءات و التدابير الكافية للمحافظة على سرية هذه المعلومات.وهذه الاجراءات تختلف من مؤسسة الى اخرى بحسب حجم هذه المنشاة,فكلما كان حجم الشركة او المنشاة كبيرا كلما كانت اجراءات الامن و الاحتياطات المتخذة من جانبها معقدة.

ومن امثلة هذه الاجراءات اللتي يمكن اتخاذها للمحافظة على سرية المعلومات استخذام كلمات او رموز سرية لفتح الابواب المغلقة الخاصة باماكن تخزين المعلومات.وفي نطاق الدراسة القيام باجراء عملية تشفير لمفاتيح بنوك المعلومات والاحتفاظ بالمعلومات بعد تشفيرها باستخذام شفرات معقدة.

رابعا:النظام القانوني لحماية الاسرار التجارية في التشريعات المقارنة:

في الواقع لايوجد نظام قانوني موحد في التشريعات المقارنة لحماية المعلومات السرية وقد جاءت هذه التشريعات المقارنة بنظم حماية متباينة للمعلومات السرية واختلفت في كيفية الحماية ومستواها.

وقد وضعت اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (اتفاقية التربس) نظاماً لحماية المعلومات السرية.

وهذا النظام يتفق في كثير من الوجوه مع "نظام حماية أسرار التجارة" trade secrets في القانون الأمريكي، رغم اختلاف المسميات ووفقا للمادة الأولى فقرة (2) من اتفاقية التربس فإن

اصطلاح الملكية الفكرية يشمل جميع فئاتها المنصوص عليها في الأقسام من 1 - 7 من الجزء الثاني من الاتفاقية وهي: حقوق المؤلف والعلامات التجارية والمؤشرات الجغرافية والتصميمات الصناعية وبراءات الاختراع والتصميمات التخطيطية للدوائر المتكاملة وحماية المعلومات السرية. ومن ثم فقد اعتبرت اتفاقية التربس المعلومات السرية شكلا من أشكال الملكية الفكرية.[1]

ووضعت الاتفاقية في القسم 7 من الجزء الثاني منها نظاما لحماية الأسرار التجارية أطلقت عليه "حماية المعلوماتغيرالمفصحعنها" Protection of Undisclosed Information وتناولت أحكامه في مادة وحيدة هي المادة 39. وكانت الولايات المتحدة الأمريكية قد اقترحت في الجولة الثامنة لمفاوضات الجات التوسع في المفاوضات الخاصة بالملكية الفكرية لتشمل حماية أسرار التجارة، وتضمَّن الاقتراح الذي قدمته سنة 1987 تعريف أسرار التجارة وحمايتها وفقا للمعايير السائدة في القانون الأمريكي. غير أن الدول النامية اعترضت على ذلك وطالبت باستبعاد حماية أسرار التجارة من نطاق المفاوضات لأنها لا تدخل في عداد أشكال الملكية الفكرية. ورغم عدم الاستجابة لمطالب الدول النامية إلا أن الاتفاقية لم تعترف بحق صاحب المعلومات غير المفصح عنها في ملكيتها، فلم تقم المسئولية عن الاعتداء على المعلومات السرية على فكرة الملكية، على خلاف الوضع السائد في القانون الأمريكي الذي يعتبر أسرار التجارة محلا لحق الملكية، بل جعلت أساس المسئولية ارتكاب أعمال تتناقض مع المنافسة المشروعة وفقا لقواعد قمع المنافسة غير المشروعة. وتنصب الحماية المقررة للمعلومات غير المفصح عنها على نوعين من المعلومات: المعلومات السرية التي تخص الأشخاص الطبيعيين والاعتباريين وتقع تحت سيطرتهم بصورة قانونية، والبيانات والمعلومات الأخرى التي تقدم إلى الجهات الحكومية المختصة من أجل الحصول على ترخيص بتسويق منتج[2].

[1] د. حسام الدين عبد الغني الصغير، حماية المعلومات غير المكشوف عنها بناءا على اتفاق تريبس، ورقة عمل مقدمة إلى الندوة الوطنية المشتركة بين الويبو واتحاد المحامين العرب عن الملكية الفكرية للمحامين، تنظمها المنظمة العالمية للملكية الفكرية (الويبو)، اتحاد المحامين العرب بالتعاون مع حكومة مملكة البحرين ونقابة محامي البحرين، المنامة، من 23 إلى 25 يناير 2003 wipo-alm/bah/03doc7-

[2] د. حسام الدين عبد الغني الصغير، حماية المعلومات غير المكشوف عنها بناءا على اتفاق تريبس، المرجع السابق الذكر.

ففي الولايات المتحدة الأمريكية تنصب الحماية المقررة لأسرار التجارة على أي معلومات سرية يكون لها قيمة اقتصادية، وتبذل جهود معقولة من قبل صاحبها للمحافظة على سريتها. ولا تقتصر الحماية المقررة للأسرار التجارية على المعارف الفنية، بل تشمل كافة المعلومات التجارية مثل قوائم العملاء، والخطط التسويقية، والمعلومات الإدارية والمالية مثل النماذج والاحصائيات والدراسات المالية والاقتصادية.[1]

وهذا المفهوم السائد في الولايات المتحدة الأمريكية لأسرار التجارة أوسع في نطاقه من نظم الحماية المقررة في معظم البلدان الأوربية وغيرها من الدول الأخرى للمعرفة الفنية know-how، إذ يقتصر مدلول المعرفة الفنية – في الغالب – على المعلومات والخبرات والمهارات المتعلقة بطرق وأساليب التصنيع ، ولا يمتد إلى المعارف الإدارية والتنظيمية والتجارية.

أما في انجلترا فتحمى الأسرار بوجه عام عن طريق نظام المعلومات السرية Confidential Information. ولا تقتصر الحماية التي يقررها القانون الإنجليزي بموجب هذا النظام على الأسرار التجارية والصناعية بل تشمل كافة الأسرار السياسية والأسرار العائلية أو الشخصية وغيرها من الأسرار على اختلاف أنواعها، إذ لا يوجد تفرقة في القانون الإنجليزي بين أنواع المعلومات السرية المختلفة فيما يتعلق بتمتعها بالحماية. وفى عديد من الدول الأخرى تحمى الأسرار التجارية والصناعية عن طريق تطبيق القواعد العامة في ق.م[2].

ففي مصر يعتبر الاعتداء على الأسرار التجارية والصناعية عملا غير مشروع يمكن مواجهته عن طريق إقامة دعوى المنافسة غير المشروعة تأسيسا على قواعد المسئولية التقصيرية التي تقضي بأن كل خطأ سبب ضررا للغير يلزم من ارتكبه بالتعويض وفقا للمادة 163 من ق.م.

[1] دكتور حسام الدين عبد الغني الصغير ، المرجع السابق الذكر.
[2] المرجع نفسه.

وفي حالة الأردن, نجد المادة السابعة من قانون المنافسة غير المشروعة والأسرار التجارية رقم 15 لسنة 2000 تتحدث فقط عن إقامة الدعوى المدنية للمطالبة بالتعويض عن الضرر الذي لحق بصاحب الحق في السر التجاري نتيجة إساءة استعمال الغير لهذا السر, دون وجود أية نصوص تتحدث عن إقامة دعوى جزائية في حالة سرقة السر التجاري مثلاً. لذا نستطيع القول إنه إذا توافرت أركان جريمة السرقة, فيما يتعلق بالسر التجاري، فإنه يمكن تطبيق قانون العقوبات المتعلق بذلك. لكننا نرى أن بعض القوانين الأجنبية قد أفردت قوانين خاصة مستقلة بسرقة السر التجاري, مثل قانون التجسس الاقتصادي الأمريكي لسنة 1996 الذي لا يتعلق فقط بالسرقة المقصودة للسر التجاري وإنما أيضا بنسخه أو كشفه. هذا القانون يدمج بين كل من المطالبة المدنية (التعويض المادي) الذي قد يصل كحد أعلى إلى نصف مليون دولار أمريكي للأشخاص الطبيعيين وخمسة ملايين دولار أمريكي للأشخاص المعنويين، والمطالبة الجزائية بحيث قد يسجن الشخص لعشر سنوات كحد أقصي.

ورغم تباين النظم القانونية في حمايتها للأسرار التجارية وتنوعها، فضلا عن اختلاف مسمياتها، إلا أن هناك مجموعة من المبادئ المشتركة تقوم عليها حماية الأسرار التجارية في معظم الدول، وتميزها عن نظام براءات الاختراع، وهي تتلخص في الآتي:

(1) لا تتوقف الحماية التي يضفيها القانون على الأسرار التجارية على تقديم طلب من حائزها لأي جهة إدارية لكي تفحص مدى توافر شروط الحماية، بل يتمتع حائز المعلومات السرية بالحماية تلقائيا طالما توافرت الشروط التي ينص عليها القانون. وينبني على ذلك عدم وجود نظام لتسجيل الأسرار التجارية أو النشر عنها، فضلا عن عدم إصدار الجهة الإدارية لأي صك أو وثيقة تتضمن الاعتراف بحق حائز المعلومات، وذلك لأنها لا تفحص الأسرار التجارية لتتأكد من توافر شروط الحماية التي ينص عليها القانون، على خلاف نظام براءات الاختراع.

(2) لا تعطي الحماية التي يقررها القانون لحائز الأسرار التجارية حقا استئثاريا Exclusive right في منع الغير من استغلال تلك الأسرار، إذ يجوز للغير استغلال المعلومات السرية المشمولة بالحماية بكافة الطرق طالما أنه توصل إليها أو كشف سريتها بطرق وأساليب مشروعة، على النقيض من نظام براءة الاختراع، إذ تخول البراءة لصاحبها حقا استئثاريا Exclusive Right يمنع بموجبه الغير من استغلال الاختراع بأي طريق من الطرق، ولو توصل الغير إلى ذات الاختراع عن طريق الأبحاث والتجارب المستقلة التي أجراها دون الاستعانة بالاختراع المحمي عن طريق البراءة. ومن ثم فإن الحماية المقررة للأسرار التجارية معناها أن القانون يكفل لحائز الأسرار التجارية الحق في حمايتها والدفاع عن مصلحته في استغلالها والحفاظ على سريتها عن طريق القواعد والإجراءات التي يحددها القانون، إذا ما تعرضت تلك الأسرار للاعتداء عليها من الغير بوسائل وأساليب غير مشروعة. ولا تقتصر الحماية المقررة للأسرار التجارية على مدة محددة كقاعدة عامة، بل تستمر الحماية قائمة مهما طالت مدتها طالما بقيت المعلومات سرية، فلم يتم الافشاء عنها أو التوصل إليها بمعرفة الغير. والأمثلة على الأسرار التجارية والصناعية التي تحتكرها الشركات الكبرى لمدة طويلة متعددة، من بينها سر الوصفة Secret Formula الخاصة بتركيبة المادة الرئيسة التي تدخل في صناعة مشروب الكوكاكولا التي تحتفظ الشركة بسريتها منذ مدة تزيد على قرن من الزمان. أما الحماية التي يقررها القانون للاختراع المحمى عن طريق البراءة فهي حماية مؤقتة بالمدة التي يحددها القانون، وهي عشرون عاما في أكثر التشريعات المقارنة حاليا، يبدأ حسابها اعتبارا من تاريخ إيداع طلب الحصول على البراءة. وبانتهاء مدة الحماية تنقضي ملكية البراءة، ويجوز لمن يشاء استغلال الاختراع بأي طريق من الطرق دون أن يدفع للمخترع أي مقابل مالي. ومن أجل ذلك فإن المشروعات لا تلجأ إلى حماية اختراعاتها عن طريق الحصول على براءات اختراع إلا بالنسبة للاختراعات التي تخشى أن يتوصل منافسوها إلى كشف سريتها في زمن قصير نسبيا[1].

