

مخاطر شبكة الانترنت في ظل متطلبات الأمن المعلوماتي وآليات تحقيقه

The risks of the Internet in the light of the requirements of information security and the mechanisms of the achieved

أوهيبة بشريف، جامعة باتنة 01- الجزائر

ملخص: برزت شبكة الانترنت بعد الحرب الباردة في القطاع العسكري الحربي، لكن ما لبثت أن تغزو كل مجالات العلمية والعملية، وبدأ الحديث حول ما تحمله مضامين هذه الشبكة وانعكاسه على المجتمع، فبعد فترة من الزمن، بدأ الجدل بين الباحثين حول تأثير وسيلة الوسائل ألا وهي الانترنت على الأفراد والمجتمع، التي مازالت تشهد تضارب الآراء والاتجاهات حولها، حيث برزت دراسات حول مخاطر هذه الوسيلة، خاصة في ظل ترجيح احتمالات سوء استخدامها من قبل الأفراد والمؤسسات الناشطة، ومن هنا، يتبادر إلينا طرح الإشكالية التالية: ما هي مخاطر شبكة الانترنت في ظل متطلبات الأمن المعلوماتي؟

وتوصلت هذه الورقة البحثية إلى أن الانترنت يشكل العديد من المخاطر سواء على الأفراد أو المؤسسات على حد سواء، من تهديد سرية المعلومات وكذا الإباحية الالكترونية، إضافة إلى تهديد أمن الدول وسيادتها، مما وجب إيجاد منظومة تشريعية و أخلاقية صارمة للحد من هذه التجاوزات و الاستثمار الأمثل لوسيلة الوسائل.

الكلمات المفتاحية: الانترنت، الوقاية، وسيلة الوسائل، الأمن المعلوماتي.

Abstract: The Internet has emerged after the cold war in the military sector in war, but the scaffolding invade all areas of scientific and process, started to talk about what's in the contents of this network and reflect on the society, after a period of time, the controversy between researchers on the impact of the means the means, the Internet on individuals and society, which is still witnessing conflicting views and trends around, as studies on the risks of these means, especially in the light of the reverse their possible misuse by individuals and institutions that are active, and here, the problem comes to us ask the following: What are the risks of the Internet in the light of the requirements of the information security?

Keywords: internet, Internet dangers, prevention, as a means of means of information security.

مقدمة:

تواصلت الجهود في اختراع الوسائل التكنولوجية الحديثة، حيث ظهرت الانترنت بعد نهاية الحرب العالمية الثانية، وبداية الحرب الباردة، هذه الشبكة التي مكنت الفرد أين ما كان، وفي أي وقت، أن يوصل صوته وصورته في آن واحد إلى أبعد مكان، ما ميزها عن أية وسيلة أخرى، حتى أنها أدخلت مصطلحات ومفاهيم خاصة بها، فلم يعد استعمال مصطلح جمهور الانترنت، مستعملا كثيرا، بل ظهر مفهوم "مستخدمي الانترنت" والذي شاع صيته واستخدامه في الدراسات الاتصالية والإعلامية، حيث اشتغل الباحثين والعلماء في مجالات مختلفة، خاصة مجال علوم الإعلام والاتصال، بعدما تباينت آرائهم واختلافاتهم حول تصنيف هذه الوسيلة، فهناك طرف، صنفاها على أنها وسيلة إعلام نتيجة لوجود مؤسسات إعلامية تنشط على هذه الشبكة ومنه تبث الخبر على نطاق واسع للجمهور، في حين الكفة الأخرى مالت إلى اعتبار وسيلة الإنترنت وسيلة اتصال حديثة، حيث مكنت المستخدمين من الاتصال والتواصل مع الآخرين، ونقل الثقافات من مكان إلى آخر، ومنه ألغت هذه الوسيلة الحدود الجغرافية التي أعاققت الاتصال منذ القدم، وجعلت الاتصال يحدث في ثانية فقط، في حين كان هناك طرف آخر، ذهب إلى أن الإنترنت ليست وسيلة اتصال ولا وسيلة إعلامية، بل هي وسيلة الوسائل، كونها شملت كل خاصية من خصائص الوسائل التقليدية، فأخذت خاصية المكتوب من الجريدة الورقية، وخاصية الصوت من الإذاعة المسموعة، وخاصية الرؤية من التلفزيون، وبذلك دمجت القراءة والمسموع والمرئي فيها، ما جعلها وسيلة تستهوي العديد من الأفراد، لينتقل تركيزهم واهتماماتهم على دور وسائل الإعلام والاتصال ومدى تأثيرها على المجتمع، ومنه الانشغال بتأثير مضامين الوسيلة الجديدة ألا وهي الانترنت على الأفراد والمنظمات على حد سواء باعتبارها من الوسائل الأكثر تطورا وعصرنة، إلى البحث والنقاش حول إيجابيات الانترنت ومخاطرها، ومما سبق، يتبادر إلينا طرح الإشكالية التالية:

-ما هي أبرز مخاطر شبكة الانترنت في ظل المجتمع المعلوماتي؟

وتتفرع عن هذه الإشكالية مجموعة من التساؤلات التالية:

-ما المقصود بالإنترنت، الأمن المعلوماتي؟

-ما هي الآليات المنتهجة للحد من مخاطر الإنترنت في ظل المجتمع المعلوماتي؟

وللإجابة على هذه الإشكالية نعتمد على المحاور الآتية:

المحور الأول: المدخل المفاهيمي

المحور الثاني: مخاطر شبكة الانترنت في ظل المجتمع المعلوماتي.

المحور الثالث: الآليات المنتهجة للحد من مخاطر الإنترنت في ظل متطلبات الأمن المعلوماتي.

أولا. مدخل مفاهيمي:

الانترنت: تتلخص الانترنت في كلمة Internet (Michel Grenie, 1997, p126)، كلمة منحوتة من كلمتين Interconnection، وهي بمعنى أكثر من شيين ببعضها البعض، وكلمة شبكة Network فاستعير من الكلمة الأولى الجزء الأول منها هو Inter، ومن الثانية الجزء الأول هو Net فصارت الكلمة هي Internet، وكثير من يعتقد أن الجزء الأول مأخوذ من كلمة

Inter national ويصفها بأنها الشبكة الدولية للمعلومات، حيث أنه عندما أطلق اسم Internet على الإنترنت لم تكن دولية بل كانت شبكة محلية أمريكية. (علي محمد سمو، دس، ص240). وهي أيضا تعتبر " شبكة ضخمة من الحواسيب تربط بين العديد من الأعمال والمعاهد والأفراد في أنحاء العالم، وكلمة إنترنت مأخوذة من اللغة الانجليزية، وهي في الانجليزية اختصار لعبارة تعني شبكة الشبكات المترابطة، حيث يربط الإنترنت بين عشرات الآلاف من الشبكات الحاسوبية الصغيرة، وتبث هذه الشبكات كميات ضخمة من المعلومات في شكل كلمات وصور وأصوات" (الموسوعة العربية العالمية، 1999، ص163).

المجتمع المعلوماتي: ويقصد بالواقع الافتراضي Virtual Reality " كل ما يحاكي الواقع أو يناظره إلى درجة يخيل لنا معها أنه واقع، ويقصد بها كذلك ما يتجاوز هذا الواقع، والواقع الخائلي هو مفهوم آخر من المفاهيم التي أضافتها تكنولوجيا المعلومات إلى قاموس حياتنا، وينظر إليه على أنه بيئة اصطناعية لممارسة الخبرات بصورة أقرب ما تكون إلى تلك الموجودة في الواقع" (مجبل لازم المالكي، دس، ص253-254).

الأمن المعلوماتي: ويقصد به إيجاد آليات وإجراءات لحماية المعلومات والبيانات الموجودة على شبكة الانترنت من عمليات التخريب والسرقة، وكل أشكال الإجرام الممارسة عبر الانترنت، بإتباع استراتيجيات وقائية وعلاجية.