[1] الأسرار التجارية في مجال الملكية الفكرية – دكتور قيس محافظة – أستاذ القانون بكلية الحقوق بالجامعة الأردنية – ورقة مقدمة إلى: ندوة الويبو الوطنية

اذا فالحماية للاسرار التجاريا اوسع نطاقا من حيث محلها من براءة الاختراع

إذ لا يشترط في المعلومات التي تعد أسرارا تجارية توافر الشروط اللازمة لمنح البراءة، وهي: الجدة، والخطوة الإبداعية، والقابلية للتطبيق الصناعي. بل يكفى لحماية الأسرار التجارية أن تكون المعلومات محل الحماية لها قيمة اقتصادية نظرا لسريتها شريطة إخضاعها لإجراءات معقولة من قبل صاحبها للحفاظ على سريتها كما سلف الذكر.

عن الملكية الفكرية لأعضاء هيئة التدريس وطلاب الحقوق في الجامعة الأردنية تنظمها المنظمة العالمية للملكية الفكرية (الويبو) بالتعاون مع الجامعة الأردنية – عمّان، من 6 إلى 8 أبريل 2004. و حماية المعلومات غير المكشوف عنها بناء على اتفاق تريبس- دكتور حسام الدين عبد الغني الصغير أستاذ ورئيس قسم القانون التجاري والبحري، كلية الحقوق جامعة المنوفية – وعضو لجنة إعداد مشروع قانون حماية حقوق الملكية الفكرية – ورقة مقدمة إلى: الندوة الوطنية المشتركة بين الويبو واتحاد المحامين العرب، عن الملكية الفكرية للمحامين، تنظمها: المنظمة العالمية للملكية الفكرية (الويبو)، اتحاد المحامين العرب، بالتعاون مع حكومة مملكة البحرين، ونقابة محامي البحرين المنامة، من 23 إلى 25 يناير 2003.

المبحث الثالث: الاتجاهات التشريعية المختلفة في مواجهة الجرائم المعلوماتية

لقد تباينت اتجاهات الدول المختلفة في التعامل مع ظاهرة ج.م، فبينما توجد في بعض الدول نصوص قابلة للتطبيق على الجرائم التي ترتبط بالحاسبات الآلية، توجد دولا أخرى عجزا تشريعيا في التعامل مع هذه الحالات. ويرجع ذلك بصفة أساسية إلى اختلاف الأنظمة القانونية لهذه الدول من ناحية، ومن ناحية أخرى إلى اختلاف تجربة كل منها مع ج.م.

ومن ناحية ثالثة فإن النتائج الاقتصادية التي تترتب على جرائم الحاسب الآلي تختلف من دولة لأخرى، وهو ما ينعكس بدوره على أشكال السلوك التي تلقى اهتماما منها، فبينما تهتم بعض الدول بقرصنة برامج الحاسب الآلي أكثر من مجرد الدخول إلى نظام الحاسب الآلي والتعرف على محتوياته، نجد منها من يولي هذا الدخول اهتماما كبيرا. ومن ناحية أخرى، فإن بعض الدول ترى أن الخسائر الناجمة عن هذه الأفعال لا تتعدى أصحابها ولا تؤثر على المجتمع بصفة عامة. وهو ما يشكك في الحاجة إلى النصوص الجنائية للتعامل مع هذه الأنماط من السلوك، أو على الأقل يثير التساؤل حول مدى جسامة العقوبات التي يجب أن تتضمنها هذه النصوص.[1]

وهكذا تفسر العوامل السابقة الاختلاف في الاتجاهات التشريعية للدول في مواجهة الجرائم المعلوماتية. ونضيف كذلك عدم ظهور هذه الجرائم في الإحصائيات بما يتناسب مع حجمها الحقيقي للأسباب التي تناولناها فيما سبق. واختلاف ذلك من دولة إلى أخرى يؤثر بشكل كبير على مواقف هذه الدول ويمكن بصفة عامة التمييز بين اتجاهين رئيسيين في هذا الخصوص:

الاتجاه الأول: هذا الاتجاه يعتبر الجرائم المرتبطة بالحاسبات الآلية جرائم عادية، لا تتصف بخصائص تميزها عن غيرها من الجرائم. فأنصار هذا الاتجاه لا يرون ضرورة للتفرقة بين الجرائم التي ترتبط بالحاسب الآلي وتلك الجرائم التي لا ترتبط بالحاسب الآلي. فهذا الأخير ما هو إلا وسيلة

[1] OECD Compter Related Crime : Analysis of legal policy, op.cit, P.12.

لارتكاب جريمة معاقب عليها بالفعل بواسطة النصوص القائمة وما يجب الاهتمام به هو تطوير الإجراءات الأمنية الخاصة بأنظمة الحاسبات والتعويض عن الأضرار التي تترتب على هذه الأفعال دون البحث عن نصوص جنائية جديدة.

وتبنى هذا الاتجاه كل من بلجيكا وإيسلندا واليابان من خلال التقرير الصادر عن منظمة التعاون الاقتصادي والتنمية في باريس سنة 1986 في خصوص جرائم الحاسبات الآلية، وبعدها عدلت كل من بلجيكا واليابان عن هذا الاتجاه، بحيث أفردت كل منهما نصوصا خاصة بج.م.

الاتجاه الثاني: أما الاتجاه الثاني فقد ذهب عكس الاتجاه الأول، حث على ضرورة التدخل التشريعي لمواجهة ج.م لما تتميز به من سمات تميزها عن غيرها من الجرائم، ويختلف الأساس الذي يرتكز عليه هذا التدخل التشريعي من دولة إلى أخرى، أو من تشريع إلى آخر باختلاف الاتجاهات السائد، والمفاهيم القانونية التي تؤثر في النظام القانوني بشكل عام.

ومن ناحية أخرى فإن الاختلاف بين التشريعات المختلفة فيما يتعلق بالتعامل مع ج.م لا يقف عند هذا الحد، بل يظهر أيضا بوضوح في شكل هذا التدخل التشريعي، الذي يتفرع إلى عدة وسائل، قد تتمثل في خلق نصوص جديدة يضاف إليها البعد الخاص بالحاسب الآلي، أو تعديل بعض النصوص القائمة بحيث تتوائم مع هذا الشكل الجديد من الجرائم، كما أنه يمكن من ناحية أخرى أن تستخدم الوسيلتين معا.[1]

وسوف نتناول هذا في مطلبين:

أما المطلب الأول: سنتناول المواقف التشريعية المختلفة في تحديد المصلحة الجديرة بالحماية في جرائم المعلوماتية التي تؤثر بلا شك في تحديد مضمون هذه الحماية ونطاقها.

[1] الدكتورة نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، رسالة دكتوراه، جامعة القاهرة، كلية الحقوق، طبعة 2003، ص.314-315.

أما المطلب الثاني: نتعرف على الأساليب والأشكال المختلفة التي يلجأ إليها المشرع لوضع نصوص الحماية الجنائية للمعلوماتية في الدول المختلفة.

المطلب الأول: المواقف التشريعية بالنسبة للمصالح المحمية بالجريمة المعلوماتية

هناك ثلاثة مواقف تشريعية بالنسبة لتحديد المصلحة المحمية التي تؤثر في مضمون الحماية الجنائية لنظم المعلومات، وهذه المواقف تختلف من تشريع لآخر، ويمكن إيجاز هذه المواقف فيما يلي:

أولا: اتجاه يهتم بفكرة الملكية Property Approach

الهدف من ج.م هو حماية الملكية الخاصة من الاعتداء عليها، وذلك من جراء حصول الفاعل على ربح مادي يتحصل عليه عن طريق النشاط الإجرامي. وشأن ج.م في ذلك شأن غيرها من الجرائم التقليدية، ويترتب على هذا الاتجاه اعتبار المعلومات التي يختزنها الحاسب الآلي، والبرامج الخاصة به منن الأشياء التي يمكن أن يتعلق بها حق الملكية، وتعد بعض تشريعات الولايات في الولايات المتحدة الأمريكية نموذجا لهذا الاتجاه.

ولا يلاقي هذا الاتجاه تأييدا نظرا للانتقادات التي توجه إلى اعتبار المعلومات من الأشياء التي يمكن أن يرد عليها حق الملكية.

ثانيا: اتجاه يركز على حماية سلامة المعلومات والبيانات التي يحتوي عليها نظام الحاسب الآليForgery Approach

يركز هذا الاتجاه على حماية سلامة المعلومات والبيانات التي يحتوي عليها نظام الحاسب الآلي، وذلك بصرف النظر عن طبيعة النشاط الإجرامي الذي تتعرض له هذه المعلومات.

ويعتبر هذا الاتجاه التلاعب بهذه المعلومات، شكلا من أشكال التزوير، وتبنت هذه الفكرة المملكة المتحدة في التشريع الخاص بجرائم التزوير والتزييف الصادر عام 1981، إلا أن العمل قد أسفر عن حالات محدودة أمكن تطبيق النص من خلالها.

ثالثا:اتجاه يهتم بالمعلومات في ذاتها وخاصة تلك التي تتصل بالأشخاص

Information Approach

الهدف من هذه الحالة هو حماية المعلومات من الإطلاع على سريتها سواء تعلقت هذه المعلومات بالحياة الخاصة أو كانت لها قيمة اقتصادية أو تعلقت بالدولة ومصالحها أو غير ذلك من المعلومات التي يخشى من الإطلاع عليها. وتتجه التشريعات التي تتأثر بهذا الاتجاه إلى تجريم الدخول غير المصرح به إلى نظام الحاسب الآلي بصفة عامة، ومن الدول التي تأثرت تشريعاتها بهذا الاتجاه الولايات المتحدة الأمريكية (المستوى الفيدرالي) والدول الإسكندنافية وخاصة النرويج وفنلندا.

رابعا:الموقف التشريعي الذي يجمع بين أكثر من اتجاه من الاتجاهات السابقة

Mixed Approach

هذا الاتجاه بطبيعة الحال يتوقف على شكل السلوك الذي يرى المشرع أنه يهدد المصالح في المجتمع. فعلى سبيل المثال يمكن أن تقوم بعض النصوص بحماية الملكية من الاعتداء عليها (وهذا حسب الاتجاه الأول)، بينما تحمي نصوص أخرى المعلومات في ذاتها من الإطلاع عليها (وهذا حسب الاتجاه الثالث).

فإذا كانت الجريمة المعلوماتية كما يصفها البعض بوحش متعدد الوجوه، فهي إذا بحاجة إلى مثل هذا الاتجاه المختلط لمواجهتها.

المطلب الثاني: الأساليب والأنماط المختلفة للصياغات التشريعية الخاصة

تتباين الأساليب التي تلجأ إليها التشريعات في الدول المختلفة في صياغة نصوص الحماية الجنائية لنظم المعلومات. ويمكن القول أن هناك عدة أنماط تشريعية قد يلجأ إليها المشرع في هذا الصدد مع إمكانية الجمع بينها.

ويمكن إيجاز هذه الأنماط أو الأساليب التشريعية فيما يأتي:

أولا:وضع نصوص جديدة قياسا على نصوص تقليدية قائمة بالفعل Extention

تتجه بعض الدول إلى وضع نصوص جديدة قياسا على نصوص تقليدية قائمة بالفعل، حيث يصاغ نص جديد يتفق مع أحد الأشكال التقليدية للسلوك الإجرامي حيث يتمن تحويل السلوك في صورته التقليدية إلى صور أخرى ترتبط بالحاسب الآلي ونظامه باعتبارهما المحل الجديد للسلوك الإجرامي، وعادة ما تتبع أغلب الدول هذه الطريقة.

ثانيا: الإضافة Supplementation

تتجه بعض الدول إلى أن تضيف إلى النصوص القائمة بالفعل تلك الحالات التي يرتكب فيها الجاني النشاط الإجرامي، الوارد بها، بواسطة الحاسب الآلي ومن هذا القبيل ما نصت عليه المادة الثامنة من القانون الخاص بجرائم التزوير والتزييف لعام 1981 في المملكة المتحدة. أو أن تضيف إلى محل السلوك الإجرامي الوارد بالنصوص القائمة المعلومات التي يحويها نظام الحاسب الآلي، مثل اعتبارها محلا للاستيلاء عليها في نصوص جريمة السرقة. ومن بين الدول التي تبنت هذا الاتجاه الولايات المتحدة الأمريكية.[1]

[1]SIEBER (ulrich), op. cit, P.51.

ثالثا: وضع نص رئيسي واحد يستطيع التعامل مع الأوجه المختلفة للجريمة المعلوماتية One-for-all

تتجه بعض الدول إلى وضع نص رئيسي واحد يستطيع التعامل مع الأوجه المختلفة للجريمة المعلوماتية one for all (الولايات المتحدة الأمريكية)، أو تجميع كل ما يتعلق بج.م في قسم مستقل ملحق بالتشريع الجنائي أو في تشريع مستقل. وتوضح كل من هاتين الطريقتين الطبيعة الخاصة للجريمة المعلوماتية، كما تسمح بوضع عقوبات خاصة لهذه الجريمة بحيث تتلاءم معها.

وأخيرا فإن الجمع بين أكثر من نمط من هذه الأنماط أمر وارد.

والحقيقة أن اختيار أي من هذه الطرق يتأثر بشكل كبير بالوقت الذي تدخل فيه المشرع لمواجهة ج.م، وكذلك على طبيعة النظام القانوني في كل دولة.[1]

ومثال ذلك تعد السويد واحدة من أولى الدول التي واجهت ج.م تشريعيا، فقد قامت بوضع نص عام يتعلق بج.م في تشريع خاص. وبعد عدة أعوام أثناء تعديل قانون العقوبات قام المشرع بإضافة عدة نصوص تتعلق بج.م قياسا على نصوص قائمة بالفعل في القانون، مع الاحتفاظ بالنص الأول المتعلق بج.م.

ويرى البعض أن التعامل مع ج.م عن طريق اختيار نمط تشريعي واحد دون غيره يمكن أن يسفر عن فراغ تشريعي في كثير من الحالات، كما أن الجمع بين أكثر من أسلوب لا يخلو أيضا من المخاطر، فالإضافة إلى النصوص وإضافة نصوص جديدة قياسا على نصوص قائمة بالفعل إذا لم يتم بكثير من الحذر فإن أكثر من نص قانوني يمكن أن ينطبق في ذات الوقت على النشاط الإجرامي الواحد.

[1] د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، مرجع سبق ذكره، ص.317.

وفي دراسة أجريت حول الاتجاهات التشريعية للدول التي تعاملت مع ج.م تشريعيا حتى أكتوبر 1987، سواء فيما يتعلق بالاتجاه السائد أو الوسيلة التي لجأ إليها المشرع، أسفرت الدراسة عن تباين في مواقف الدول المختلفة في هذا الخصوص. فبينما تأخذ الولايات المتحدة الأمريكية على سبيل المثال على المستوى الفيدرالي بالاتجاه الذي يهتم بالمعلومات في ذاته Informationapproach، نجد أن قوانين الولايات تركز على حماية الملكية Property Approach وتأخذ كل من الدنمارك وفنلندا والنرويج بالاتجاه الثاني، بينما تأخذ كل من النمسا وسويسرا بالاتجاه الأول، ومن ناحية أخرى تأخذ المملكة المتحدة بالاتجاه الذي يركز على سلامة المعلومات Forgery Approach، وتجمع بعض الدول بين أكثر من اتجاه Mixed Approach كبلجيكا وكندا والسويد وألمانيا، ولقد خرجت بعض الدول حاليا على التقسيم السابق كالولايات المتحدة (مستوى الولايات) وسويسرا حيث جمعت بين أكثر ن اتجاه، فإذا كان التشريع في سويسرا يتجه إلى حماية الملكية بصفة أساسية فإن جانبا بدأ يتجه إلى حماية سلامة المعلومات.[1]

أما فيما يتعلق بالوسيلة التي يلجأ إليها المشرع لتجريم جرائم المعلوماتية فقد أظهرت الدراسة أيضا تباينا في مواقف الدول في هذا الخصوص فبينما تتجه بعض الدول إلى الإضافة إلى نصوص قائمة Supplementation كالولايات المتحدة الأمريكية، أو إلى إضافة نصوص قياسا على نصوص تقليدية Extention كالنمسا وكندا والدنمارك والنرويج وسويسرا، تتجه دول أخرى إلى تمييز ج.م عن غيرها من الجرائم إما بوضع نص عام يتعامل مع الأوجه المختلفة لها أو بوضع مجموعة من النصوص المستقلة في قسم خاص ملحق بقانون العقوبات أو في تشريع مستقل One For All كالولايات المتحدة (المستوى الفدرالي) وبلجيكا وفرنسا، وأخيرا اتجهت دول أخرى إلى الجمع بين أكثر من وسيلة من هذه الوسائل كهولندا والسويد والحقيقة أن هذا الاتجاه الأخير بدأ يغلب الآن على كثير من التشريعات.

[1] د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، مرجع سبق ذكره، ص.318.

الخاتمة

تعد هذه الدراسة حصيلة جهد متواضع قمنا به بهدف التصدي لهذا الموضوع الا وهو الحماية الجنائية للمعلومات على شبكة الانترنت, ذو الصبغة العلمية الغربية ،غير أنه لا يجب أن يكون هذا الطابع العلمي عقبة تمنعنا من التوسع في قاعدة النقاش حول الاجرام المعلوماتي ؛ و حتى لا يبق موضوع ج.م من المناطق المحرمة التي يتجنب معظم الباحثين و دارسي القانون الخوض فيها.

ولا ننكر الصعوبة التي واجهتنا لانجاز هذه الدراسة نظرا لنقص المراجع في هذا الميدان من جهة , و من جهة اخرى نظرا لضرورة المامنا بالجوانب التقنية حتى نتمكن من الاحاطة بالجوانب القانونية ،الا أن ذلك لا يمنع اننا توصلنا في ختام دراستنا لهذا الموضوع الى عدة جوانب يمكن بلورتها فيما يلي :

1- النتائج :

- لقد توصلنا الى نتيجة بالغة الاهمية وهي غياب مفهوم عام متفق عليه بين الدول –حتى الأن – حول التعريف القانوني للنشاط الاجرامي المتعلق بج.م و اللأنماط المكونة لها من جهة.

- ومن جهة اخرى عدم كفاءة و ملاءمة النصوص التقليدية مع جرائم اختراق نظم الكمبيوتر لأنها عادة ما تكون متعلقة بوقائع مادية خاصة بالجرائم التقليدية و بالنتيجة فهي لا تتلاءم مع الوقائع " المعنوية" التي تتميز بها ج.م كاختراق المعلومات المبرمجة و تغييرها في الكمبيوتر من جهة أخرى .

وخلصنا الى ان المعلومة مرتبطة بوسيلة نقلها وتتطور بتطورها,فالمعلومة المنقولة عن طريق شبكة الانترنت تختلف وتتطور عن المعلومة المنقولة بواسطة الصوت والالواح قديما,حيث ظهرت المعلومات الصوتية و المرئية واندماج الصوتيات والمرئيات ويشترط في المعلومات لكي يمكن ان تتمتع بالحماية الجنائية لها على شبكة الانترنت,وهذه الشروط هي,ان تكون المعلومة محددة ومبتكرة بان تكون نتاج عمل ذهني و فكري لاحاد الناس او مجموعة منهم,وبالتالي تكون متميزة عن المعلومات العامة المتاحة

لكافة الناس, وان يتوافر لها خاصية السرية و الاستئثار ويقصد بالسرية ان تكون الرسالة اللتي تحملها المعلومة محددة بمجموعة معينة من الاشخاص وان تخص احدهم,وان تكون المعلومة معالجة اليا.

ووفقا لنظرية المال الاعلامي, فان المعلومات اصبحت تمثل قيمة اقتصادية كبرى,فهي بالاستقلال عن دعامتها تمثل قيمة قابلة للاستحواذ, وذلك من شانه ان يغير نظرة القانون الجنائي الى الاشياء المعنوية, بينما يربالاتجاه التقليدي,بان المعلومة لها طبيعة من نوع خاص فهي غير قابلة للاستئثار الا عن طريق حقوق الملكية الفكرية,وعلى ذلك فان المعلومات اللتي لاتدخل من ضمن هذه الحقوق لا تندرج في مجموعة القيم المحمية نظرا لطبيعتها المعنوية.

وتوصلنا الى ان سمات م.م. تختلف عن سمات المجرم العادي ,فالاول يجب أن تكون له ثقافة ومعرفة بتقنيات الحاسب الالي وشبكة الانترنت, كما انه يتميز بالذكاء العالي بالمقارنة بالمجرم العادي, ويطلق عليهم مصطلح الهكرة او الهاكرز بمعنى القراصنة.

- السمة المميزة للكثير من الجرائم المعلوماتية هي أنها من النوع العابر للحدود TRANSNATIONAL. و بالتالي فانه بات من الضروري ابرام معاهدات للتسليم أو للمعاينة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولي و ان وجدت فانها غير كافية لمواجهة المتطلبات الخاصة .

- غياب نصوص دولية موحدة تواجه جرائم العالم الافتراضي،غياب نصوص دولية موحدة تكفل الحماية الجنائية للمعلومات على شبكة الانترنت.

- وجود قصور في قوانيننا في مجال الجرائم المعلوماتية ،اذ أنه لا تزال الكثير منها تخضع للنصوص التقليدية و هو الشيء الذي يعد مساسا مباشرا لمبدأ الشرعية من جهة و الذي ينعكس سلبا في مجال المتابعة اذ انه يؤدي الى افلات الكثير من الجناة من العقاب. و نظرا لنسبية الحماية من خلال النصوص التقليدية لجرائم الأموال نتيجة للطبيعة المتميزة للمال المعلوماتي استقر الفكر القانوني على اخضاع المعلوماتية لقوانين الملكية الفكرية.

- كلما زادت تحصينات الكمبيوتر كلما تفاقمت معها الاختراقات بوجه عنيف و ذكي يخترق سياج الحكومة الالكترونية.