ثانيا. مخاطر الإنترنت في ظل المجتمع المعلوماتي:

المشاكل اللا أخلاقية: تتضمن شبكة الإنترنت حوالي مليون صورة أو رواية خليعة جنسية، كما أن هناك معلومات تعطي لبعض المستخدمين عن عناوين بيوت الدعارة في العديد من مدن العالم، والأثر من ذلك وجود أحاديث هاتفية جنسية تؤديها بعض الفتيات ومدربات المؤسسات المشتركة في الشبكة.

المعلومات التي تشجع العنف والإجرام: هناك بعض التطبيقات التي يعتقد بأنها تساعد على العنف والإجرام، فهناك هجمة صحفية أثرت في ولاية أركنساس الأمريكية حول طفل في العاشرة من عمره كان يحاول صنع قنبلة من خلال المعلومات التي حصل عليها عبر الشبكة فانفجرت عليه وقتلته (ريا أحمد الدباس، 2010، ص277).

تهديد الإنترنت لسيادة المعلومات: لم تكن سيادة الدولة على المعلومات، وبالتحديد قدرتها على منع الغير من خارج حدودها من أن يحصلوا على المعلومات عن قضايا الشأن الداخل، حيث أن انتهاك الإنترنت لسيادة الدولة للمعلومات لا يقارن بوسائل الإعلام التقليدي، حيث أن الإنترنت مكن المواطنين في أي دولة من المقارنة مع أوضاع غيرهم في كافة أرجاء المعمورة، ولم يعد بإمكان أي دولة إخفاء الأسرار عن مواطنيها، كما أن حكومات العالم عاجزة عن احتكار المعلومات وإخفاء الحقائق (إبراهيم حمادة بسيوني، 2008، ص66-67).

الجريمة الالكترونية: وفقا معطيات أحد مكاتب الأبحاث المعنية فإن الشركات الأمريكية أنفقت 6 مليارات دولار لمقاومة هجمات "قراصنة الكمبيوتر" خلال عام 2000، وأن هذا سيتجاوز 20 مليار دولار عام 2004 (محمد فتحي، 2003، ص73).

خلقت الجرائم الالكترونية ما يسمى بـ "الحرب الالكترونية"، حيث تكون المعلوماتية هي الساحة التي يتحارب فيها الأعداء، ومثال على ذلك "حرب الهاكرزية" بين مجموعات عربية ويهودية، التي استمرت عدة أشهر عامي 2000 و2001 حيث قام كل طرف بتعطيل وتخريب مواقع الطرف الأخر، فقد تم في الشهر الأول لهذه المعركة في أكتوبر 2000 بتخريب 40 موقع يهودي مقابل 15 موقع عربي (طارق محمود عباس، 2003، ص47).

حيث نقلت وكالة رويترز بتاريخ 2010، أن شركة المعلومات والبحث العملاقة غوغل قد بدأت حملة داخلية لاستبدال نظام "ويندوز" بعد المخاوف الأمنية الالكترونية (عباس بدران، 2010، ص13).

مشاكل حقوق النشر والتأليف: تعتبر حقوق النشر والطبع للمنتجات الفكرية المختلفة من الأمور المهمة والحساسة للمؤلفين والناشرين التي يترتب عليها أمور قانونية ومالية (ريا أحمد الدباس، 2010، ص277).

حيث أن النشر الإلكتروني يعتمد على التخزين والبث والتقديم الرقمي للمعلومات على أن تنظم المعلومات في شكل وثيقة ذات بناء معين، ويمكن أن تشمل هذه الوثائق معلومات نص أو صور أو رسومات (محمد فتحي عبد الهادي، 2001، ص26).

الفجوة الرقمية (التكنولوجية): استخدام الإنترنت يعتمد على تكنولوجيا عالية الثمن بالنسبة للجنوب، وأحيانا نادرة الوجود بالمقارنة بالدول الصناعية، فحوالي 80% من دول العالم تعاني من نقص شديد في البنية التحتية للاتصالات (أحمد محمد صالح، دس، ص27).