- و بالتالي خلصنا الى أن فكرة تطويع النصوص التقليدية المتعلقة بجرائم الأموال و تعديلها بما يتلاءم و طبيعة المال المعلوماتي نجحت و لو نسبيا في تغطية بعض الحالات فقط ،و ان كانت لا تحقق الحماية الكافية للمال المعلوماتي نظرا للطبيعة المتطورة لهذا المال و التي تختلف عن المال التقليدي ، و عليه يصبح البحث على سبيل آخر للحماية أمر لا مفر منه .

2- **الاقتراحات:**

- اعتمادا للنتائج التي توصلنا اليها من خلال دراستنا هذه سنحاول القاء الضوء على موقف المشرع الجزائري الذي اتخذه لمواجهة هذا الشكل الجديد من الاجرام الحديث ، فالملاحظ أن مشرعنا قد استدرك مؤخرا الفراغ القانوني الملحوظ في مجال الاجرام المعلوماتي و قد اعتمد في ذلك حلا يضمن حماية مزدوجة للحاسب الآلي من خلال نصوص حق المؤلف من جهة، و من خلال نصوص خاصة أدمجها في قانون العقوبات من جهة أخرى .

- رغم اعتراف المشرع لبرامج الحاسب الآلي بصفة المصنف المحمي الا أنه نظرا لوجود بعض المفاهيم التقليدية لحقوق المؤلف لا تتماشى مع برامج الحاسب الآلي و التي لم بتداركها تعديل قانون الملكية الأدبية و الفنية و عليه نقترح اجراء تعديل بوضع نظام خاص بايداع برامج الحاسب الآلي مع تقصير الحماية الى أقل من 50 سنة بعد الوفاة نظرا للتطور السريع للمعلوماتية .

- و عليه و رغم اعتراف المشرع الجزائري لبرامج الاعلام اللآلي و قواعد البيانات بصفة المصنف المحمي الا أنه لا يخفى علينا أن الحماية الجزائية للبرامج من خلال حق المؤلف تنصب بصفة أساسية على شكل البرنامج أو مضمونه الابتكاري فقط دون أن تغطي تلك الحماية كل مضمون البرنامج ،و لهذا السبب كان البحث عن نوع آخر من الحماية ينضم الى الحماية السابقة من الحماية الجزائية لهذه

البرامج في مثل هذه الحالات أمرا ضروريا،و لذلك فلا مفر من ضرورة اللجوء الى استحداث نصوص تجريمية خاصة بالمعلوماتية.

- استحداث نص خاص بالاعتداء على سير نظام المعالجة الآلية للمعطيات.
- استحداث نص خاص بالتزوير المعلوماتي ،وكذا توسيع مفهوم المحرر ليشمل أية دعامة أخرى.
- حماية البرامج و المعلومات المعالجة بصفة مستقلة عن طريق معاقبة الاستيلاء عليها دون المساس بسلامتها أوأصالتها أو نسخ صور منها عند تشغيل الجهاز.

ضرورةتكوين القضاةفي مجال الجرائم المعلوماتيةخاصة وأن القاضي الجزائري وفي غياب النصوص التجريمية ونظرالمستلزمات مبدأشرعيةالجرائم والعقوبات وحظر القياس في المجال الجنائي،يجد نفسه مقيدا تجاه هذا الشكل المستحدث من الإجرام.

-ضرورة التعاون الدولي لمواجهة صور السلوك المنحرف في البيئة المعلوماتية، وهذا ماأوحت به الاتفاقية الدولية للإجرام المعلوماتي المبرمة في سنة2001وذلك بتشجيع الدول على إدراج الجرائم المعلوماتيةفي قوانينها العقابية،كماأن المنظمة الدولية للملكية الفكرية أصدرت نصوصا نموذجية أدرجت منخلالها الحاسب الآلي في إطار المصنفات المحمية،ووضعت أحكاما تتماشى وطبيعة هذا المصنف.

المراجع والمصادر

I- المراجع باللغة العربية

أولا: المراجع العامة

1- جميل عبد الباقي الصغير: القانون الجنائي والتكنولوجية الحديثة الكتاب الأول: الجرائم الناتجة عن استخدام الحاسب الآلي. دار النهضة العربية القاهرة 1992.

ثانيا: المراجع الخاصة

1- أحمد السمدان –النظام القانوني لحماية برامج الحاسب الآلي–مجلة الحقوق–الكويت– العدد4،سنة 1987.

2- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الثانية، 2006.

3- خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الطبعة 2008

4- عامر إبراهيم قنديلجي– الدكتورة إيمان فاضل السامرائي، تكنولوجيا المعلومات وتطبيقاتها، الورالي للنشر والتوزيع.

5- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الطبعة الأولى 2006.

6- عبد الله عبد الكريم، الجرائم المعلوماتية والانترنت، منشورات الحلي الحقوقية، الطبعة الأولى، 2007.

7- عفيف كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون.

8- عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلي الحقوقية، الطبعة الثانية، 2007.

9- المؤلفان منير محمد الجنبيهي– ممدوح محمد الجنبيهي، أمن المعلومات الالكترونية، دار الفكر الجامعي، 2006.

10- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، 2004.

11- مدحت رمضان جرائم الاعتدار على الأشخاص والانترنت، دار النهضة العربية، القاهرة، 2000.

12- المستشار عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، 2006.

13- منير محمد الجنبيهي- ممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، 2006.

14- نائلة عادل فريد، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبى الحقوقية، 2005.

15- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، 1429هـ- 2008م.

16- أمير فرج يوسف، الجرائم المعلوماتية على شبكة الأنترنت، دار المطبوعات الجامعية، بدون تاريخ نشر.

17- أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، 2005.

18- عمر محمد بن يونس: مشكلة قواعد البيانات، موسوعة التشريعات العربية ، دار الفكر الجامعي: الاسكندرية:2004.

19- عمرو عيسى القي، الجرائم المعلوماتية، جرائم الحاسب الآلي والأنترنت في مصر والدول العربية، المكتب الجامعي الحديث، 2006.

20- عمرو عيسى الفقي، الجرائم المعلوماتية، المكتب الجامعي الحديث، طبعة 2006.

ثالثا: الرسائل والمذكرات:

1- قارة أمال، الجريمة المعلوماتية، رسالة ماجستير، جامعة الجزائر، كلية الحقوق –بن عكنون–، الاختصاص القانون الجنائي والعلوم الجنائية، 2005.

2- محمد أحمد: حقوق الإنسان بين الخصوصية والعالمية، رسالة لنيل دبلوم الدراسات العليا المعمقة: كلية الحقوق الدار البيضاء 2003.

3- محمد هلي العريان، الجرائم المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة الإسكندرية.

4- محمود عبده الدلالعة: الحماية الدولية والقانونية لتكنولوجيا المعلومات وبرامج الحاسب رسالة لنيل الدكتورة: كلية الحقوق الدار البيضاء 2002.

5- أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دراسة مقارنة، رسالة دكتوراه، جامعة القاهرة، كلية الحقوق.

6- أيمن عبد الله فكري، جرائم نظم المعلومات، رسالة دكتوراه، جامعة المنصورة، كلية الحقوق، 2005-2006.

7- نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، رسالة دكتوراه، جامعة القاهرة، كلية الحقوق، طبعة 2003.

8- رشدي محمد علي محمد علي، الحماية الجنائية للمعلومات على شبكة الانترنت، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، 2009.

9- طيبي مؤنس، العالم يتحول إلى قرية، الرسالة بيت بيرل، 1997.

10- كوثر مازوني، الشبكة الرقمية وعلاقتها بالملكية الفكرية، مذكرة مجستير، كلية الحقوق جامعة بن عكنون الجزائر، 2004- 2005.

11- عمر نجوم: الحجية القانونية لوسائل الاتصال الحديثة: دراسة تحليلية في نظام الإثبات المدني. أطروحة لنيل الدكتوراه: كلية الحقوق الدارالبيضاء 2003-2004.

رابعا: المقالات والمجلات:

1- المذكرة الإيضاحية للقانون رقم 354 لسنة 1954م الصادر بشأن حماية حقوق المؤلف في مصر والذي ألغي، وتم العمل بالقانون رقم 82 لسنة 2002 بشأن حماية الملكية الفكرية.

2- طيبي مؤنس: شبكة الانترنت للطالب والمعلم، صدى التربية 47، آذار 1999.

3- علي كريمي: تطور قوانين الإعلام في الدول المغاربية"ورقة مقدمة في الحلقة الدراسية المنظمة من طرف الإيسيسكو يونيو 2009 بطرابلس ليبيا"

4- غزة على محمد الحسن: قانون الانترنت، شركة مطابع السودان للعملة: رقم الإبداع 404/2005

5- مالك خدام: جرائم الحاسب والانترنت... ارتفاع معدل استغلال الأطفال جنسيا جريدة الثورة: الاثنين 2005/3/7

6- مركز حرية الإعلام بالشرق الأوسط وشمال إفريقيا: القاصرون وجرائم الانترنت في المغرب سبتمبر 2006.

7- ورقة عمل مقدمة من: الدكتور محمود صالح العادلي – الجرائم المعلوماتية – ماهيتها وصورها

8- يونس عرب: التشريعات والقوانين المتعلقة بالانترنت في الدول العربية.ورقة عمل: مقدمة إلى مؤتمر ومعرض التكنولوجيات المصرفية العربية والدولية- اتحاد المصارف العربية 28-29 تشرين الأول 2002 عمان الأردن

9- يونس عرب: مقال في جريدة المساء: عدد:535/ السبت الأحد 2008/8/7 تحت عنوان: قانون الكمبيوتر... بين حرية تبادل المعلومات وحماية الإبداع.

10- يونس عرب، جرائم الكمبيوتر والأنترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002، تنظيم المركز العربي للدراسات البحوث الجنائية، أبو ظبي 10-2002/02/12.

11- الأسرار التجارية في مجال الملكية الفكرية – دكتور قيس محافظة – أستاذ القانون بكلية الحقوق بالجامعة الأردنية – ورقة مقدمة إلى: ندوة الويبو الوطنية عن الملكية الفكرية لأعضاء هيئة التدريس وطلاب الحقوق في الجامعة الأردنية تنظمها المنظمة العالمية للملكية الفكرية (الويبو)

بالتعاون مع الجامعة الأردنية – عمّان، من 6 إلى 8 أبريل 2004. و حماية المعلومات غير المكشوف عنها بناء على اتفاق تريبس- دكتور حسام الدين عبد الغني الصغير أستاذ ورئيس قسم القانون التجاري والبحري، كلية الحقوق جامعة المنوفية – وعضو لجنة إعداد مشروع قانون حماية حقوق الملكية الفكرية – ورقة مقدمة إلى: الندوة الوطنية المشتركة بين الويبو واتحاد المحامين العرب، عن الملكية الفكرية للمحامين، تنظمها: المنظمة العالمية للملكية الفكرية (الويبو)، اتحاد المحامين العرب، بالتعاون مع حكومة مملكة البحرين، ونقابة محامي البحرين المنامة، من 23 إلى 25 يناير 2003.

12- حسام الدين عبد الغني الصغير، حماية المعلومات غير المكشوف عنها بناءا على اتفاق تريبس، ورقة عمل مقدمة إلى الندوة الوطنية المشتركة بين الويبو واتحاد المحامين العرب عن الملكية الفكرية للمحامين، تنظمها المنظمة العالمية للملكية الفكرية (الويبو)، اتحاد المحامين العرب بالتعاون مع حكومة مملكة البحرين ونقابة محامي البحرين، المنامة، من 23 إلى 25 يناير wipo-2003 alm/bah/03doc7-

خامسا: الأحكام والقرارات القضائية

1- المادة 138 فقرة أولى من القانون رقم 82 لسنة 2002 الصادر بشأن حماية الملكية الفكرية في مصر.

2- المرسوم الرئاسي رقم 341/97 (97/09/13) المتضمن انضمام الجزائر مع التحفظ إلى اتفاقية برن لحماية المصنفات الأدبية والفنية المؤرخة في 1896/06/09 والمتممة في باريس في 1896/05/04 والمعدلة في 1979/09/28 (ج.ر. مؤرخة في 97/09/14).

3- الاتفاقية الدولية حول الإجرام السيبيري التي أبرمت بتاريخ 2001/11/08 من طرف المجلس الأوروبي وتم وضعها للتوقيع منذ تاريخ 2001/11/23.

4- الأمر 05/03 الصادر بتاريخ 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة المعدل والمتمم للأمر 14/73.

5- القانون 15/04 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر 156/66 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات (ج ر 71 بتاريخ 2004/11/10).

6- قانون رقم 09-04 مؤرخ في 14شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها.

7- قانون المعالجة الآلية للمعطيات – ملفات المعطيات والحريات الفردية رقم 17-78 تاريخ 1978/01/6.

8- قانون حماية الكمبيوتر: بين تبادل المعلومات وحماية الابداعجريدة المساء: عدد 535 السبت/ الأحد 7/6 يونيو 2008.

9- الجريدة الرسمية العدد 48 في 1979/11/29، موسوعة التشريعات العربية، الجزء 46 مكرر، مصر، ثقافة وقانون.

10- الجريدة الرسمية رقم 5584 الصادرة يوم الخميس 6 دجنبر 2008.

II- المراجع باللغة الأجنبية

Bibiographie en Langues étrangères

A- Ouvrage généraux :

1- EL HOUCINE ENNACIRI : droit d'Internet au Maroc Mémoire de D.E.S.A faculté de droit - Rabat Agdal 2006 Du droit et des libertés sur l'Internet rapport au premier ministre français. Paris- documentation française 2001.
2- HOLLEAUX, « la loi de 6 Janvier 1978 sur l'informatique et liberté » rev. Adm. 1978. N°181, P.31-40 et N°182.

B- Ouvrage spéciaux :

3- KAPLAN, YASMINE- internet, zone de non droit ? 1996.

C- Revues (articles) :

1- AIGRAIN : Au-delà du logiciels libre, le temps des biens communs : le monde diplomatique, Octobre 2005
2- BOUTI : les enjeux du commerce électronique pour les commerçants : cybers PME-PMI artisans on line, REMALD, sirie études, n°50, Mai-juin 2003.
3- CATALA « la propriété de l'information » Cité par f.Toubal ;le logiciel- analyse juridique FUDUL .L.G.D.J.1986.
4- Du droit et des libertés sur l'Internet rapport au premier ministre français. Paris- documentation française 2001.
5- LAJMI : la liberté de l'information a l'ére du cyberespace, Revue Tunisienne de la communcation n° 37-38, Janvier/ décembre 2001

D- Lois et conventions :

1- ABA Section Creates First Digital Signature Guidelines To Aid In Security of The Internet, 1996.
2- Conseil de l'Europe : convention sur la cybercriminalité Budapest, 23 Novembre 2001
3- Computer viruses: Information age vulnerability and the technopath, Amercan criminal Law Review, Vol. 27, 1990.
4- E-Government in Sweden - visions and actions Speech by State Secretary at the conference Digital Government in Finland 4 October 2001.Kansas Statute No. 16-1602. 2001-2002.
5- OECD Compter Related Crime : Analysis of legal policy.
6- Shuterland (Edwin H) "White collar criminality " Gers (Gilbert) in white collar criminal The offender in business the professions atherton press 1968
7- The act on Data processing, Data Files and individual liberties N°17-78 (1978).
8- Loi N°17-78 du Janvier 1978 relative à l'informatique aux fichiers et aux libirtes (J.O du 7 Janvier 1978).
9- The Related crimeon computerRecommandation N R89 – 9.

ثالثا:مواقع الأنترنت

4- Re No V. American civil liberties unian, 0000 u, s 96- 511, 1997, http : // Supect. Lawi. Carnell. Edu/ htmt/ 96-511.ZS. htm/.
1- يونس عرب، جرائم الكمبيوتر والأنترنت، المعنى والخصائص والصور واستراتيجية المواجهة القانونية:www.arablaw.org/download/cyber-crimes-general.doc
2- http : // Ahmad Farag. bbF/ aSh. Net/ t 49- topic
3- http : // alyaseer. Net/ vb/ sHowthread. Php ? t 13301.
4- http : // ar. Wikipedia. Org/ wiki/.
5- http : // Knol. Google. Com/k/. .الملكية الفكرية وج.م، مقالة لـ محمود هيبة
6- http : // www. Aluah. Net/ culture/ /128516/.

7- http : // www. Bna. Com/ e- law/ docs/ aolcuber. Htm/.
8- http : // www. Cbi. Um n. edu/ darpa/ ipto. Htm/.
9- http : // www. Cksu. Com/ vb/ sHowthread. Php ? t 201452.
10- http : // www. Conventions. Coe. Int/ treaty/ en/ projects/ finalcyberapex. Htm.
11- http : // www. inF- te. Com/ vb/ inF 2548. جرائم الانترنت، كلية الحاسوب وتكنولوجيا المعلومات.
12- http : // www. Kenana online. Com/ page / 8907
13- http : // www. Lawjo. Net/ Vb/ SHowthread. Php ? t= 4225
14- http : // www. Omanlega/ net/ journal/ ? p = 133. الجرائم الإفتراضية وجهود سلطنة عمان التشريعية في مواجهتاه، مجلة عمان القانونية.
15- http : // www. Shaimaatalla. Com/ Vb/ SHowthread. Php ? t= 3951.
16- http : // www. Zinj- org/ Forum/ SHowthread. Php ? t = 2821. صفات م.م.- شبكة الزنج الإسلامية.
17- http : // yomgedid. Kenanaonline. Com/ topicas/ 57592.
18- http://coeria.edu.sa/index.php/ar/assurance-awamess/articles/51-forensic-and-computer-crimes/987-tupes-of-electronic-crime-and-regulations-in-force-in-saudi-arabia.html.
19- http://internet–juridique.net/chroniques/sitejuridique.html
20- http://news.bbc.co.uk/hi/arabic/news/newsied1153000/1153/24.stm.
21- http://www.arablaw.org/download/cybercrimes-workpaper.doc
22- http://www.iitf.nist.gov
23- http://www.legifrance.gouv.fr/waspad/uncode?code=cpenalll.rcv.
24- Internet society, « ABrief History of internet and related networks. http : // www. Isoc. Org/ internet/ history/ cerf. Shtm/.
25- Georgio Bovenzi, labilités of system opératoires an the internet, Berkeley technologie law journal-voll. Lart.1, p2, available on

line at : http : // www.Berkeley. Edu/ journal/ ptlg/ articles/ 1111 Bovenzi/ htm 1/ text/ htm.

26- The internat Society hime page online available : http : // www. Isoc.org.

27- www. Minshawi. Com/ old/ intern et crime- in 20% law- htm.

28- محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتاه، مركز الإعلام الأمني، وزارة الداخلية، الأكاديمية الملكية للشرطة....4 -1 /www.policemc. Giv. Bh/ reports/ 2011/ april

29- Samia MIHOUB : « la question le l'Internet arabe ou quand les états se trompent de cible, www.africultures.com/php/index.php

الملاحق

أول حكم قضائي فى جرائم الإنترنت بالوطن العربي

23/12/2008

الرياض: في أول حكم قضائي في الوطن العربي، قضت محكمة سعودية بسجن شاب سعودي وجلده وتغريمه بعد اتهامه بارتكاب جريمة إلكترونية عبر الإنترنت.وأمرت محكمة في منطقة الاحساء شمال شرق السعودية، بسجن مواطن وجلده وتغريمه، بعدما ثبت أنه قام باختراق البريد الإلكتروني الخاص بفتاة سعودية، وسحب صورها الشخصية منها، وابتزازها.

وأوضح رئيس المحكمة الجزئية في الاحساء، في تصريحات نقلتها عنه صحيفة الوطن، أن المحكمة اعتبرت الشاب قد ارتكب "جريمة إلكترونية"، وتم معاقبته وفق نظام مكافحة الجرائم الإلكترونية السعودي .

وأشار إلى أن الحكم الذي يعد أول حكم قضائي يعاقب فيه متهماً في جريمة إلكترونية كان تطبيقاً لنظام مكافحة الجرائم الإلكترونية – الفقرة الثالثة من المادة الثالثة من نظام مكافحة الجرائم المعلوماتية.

وأكد أن إقرار المتهم الصريح بجرمه في التحقيقات التي تمت من قبل هيئة التحقيق والادعاء العام كان دليلاً كافياً لثبوت التهمة المنسوبة إليه، بعد أن عمد شاب سعودي إلى ابتزاز فتاة سعودية من خلال اختراق بريدها الإلكتروني والحصول على صورها وتهديدها بفضح هذه الصور لذويها.

وأوضح إلى أن الحكم في القضية لم يتطلب وجود خبراء في الشبكة العنكبوتية لأن المسألة واضحة وهيئة التحقيق والادعاء العام أدانت المتهم وبعد مناقشته اعترف تلقائياً وصدر الحكم.

- **<u>للجريمة أشكال وأنواع</u>**

عندما ظهرت شبكة الإنترنت ودخلت جميع المجالات كالكمبيوتر بدءًا من الاستعمال الفردي ثم المؤسسي والحكومي كوسيلة مساعدة في تسهيل حياة الناس اليومية، انتقلت جرائم الكمبيوتر لتدخل فضاء الإنترنت، فظهر ما عرف بجرائم الإنترنت كأداة أساسية، وكما هو الحال في جرائم الحاسوب كذلك جرائم الإنترنت قد تكون الإنترنت هدفًا للجريمة أو أداة لها.

ويقسّم المهندس حمد بن عبد العزيز السليم – مدير مركز أمن المعلومات بوحدة خدمات الإنترنت في مدينة الملك عبد العزيز للعلوم والتقنية- جرائم الإنترنت ضمن فئات متعددة منها ما يتعلق بجهاز الكمبيوتر كإتلاف وتشويه البيانات والتلاعب في المعلومات المخزنة، وأخرى تتعلق بالشخصيات أو البيانات المتصلة بالحياة الخاصة، بالإضافة إلى جرائم ترتبط بحقوق الملكية الفكرية لبرامج الكمبيوتر، وانتحال شخصية أخرى بطريقة غير شرعية على الإنترنت، والمضايقة والملاحقة، والتغرير والاستدراج وهما من أشهر جرائم الإنترنت وأكثرها انتشارًا خاصة بين أوساط صغار السن من مستخدمي الشبكة.

وركز مدير مركز أمن المعلومات على صناعة ونشر الإباحية مما يحضُّ القاصرين على أنشطة جنسية غير مشروعة، وصناعة الإباحية من أشهر الصناعات الحالية وأكثرها رواجًا خاصة في الدول الغربية والأسيوية علاوة على عمليات النصب والاحتيال نظرًا لأن الإنترنت مجال رحب تمارس فيه جميع أشكال التعاملات إلا هذه الميزة شابتها سلبيات عديدة أبرزها إمكانية النصب والاحتيال بخرق هذه التعاملات .