وفي التقرير السنوي لبرنامج الأمم المتحدة الإنمائي UNDP لعام 2001 حول الشراكة من أجل محاربة الفقر الذي قدم معطيات لغاية عام 2000 ترد النسبة كما يلي وبالصيغة التالية: "مستخدمو الإنترنت حسب المنطقة (الإقليم) النسبة المئوية من السكان، في الدول العربية 0,6، وهذا مقارنة بأمريكا 54,3%، ودول منطقة التعاون الاقتصادي والتنمية عالية الدخل (باستثناء الولايات المتحدة) 28,2% (معن النقري، 2003، ص35).

إن الدول العربية قد أحرزت بعض التقدم نسبيا في مجال المعلوماتية، ولديها إمكانيات تطبيق الحكومة الإلكترونية، لكن الأوضاع التي تعرفها تلك البلدان أشارت إلى أن ثمة فجوة كبيرة بينهم وبين بقية دول العالم (راسم محمد جمال، 2006، ص188).

والحكومة الالكترونية حسب تعريف منظمة التعاون والتنمية الاقتصادية (OCDE): "استخدام تكنولوجيا الإعلام والاتصال وبالخصوص الإنترنت، كأداة يهدف وضع حيز التنفيذ إدارة ذات جودة عالية" (زهرة بوراس، بوشارب أحمد، 2014، ص17).

أما منظمة الأمم المتحدة فعرفتها بأنها "هي التحسين المستمر للخدمة المقدمة، المشاركة الدستورية والحكومة المرتبطة بتغيير شكل العلاقات الداخلية والخارجية بالاعتماد على التكنولوجيات، الإنترنت ووسائل الإعلام الجديدة" (زهرة بوراس، أحمد بوشارب، 2014، ص16).

وهناك عدة عوامل مسببة للفجوة التكنولوجية، كعدم اهتمام الدول النامية اهتماما كافيا بالتعليم في مراحلها المختلفة، فما زالت غالبية السكان تجهل القراءة والكتابة، بالإضافة إلى عيوب نظم

التعليم القائمة بالشكل الذي لا يساعد على استيعاب وتطوير التكنولوجيا المستوردة(السيد رشاد غنيم، 2008، ص132).

إن كلمة التكنولوجيا التي "عربت تقنيات من الكلمة اليونانية تكني، وتعني مهارة أو حرفة أو صنعة، والكلمة "الوجيا" وتعني علما أو فنا، وتصير بعض الكتابات إلى أن المقطع الثاني من كلمة تكنولوجيا وهو "Logic" ويعني منطق، وبذلك فإن كلمة تكنولوجيا تعني علم المهارات بشكل منطقي لتأدية وظيفة محددة"(عبد الفتاح أبو معال، 2006، ص243).

ويعتبر "صادق الحمامي" أن من بين الأسباب التي جعلت تأخر البلاد العربية " تلك الرؤية الأخلاقية المفروضة على الشبكة والتي تحدد قيم مسبقة للمستخدم إن اتبعها فهو مستخدم سوي، وإن رفضها فهو مستخدم ضال مائع"(http://arabic. 42: 11, 29-03-2016, pid=44602, Tebyan.net/index.aspx).

هناك خطوات لتقليل حجم الفجوة الرقمية ومن أبرزها مايلي: قيام الحكومات بإنشاء مراكز بحث وتطوير مشاريع رائد للعلوم والتكنولوجيا على مستوى القطاعين العام والخاص، و العمل على تكوين ربط الكتروني بين مؤسسات ودوائر الحكومة المختلفة (G-2-G) وبينها وبين المواطنين وبين الحكومة والأعمال (G-2-B)(محمد سمير أحمد، 2009، ص106-107).

تسيطر اللغة الانجليزية على 89% من المواقع المصرية، حيث قام الباحث " هشام فتحى" في أطروحة الماجستير بتحليل المواقع المصرية المتاحة خلال الشبكة العنكبوتية، حيث اختار الباحث عينة بلغت 625 مفردة من أصل 1545 موقعا مصريا، واحتلت اللغة العربية المركز الثاني بنسبة 9%(محمد فتحى عبد الهادي، 2007، ص87).