وهناك العديد من الأمثلة لجرائم ارتكبت بالفعل من خلال الانترنت ففي بنك لويدز في أمستردام قام شاب عمره 26 عاماً بتحويل مبلغ 8.4 مليون دولار عبر نظام الحوالات العالمية من فرع هذا البنك في نيويورك إلى حساب في بنك آخر في سويسرا .

واعتقلت الشرطة في إحدى مدن ولاية أوريجن الأمريكية شابًا عاطلاً عن العمل عمره 26 عامًا استخدم أحد مواقع الدردشة على الإنترنت لتنظيم انتحار جماعي فيما يسمى بعيد الحب هذا العام لمن لم يوفق في حياته العاطفية.

روبر مورس شاب أمريكي يبلغ من العمر 23 عامًا أطلق فيروسًا باسمه دمّر 6 آلاف نظام عبر الإنترنت بينها أجهزة عدد من المؤسسات الحكومية بخسائر بلغت مئة مليون دولار، عوقب على إثرها بالسجن لمدة 3 سنوات .

أما تيموثي ألن ليود فهو مصمم ومبرمج فصل من عمله، فما كان منه إلا أن أطلق قنبلة إلكترونية ألغت كافة التصاميم وبرامج الإنتاج لأحد أكبر مصانع التقنية العالية في نيوجرسي التي تعمل لحساب وكالة الفضاءnasaوالبحرية الأمريكية .

وآخر تزعم عصابة من "الهاكرز" بمدينة الإسكندرية المصرية تضم خمسة أشخاص للاستيلاء على حسابات بطاقات "في" الخاصة بعملاء البنوك، لكن الشاب الفرنسي جان كلود كان أكثر نبلاً من أفراد العصابة المصرية، فقد استطاع تصميم بطاقة صرف آلي وسحب بها مبالغ من أحد البنوك ثم ذهب إلى البنك وأعاد إليه المبالغ وأخبرهم أنه فعل ذلك ليؤكد لهم أن نظام الحماية في بطاقات الصرف الخاصة بالبنك ضعيف ويمكن اختراقه، إلا أن ذلك لم يمنع الشرطة الفرنسية من إلقاء القبض عليه ومحاكمته .

الأمر نفسه فعلته مجموعة من الشباب الأمريكي أطلقوا على أنفسهم "الجحيم العالمي" إذ تمكنوا من اختراق مواقع البيت الأبيض، والمباحث الفيدرالية، والجيش، ووزارة الداخلية؛ لكنهم لم يخربوا تلك المواقع، بل اقتصر دورهم على إثبات ضعف نظام الحماية في تلك المواقع، إلا أنهم حوكموا أيضًا .

وقبل 5 سنوات ألقت السلطات الإسرائيلية القبض على شابين شقيقين ضريرين من الفلسطينيين ووجهت إليهما تهمة اختراق مواقع وزارة الدفاع الإسرائيلية.

Computer Crime Cases

Year 2000

- Hacker Pleads Guilty in New York City to Hacking into Two NASA Jet Propulsion Lab Computers Located in Pasadena, California (December 1, 2000)
- Orange County Man Pleads Guilty to Hacking into Government Computers (November 7, 2000)
- Texas Man is indicted for Unlawfully Accessing Computers of U.S. Postal Service, State of Texas, and Canadian Department of Defense (October 12, 2000)
- Man Suspected of Hacking into NASA Computers Taken into Federal Custody (September 21, 2000)
- Juvenile Computer Hacker Sentenced to Six Months in Detention Facility (September 21, 2000)
- "Global Hell" Hacker Sentenced to 26 Months Imprisonment (September 6, 2000)
- Three Kazak Men Arrested in London for Hacking into Bloomberg L.P.'s Computer System (August 14, 2000)
- "Darkside Hacker" Sentenced to 21 Months in Prison (July 24, 2000)
- Hacker Group Leader Arrested for Breaking into NASA Computers (July 12, 2000)
- Former Computer Network Administrator Guilty of Unleashing $10 Million Programming "Timebomb" (May 9, 2000)
- Alaska Man Indicted for Alleged Attack on United States Court Computer Systems (April 19, 2000)
- Second "Global Hell" Hacker Pleads Guilty; Patrick Gregory Faces up to Five Years in Prison for Conspiracy to Commit Telecommunications Fraud and Computer Hacking (April 12, 2000)
- Chad Davis, "Global Hell" Hacker, Sentenced to Six Months in Prison, Three Years Probation, for Air Force Network Hacks (March 1, 2000)
- Boston Computer Hacker Charged with Illegal Access and Use of United Stated Government and Private Systems (February 23, 2000)

Year 2001

- Bowdoinham, Maine Hacker Into United States Courts' Information System Pleads Guilty (December 18, 2001)

- Connecticut Hacker Indicted for Attacks on San Diego Auto Site (December 18, 2001)
- Man Sentenced for Unauthorized Access into Computer Systems of Connecticut Consulting Firm (December 14, 2001)
- Former Financial Institution Employee Sentenced for Unauthorized Computer Access to Customer Account Information (November 30, 2001)
- Chardon, Ohio Woman Sentenced for Computer Fraud via Unauthorized Access of Employer's Computer System (November 26, 2001)
- Former Cisco Systems, Inc. Accountants Sentenced for Unauthorized Access to Computer Systems to Illegally Issue Almost $8 Million in Cisco Stock to Themselves (November 26, 2001)
- Man Indicted for Hacking Computers Belonging to Public Affairs Group (October 22, 2001)
- Russian Computer Hacker Convicted by Jury in Seattle, Washington (October 10, 2001)
- Former Chase Financial Corp. Employee Pleads Guilty to Unlawful Access to Chase Manhattan Bank to Defraud Chase Financial Corp. and Chase Manhattan Bank (October 9, 2001)
- Brian K. West, Employee of Oklahoma ISP, Pleads Guilty to Unauthorized Access Charge Under 18 U.S.C. S 1030(a)(2)(c) (September 24, 2001)
- Chardon, Ohio Woman Pleads Guilty to Computer Fraud via Unauthorized Access of Employer’s Computer System (September 14, 2001)
- Broward County, Florida Man Convicted of Sending Computer Virus to Destroy Purity Wholesale Grocers Inc’s Computer Systems (September 6, 2001)
- Hacker Sentenced in New York City for Hacking into Two NASA Jet Propulsion Lab Computers Located in Pasadena, California (September 5, 2001)
- Former Cisco Accountants Plead Guilty to Wire Fraud via Unauthorized Access to Cisco Stock (August 20, 2001)
- Russian National Indicted in Sacramento, California, on Computer Intrusion Charges (August 16, 2001)
- Former Chase Financial Corp. Employees in Cleveland, Ohio, Indicted for Unlawful Access to Chase Manhattan Bank and Chase Financial Corp. Computer Systems (August 7, 2001)

- Orange County, California Computer Hacker Pleads Guilty to Hacking University Computers, Defrauding Western Union (August 1, 2001)
- Lusby, Maryland Man Pleads Guilty to Sabotaging IRS Computers (July 24, 2001)
- Chardon, Ohio Woman Charged for Unlawful Access to Computer Server (July 6, 2001)
- Russian Computer Hacker Indicted in California for Breaking into Computer Systems and Extorting Victim Companies (June 20, 2001)
- Hampton, New Hampshire Man Convicted and Sentenced for Hacking into Former Employer's Computer Server (June 18, 2001)
- New York City Computer Security Expert Sentenced to 27 Months' Imprisonment for Computer Hacking and Electronic Eavesdropping (June 13, 2001)
- Russian National Arrested and Indicted in Connecticut for Penetrating U.S. Corporate Computer Networks, Stealing Credit Card Numbers, and Extorting the Companies by Threatening to Damage Their Computers (May 7, 2001)
- Orange County Computer Hacker Arrested In Scheme to Use Stolen Credit Cards to Make Wire Money Transfers via Western Union (April 18, 2001)
- Former Lance, Inc. Employee, from North Carolina Sentenced to 24 Months and Ordered to Pay $194,609 Restitution in Computer Fraud Case (April 13, 2001)
- Two Men from California Indicted on Conspiracy to Commit Computer and Wire Fraud via Unauthorized Access to Cisco Stock (April 4, 2001)
- Former Cisco Employee Pleads Guilty to Exceeding Authorized Access to Obtain Information from Cisco’s Computer Systems (March 21, 2001)
- Ex-GTE Employee Pleads Guilty to Intentionally Damaging Protected GTE Computers (March 20, 2001)
- New York City Computer Security Expert Convicted by Jury of Computer Hacking and Electronic Eavesdropping (March 7, 2001)
- Former Federal Court Systems Administrator Sentenced for Hacking Into Government Computer System (January 22, 2001)

Year 2002

- St. Joseph, Missouri Man Charged in Western District's First Computer Hacking Indictment (December 20, 2002)
- U.S. Arrests Queens, New York, Man on Computer Fraud Charges (December 20, 2002)
- Disgruntled UBS PaineWebber Employee Charged with Allegedly Unleashing "Logic Bomb" on Company Computers (December 17, 2002)
- Hacker Pleaded Guilty to Attacks on San Diego Auto Site (November 15, 2002)
- British National Charged with Hacking Into N.J. Naval Weapons Station Computers, Disabling Network After Sept. 11; Indictment Also Filed in Virginia for Other Military Intrusions (November 12, 2002)
- London, England Hacker Indicted under Computer Fraud and Abuse for Accessing Military Computers (November 12, 2002)
- Russian Computer Hacker Sentenced to Three Years in Prison (October 4, 2002)
- San Gabriel Valley, California Man Pleads to Illegally Accessing Former Employer's Computers (September 9, 2002)
- San Fernando Valley Residents Indicted in Scheme to Hack Into Software Firm Computer and Delete $2.6 Million Project (August 2, 2002)
- Two Kazakhstan Citizens Accused of Breaking Into Bloomberg L.P.'s Computer and Extortion are Extradited (May 21, 2002)
- Twenty Seven Month Sentence in Internet Fraud Scheme to Defraud Priceline.Com and Others; Unauthorized Computer Access Conspiracy May 17, 2002)
- Former Chief Technology Intrusions; Transmitting Threats Via the Internet (May 16, 2002)
- Green Bay, Wisconsin Man Charged with Computer Intrusion, Software Piracy and Numerous Destructive Acts (May 7, 2002)
- Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison (May 1, 2002)
- U.S. Charges Engineer with Computer Intrusion, Destruction of Database at Manhattan Apparel Company (April 26, 2002)
- Man Pleads Guilty to Unauthorized Access of Las Vegas Medical Imaging Computer System (April 17, 2002)

- Computer Operator Sentenced for Breaking Into Ex-Employer's Database (March 27, 2002)
- Parma, Ohio Man Indicted for Unauthorized Access into Computer System of Alltel Communications, Inc.; Threatening E-Mails (March 26, 2002)
- Former Computer Network Administrator at New Jersey High-Tech Firm Sentenced for Unleashing $10 Million Computer "Time Bomb" (February 26, 2002)
- Former Chase Financial Corp. Employees Sentenced for Scheme to Defraud Chase Manhattan Bank and Chase Financial Corporation (February 19, 2002)
- Orange County Computer Hacker Sentenced to Prison for Breaking into University Computers, NASA Systems (February 4, 2002)
- Manhattan Paralegal Sentenced for Theft of Litigation Trial Plan (January 30, 2002)
- San Francisco Man Pleads Guilty to Unauthorized Access of Catholic Healthcare West Computer Causing Damage (January 18, 2002)

Year 2003

- Milford, Ohio Man Pleads Guilty to Hacking (December 18, 2003)
- Former Hellmann Logistics Computer Programmer Sentenced for Unauthorized Computer Intrusion (December 5, 2003)
- Former Employee of American Eagle Outfitters Sentenced to Prison for Password Trafficking and Computer Damage (December 2, 2003)
- Three Men Indicted for Hacking into Lowe's Companies' Computers with Intent to Steal Credit Card Information (November 20, 2003)
- Two Alleged Computer Hackers Charged in Los Angeles as Part of Nationwide 'Operation Cyber Sweep' (November 20, 2003)
- Two Alleged Computer Hackers Charged in Los Angeles as Part of Nationwide 'Operation Cyber Sweep' (November 20, 2003)
- Dallas, Texas FBI Employee Indicted for Public Corruption (November 5, 2003)
- Disgruntled Philadelphia Phillies Fan Charged with Hacking into Computers Triggering Spam E-mail Attacks (October 7, 2003)
- Former Employee of Viewsonic Pleads Guilty to Hacking into Company's Computer, Destroying Data (October 6, 2003)
- President of San Diego Computer Security Company Indicted in Conspiracy to Gain Unauthorized Access into Government Computers (September 29, 2003)

- Juvenile Arrested for Releasing Variant of Blaster Computer Worm That Attacked Microsoft (September 26, 2003)
- U.S. Charges Hacker with Illegally Accessing New York Times Computer Network (September 9, 2003)
- Minneapolis, Minnesota 18 year old Arrested for Developing and Releasing B Variant of Blaster Computer Worm (August 29, 2003)
- Former Computer Technician in Douglasville, Georgia Arrested for Hacking into Government Computer Systems in Southern California (August 25, 2003)
- Russian Man Sentenced for Hacking into Computers in the United States (July 25, 2003)
- FBI Employee Arrested and Charged in Three Federal Indictments (July 17, 2003)
- Queens, New York Man Pleads to Federal Charges of Computer Damage, Access Device Fraud and Software Piracy (July 11, 2003)
- Kazakhstan Hacker Sentenced to Four Years Prison for Breaking into Bloomberg Systems and Attempting Extortion (July 1, 2003)
- Southern California Man Who Hijacked Al Jazeera Website Agrees to Plead Guilty to Federal Charges (June 12, 2003)
- Computer Hacker Sentenced to One Year and One Day And Ordered to Pay More than $88,000 Restitution For Series of Computer Intrusions and Credit Card Fraud (June 12, 2003)
- Three Californians Indicted in Conspiracy to Commit Bank Fraud and Identity Theft (May 12, 2003)
- Ex-employee of Airport Transportation Company Guilty of Hacking into Company's Computer (April 18, 2003)
- San Jose, California Man Indicted for Theft of Trade Secrets and Computer Fraud (April 2, 2003)
- Student Charged with Unauthorized Access to University of Texas Computer System (March 14, 2003)
- St. Joseph Man Pleads Guilty in District's First Computer Hacking Conviction (March 13, 2003)
- Computer Hacker Pleads Guilty to Computer Intrusion and Credit Card Fraud (March 13,2003)
- California Woman Convicted for Unauthorized Computer Access to Customer Account Information in Credit Union Fraud Prosecution (March 10, 2003)
- Los Angeles, California Man Sentenced to Prison for Role in International Computer Hacking and Internet Fraud Scheme (February 28, 2003)

- Former Employee of American Eagle Outfitters Indicted on Charges of Password Trafficking and Computer Damage (February 26, 2003)
- U.S. Convicts Kazakhstan Hacker of Breaking into Bloomberg L.P.'s Computers and Attempting Extortion (February 26, 2003)
- Ex-employee of Airport Transportation Company Arrested for Allegedly Hacking Into Computer, Destroying Data (February 20, 2003)
- Ohio Man Attacked NASA Computer System Shutting Down Email Server (February 13, 2003)
- Former Employee of Viewsonic Arrested on Charges of Hacking into Company's Computer, Destroying Data (February 6, 2003)
- Pittsburgh, Pennsylvania Man Convicted of Hacking a Judge's Personal E-Mail Account (January 23, 2003)

Year 2004

- Hacker Sentenced to Prison for Breaking into Lowe's Companies' Computers with Intent to Steal Credit Card Information (December 15, 2004)
- Nineteen Individuals Indicted in Internet 'Carding' Conspiracy (October 28, 2004)
- Ex-Official of Manhattan Computer Consulting Firm Pleads Guilty to Computer Attack Charge (September 9, 2004)
- California Man Admits Hacking Into Computers of High-Technology Company (August 31, 2004)
- Former Employee of a Massachusetts High-Technology Firm Charged with Computer Hacking (August 23, 2004)
- Six Internet Fraudsters Indicted in International Conspiracy to Steal More Than $10 Million From World's Largest Technology Distributor (August 4, 2004)
- Vallejo, California Woman Admits to Embezzling More Than $875,035 (July 28, 2004)
- Florida Man Charged with Breaking into Acxiom Computer Records (July 21, 2004)
- China Citizen Pleads Guilty to Unauthorized Access of a Software Company with Intent to Defraud (July 7, 2004)
- Seattle, Washington Man Arrested for Hacking into Internet Search Engine Alta Vista (July 2, 2004)

- Federal Judge Sentences Staten Island, New York Ex-Official of Local Internet Service Provider to Prison for Computer Attack (June 16, 2004)
- Pennsylvania Man Sentenced to Prison for Accessing Massachusetts Investor's On-line Investment Account and Making $46,000 in Unauthorized Trades (May 5, 2004)
- Former Employee of Viewsonic Sentenced to One Year for Hacking into Company's Computer, Destroying Data (February 23, 2004)
- Two California Men Indicted for Unlawfully Obtaining Credit Information, Attempted Credit Fraud (February 10, 2004)
- Former Employees of Dallas-based Car Parts Distributorship Charged with Repeatedly Intruding into Competitor's Computer Database for Commercial Advantage and Illegally Trafficking in Computer Passwords. (February 9, 2004)
- Louisiana Man Arrested for Releasing 911 Worm to WebTV Users (February 19, 2004)
- Man Pleads Guilty to Gaining Unauthorized Access and Recklessly Damaging Computers of Several High-Technology Companies Including eBay and Qualcomm From His Graduate School Dorm Room (January 29, 2004)
- Hacker Pleads Guilty in Manhattan Federal Court to Illegally Accessing New York Times Computer Network (January 8, 2004)

Year 2005

- Man Pleads Guilty to Infecting Thousands of Computers Using Worm Program then Launching them in Denial of Service Attacks (December 28, 2005)
- Silicon Valley Engineer Indicted for Stealing Trade Secrets and Computer Fraud (December 22, 2005)
- Former RNC New England Regional Director Convicted in New Hampshire Phone Jamming Case (December 15, 2005)
- Six Defendants Plead Guilty in Internet Identity Theft and Credit Card Fraud Conspiracy (November 17, 2005)
- Computer Virus Broker Arrested for Selling Armies of Infected Computers to Hackers and Spammers (November 3, 2005)
- Houston Man Pleads Guilty to Federal Identity Theft Charges, Says Justice Department (November 1, 2005)

- Massachusetts Teen Convicted for Hacking into Internet and Telephone Service Providers and Making Bomb Threats to High Schools in Massachusetts and Florida (September 8, 2005)
- Federal Jury Convicts Former Technology Manager of Computer Hacking Offense Defendant Found Guilty of Placing Computer "Time Bomb" On Employer"s Network Following Employment Dispute (September 8, 2005)
- Creator and Four Users of Loverspy Spyware Program Indicted (August 26, 2005)
- Justice Department Announces Conviction of Florida Man Accused of Massive Data Theft from Acxiom, Inc.(August 12, 2005)
- Disgruntled Phillies Fan/Spammer Sent to Prison for Four Years (July 14, 2005)
- Former IT Manager of Silicon Valley Firm Pleads Guilty to Computer Crime Charges (June 8, 2005)
- Former Alta Vista Employee Pleads Guilty to Hacking into Alta Vista Computer Systems (May 9, 2005)
- Former Computer Science Graduate Student Sentenced for Hacking Major Corporations (April 25, 2005)
- Pleasant Hill, California Computer Hacker from "Deceptive Duo" Guilty of Intrusions into Government Computers and Defacing Websites (March 11, 2005)
- Queens Man Sentenced to 27 Months' Imprisonment on Federal Charges of Computer Damage, Access Device Fraud and Software Piracy (February 28, 2005)
- Former IT Manager of Software Firm Indicted on Computer Crime Charges (February 16, 2005)
- Computer Hacker Who Victimized T-Mobile Pleads Guilty in Los Angeles Federal Court (February 15, 2005)
- Juvenile Sentenced for Releasing Worm That Attacked Microsoft Web Site (February 11, 2005)
- Minnesota Man Sentenced to 18 Months in Prison for Creating and Unleashing a Variant of the MS Blaster Computer Worm (January 28, 2005)

Year 2006

- Former Federal Computer Security Specialist Sentenced for Hacking Department of Education Computer (May 12, 2006)

- "Botherder" Dealt Record Prison Sentence for Selling and Spreading Malicious Computer Code (May 8, 2006)
- California Man Pleads Guilty in "Botnet" Attack That Impacted Seattle Hospital and Defense Department (May 4, 2006)
- San Diego Computer Expert Charged with Hacking into U.S.C. Computer System Containing Student Applications (April 20, 2006)
- Former Federal Computer Security Specialist Pleads Guilty to Hacking Department of Education Computer (March 1, 2006)
- Cleveland, Ohio Man Sentenced to Prison for Bank Fraud and Conspiracy (February 28, 2006)
- Former Officer of Internet Company Sentenced in Case of Massive Data Theft from Acxiom Corporation (February 22, 2006)
- Grand Jury Returns Indictment Charging Student with Accessing Protected Computer at University of Utah (February 17, 2006)
- Utah Man Charged with Bringing Down Wireless Internet Services in Vernal Region (February 15, 2006)
- California Man Indicted for Botnet Attack That Impacted Hospital (February 10, 2006)
- Florida Man Indicted for Causing Damage and Transmitting Threat to Former Employer"s Computer System (February 7, 2006)
- Bot Herder Pleads Guilty to Fraudulent Adware Installs and Selling Zombies to Hackers and Spammers (January 23, 2006)
- Dayton, Ohio, Man Pleads Guilty to Sexual Exploitation Crimes Involving Minors and Computer Intrusion (January 19, 2006)

الفهرس

الـــفـــهـــرس

المقدمة: 1
مشكلة البحث 2
أهمية البحث 3
أهداف البحث 3
منهج البحث 4
الفصل الأول: واقع الانترنت والجريمة المستحدثة
المبحث الاول: الانترنت 7
المطلب الاول: ماهية الانترنت وتطورها 7
أولا: ماهية الانترنت 7
1- المحاولات الفقهية لبيان مفهوم شبكة الانترنت 9
2- المحاولات القضائية لبيان مفهوم شبكة الانترنت 10
ثانيا: التطور التاريخي لشبكة الانترنت 12
المطلب الثاني: فوائد الانترنت وسلبياته 17
أولا: فوائد أو ايجابيات شبكة الانترنت 17
1- سرعة نقل وتمرير المعلومات 18
2- بنوك ومجمعات المعلومات 18
3- الانترنت كحقيبة معلومات شخصية متنقلة مع المستخدم 19
4- تعدد الوسائط في الشبكة العالمية (WWW) 19
5- الانترنت مكتبة لكل شخص 20
6- مجموعات الحوار والمحادثة 20
ثانيا: سلبيات شبكة الانترنت أو الوجه الخطير لشبكة الانترنت 21
1- عدم الرقابة والإباحة 21
2- الإدمان 21
3- العزلة 22

4- الاعتقاد بأن المعلومات على الشاشة دوما صحيحة 22
5- نسخ معلومات واستعمالها كأنها شخصية 22
المطلب الثالث: ماهية المعلومة وطبيعتها القانونية 23
أولا: مفهوم المعلومات 24
1- مفهوم المعلومة لغة.....26
2- مفهوم المعلومات اصطلاحاً.....26
ثانيا: أنواع المعلومات 28
1- الطائفة الأولى: المعلومات الاسمية 28
أ- المعلومات الشخصية 28
ب- المعلومات الموضوعية 29
2- الطائفة الثانية: المعلومات الخاصة بالمصنفات الفكرية 29
3- الطائفة الثالثة: المعلومات المتاحة أو الشاغرة.....30
ثالثا: الشروط الواجب توافرها في المعلومة محل الحماية الجنائية وطبيعتها القانونية 30
1 - الشروط الواجب توافرها 30
الشرط الأول: أن تكون المعلومة محددة ومبتكرة.....30
الشرط الثاني: أن يتوافر في المعلومة السرية أو الاستئثار 31
الشرط الثالث: المعالجة الآلية للمعلومات 33
2- الطبيعة القانونية للمعلومات 33
1) الاتجاه الأول: اتجاه تقليدي: المعلومة لها طبيعة من نوع خاص 33
2) الاتجاه الثاني: اتجاه حديث: المعلومات مجموعة من القيم.....34
المبحث الثاني: الجريمة المعلوماتية و المجرم المعلوماتي 36
المطلب الاول: ماهية الجريمة المعلوماتية وخصائصها 37
أولا: تعريف الجريمة المعلوماتية 37
1- المفهوم الضيق لمفهوم الجريمة المعلوماتية 39
2- المفهوم الموسع لمفهوم الجريمة المعلوماتية 40
ثانيا: خصائص الجريمة المعلوماتية 42

1- الجرائم المعلوماتية جرائم ترتكب بواسطة الحاسب الآلي.....42
2- الجرائم المعلوماتية جرائم ترتكب غبر شبكة الانترنت.....42
3- الجريمة المعلوماتية متعدية الحدود أو جريمة عابرة للدول.....43
4- الجاني في الجرائم المعلوماتية 44
5- صعوبة اكتشاف الجريمة المعلوماتية 44
6- صعوبة إثبات الجريمة المعلوماتية.....45
7- أعراض النخبة 46
8- أسلوب ارتكاب الجريمة المعلوماتية 46
9- خصوصية مجرمي المعلوماتية.....47
10- الجريمة المعلوماتية جريمة مستحدثة.....47
11- قلة الإبلاغ عن وقوع الجريمة المعلوماتية.....48
المطلب الثاني: المجرم المعلوماتي.....49
أولا: السمات الخاصة بالمجرم المعلوماتي 50
1- المجرم المعلوماتي يتمتع بالمهرة والمعرفة والذكاء 51
2- المجرم المعلوماتي إنسان اجتماعي بطبعه "متكيف اجتماعياً".....53
3- المجرم المعلوماتي يبرز ارتكاب جريمته 53
4- خوف المجرم المعلوماتي من كشف جريمته.....54
5- المجرم المعلوماتي مجرم عائد للإجرام 54
6- المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي.....55
ثانيا: فئات مجرمي المعلوماتية.....55
1- الفئة الأولى: فئة الهواة 56
2- الفئة الثانية: فئة المحترفين أو المخترقين 63
أ- فئة المخادعون 64
ب- فئة الجواسيس 64
ثالثا: الأسباب الدافعة لارتكاب الجرائم المعلوماتية.....64
1- تحقيق المكسب المادي 65

2- إثبات الذات والرغبة في قهر النظام المعلوماتي 66
3- الانتقام 67
4- ارتكاب الجرائم كوسيلة للتسلية والدعابة 67
أ- التنافس السياسي والاقتصادي.....68
ب- مناهضة العولمة 68
ج-التسابق القضائي والعسكري بين الدول.....68
المطلب الثالث: تصنيف الجرائم المعلوماتية 69
أولا: تقسيم الجريمة المعلوماتية بسب دور الكمبيوتر فيها 70
1- قد يكون الكمبيوتر هدفا للجريمة.....70
2- قد يكون الكمبيوتر أداة الجريمة لارتكاب جرائم تقليدية.....71
3- قد يكون الكمبيوتر بيئة الجريمة.....72
4- أما من حيث دور الكمبيوتر في اكتشاف الجريمة 72
ثانيا: تقسيم الجرائم المعلوماتية على أساس الجرائم الواقعة على أو باستخدام النظام المعلوماتي 73
1- النوع الأول: الجرائم الموجهة ضد نظم المعلوماتية (جرائم تقع على الأنترنت).....73
أ- سرقة المال المعلوماتي.....74
ب- الدخول على المواقع المحجوبة (باستخدام البروكسي).....74
ج-جرائم الاختراقات.....75
- الاقتحام أو التسلل 75
- الإغراق بالرسائل 75
- الفيروسات.....75
د- المواقع المعادية.....76
- المواقع السياسية المعادية.....76
- المواقع الدينية المعادية.....76
- المواقع المعادية للأشخاص أو الجهات 76
هـ-جرائم القرصنة 76

- جرائم التجسس الإلكتروني 77
و- الإرهاب الإلكتروني 77
2- النوع الثاني: الجرائم المرتكبة باستخدام النظام المعلوماتي 78
أ- الجرائم الجنسية والممارسات الغير أخلاقية 78
- الجرائم غير الجنسية التي تستهدف الأشخاص.....78
- طائفة الجرائم الجنسية 79
ب- الجرائم المالية 80
- جرائم السطو على أرقام البطاقات الإئتمانية 80
- القمار عبر الأنترنت.....81
- تزوير البيانات 82
- الجرائم المنظمة.....82
- تجارة المخدرات عبر الأنترنت.....83
- غسيل الأموال.....83
ج-قيادة الجماعات الإرهابية عن بعد.....84
د- السطو على أموال البنوك 84

الفصل الثاني: الاعتداءات على المعلومات والحماية الموفرة لها

المبحث الأول: الحماية الجنائية للمعلومات و اهميتها.....88
المطلب الاول:ضرورة الحماية الجنائية للمعلومات 88
المطلب الثاني: الحماية الجنائية للمعلومات في النظم المقارنة 90
أولا:حماية المعلومات على المستوى الدولي.....91
1- تشريعات الولايات المتحدة الأمريكية 92
2- تشريعات فرنسا 94
3- القانون الألماني 95
ثانيا:حماية المعلومات على المستوى العربي او الاقليمي.....95
1- البحث حول إمكانية وجود قانون خاص بالأنترنت.....97
2- الجهود الجماعية العربية لتقنين الانترنت.....98

3- الغرض الذي أدى إلى محاولة وضع قانون (قوانين) عربية للأنترنت 100
4- التنظيم القانوني: التجارة الالكترونية، والتعاقد والتوقيع الالكتروني 102
5- المشرع العربي والجرائم الالكترونية 106
6- نماذج من القوانين الداخلية لمكافحة جرائم الانترنت عربيا 107
أ- جرائم نظم ووسائط شبكات المعلومات..... 109
ب- الجرائم الواقعة على الأموال والبيانات والاتصالات بالتهديد والابتزاز..... 109
ج- جرائم النظام العام والآداب العامة..... 109
د- جرائم الإرهاب والملكية الفكرية..... 109
هـ-جرائم الاتجار في الجنس البشري 109
و- الجرائم المتعلقة بأمن الدولة وسلامتها الداخلية والخارجية 109
ي- تشريعات القانون الجزائري..... 114
المبحث الثاني: أشكال الاعتداءات على المعلومة 115
المطلب الاول: الاعتداء على حقوق الملكية الفكرية بطريق الانترنت 115
أولا: محل الحماية الجنائية في الاعتداء على حقوق الملكية الفكرية..... 116
1- مفهوم المصنف..... 117
2- أبوة المؤلف لمصنفه 119
ثانيا: الاعتداء على حقوق المؤلف في التشريع المقارن..... 119
1- على مستوى الدولي 119
2- على مستوى الإقليمي 121
أ- حقوق المؤلف في التشريع المصري 121
ب- حقوق المؤلف في التشريع الفرنسي 125
ج-حقوق المؤلف في القانون الجزائري..... 126
المطلب الثاني: الاعتداء على البيانات الشخصية والخصوصية المعلوماتية بطريق الانترنت 140
أولا:حماية الخصوصية المعلوماتية في القانون المقارن 142
1- حماية الخصوصية المعلوماتية في القانون الجنائي الفرنسي 143
2- حماية الخصوصية المعلوماتية في القانون الجنائي الأمريكي..... 145

ثانيا:الحماية الجنائية للخصوصية المعلوماتية في التشريعات العربية..... 148
- الحماية الجنائية للخصوصية المعلوماتية في التشريع المصري..... 148
المطلب الثالث: الاعتداء على القيمة الاقتصادية و الامنية للمعلومات بطريق الانترنت 151
أولا:مفهوم الوثائق السرية..... 153
ثانيا:مفهوم المعلومات الاقتصادية والتجارية محل الحماية 154
ثالثا: الشروط الواجب توافرها في المعلومات محل الحماية..... 154
رابعا:النظام القانوني لحماية الاسرار التجارية في التشريعات المقارنة 155
المبحث الثالث: الاتجاهات التشريعية المختلفة في مواجهة الجرائم المعلوماتية..... 161
المطلب الأول: المواقف التشريعية بالنسبة للمصالح المحمية بالجريمة المعلوماتية..... 163
أولا: اتجاه يهتم بفكرة الملكية Property Approach 163
ثانيا: اتجاه يركز على حماية سلامة المعلومات والبيانات التي يحتوي عليها نظام الحاسب الآلي..... 163
ثالثا: اتجاه يهتم بالمعلومات في ذاتها وخاصة تلك التي تتصل بالأشخاص..... 164
رابعا: الموقف التشريعي الذي يجمع بين أكثر من اتجاه من الاتجاهات السابقة..... 164
المطلب الثاني: الأساليب والأنماط المختلفة للصياغات التشريعية الخاصة..... 165
أولا: وضع نصوص جديدة قياسا على نصوص تقليدية قائمة بالفعل 165
ثانيا: الإضافة 165
ثالثا: وضع نص رئيسي واحد يستطيع التعامل مع الأوجه المختلفة للجريمة المعلوماتية ... 166
الخاتمة 170
النتائج 170
الاقتراحات 172
المراجع والمصادر 175
الملاحق..... 181