جرائم الفضاء الرقمي: هناك العديد من الجرائم التي تحدث في الفضاء الرقمي، نذكر منها: -التدمير والتخريب المعتمد: يحاول مرتكبو التدمير المعتمد غزو أو تدمير أجهزة النظام والبرمجيات أو بياناته ويتراوحون بين المتلاعبين والموظفين المستائنين إلى الجواسيس، على الرغم من بعض المتلاعبين(عثمان قاسم داود اللامي، أميرة سنكرولي البياتي، 2010، ص214).

-التسلسل أو الاختراق في إنترنت (الهاكينغ Hacking): يعتمد الكثير من مستخدمي إنترنت من تسلسل أو اختراق أجهزة أشخاص أو مؤسسات دون استئذان، فيبدأ بعضهم على سبيل التجربة والفضول، وعندما يتمكن، يعجبه الأمر وينساق فيه إلى حين بعيد، فيدخل أجهزة مستخدمي إنترنت لا يعرفهم شخصيا ولا يعرف حتى مكان تواجدهم لسرقة أسرارهم والاستيلاء على ملفاتهم الخاص(فضيل دليو، 2002، ص20).

إن القرصنة عبر الإنترنت تتم بالمحاولة الحصول على معلومات مخزنة في ذاكرة الكمبيوتر دون وجه حق، قصد الاستعمال المباشر أو غير المباشر، وهي تعتبر من أكثر الجرائم المعلوماتية انتشارا وتنوعا، مما أدى إلى نشوء عدد كبير من المنظمات المتخصصة في محاربة المحاكاة (Counterfeit)، وتقدر بعض مصادر منظمة اتحاد صناعة البرمجيات والمعلومات (S.I.I.A) خسائر هذا النوع من القرصنة في سنة 1998 فقط حوالي 11 مليار دولار في مجال

البرمجيات، بغض النظر عن قرصنة الموسيقى والإنتاج الأدبي والعلمي(فضيل دليو، 2002، ص13-14).

أشار استبيان الجرائم وأمن الكمبيوتر التي كلف بإجرائها مكتب التحقيقات الفيدرالية (أف بي أي) أن "مؤسسات الأعمال الأمريكية تتكبد خسائر مالية متزايدة نتيجة لمخالفات وجنبايات أمن المعلومات، ونشرت النتائج في بيان صحفي أصدرته مؤسسة أمن الكمبيوتر أو Computer security Institute وهي جمعية من مهني الأمن المعلوماتي ومقرها كاليفورنيا.

واشترك في الاستطلاع أكثر من 500 مسؤول من أمن المعلومات أو أجهزة كمبيوتر من شريحة عريضة من مؤسسات الأعمال، وهذا الاستطلاع هو سادس استطلاع سنوي من تجربة المؤسسة، واجري في عام 2000، وأفادت نسبة 85% من المستطلعة آرائهم أن مؤسستهم تعرضت لأحد أنواع المخالفات الأمنية، ونسبة 35% (186 من المجيبين على توفير بيانات على خسائر بقيمة 378 مليون دولار)(يوسف حسن يوسف، 2011، ص221-222).

وهناك العدد من البرمجيات المستخدمة في التدمير والتخريب، أهمها: الباب المسحور: تعد مجموعة التعليمات التي تسمح للمستخدم بتجنب إجراءات الأمن القياسية لنظام الحاسوب، بعضها المبرمجون لتسهيل تعديل البرمجيات وقد تستغل إحدى الأبواب المسحورة التي تركها المبرمجون في تعطيل 6000 جهاز حاسوب.

حصان طروادة: برنامج يحتوي على تعليمات مخفية يمكن أن تسبب الضرر فمثلا يمكن أن يحدد حصان طروادة رقم معين ويهمله أو يجمع الاختلافات التي تؤدي إلى التدمير ويضعها في حساب معين.

القتيلة المنطقية: تعد نوعا من حصان طروادة يقوم بتنظيم أعمالها التدميرية لكي تظهر حيث يظهر طرف معين كبداء برنامج معين، وتستخدم عادة في الانتقام والتخريب، كما حدث في عام 1988 في إحدى قضايا المحكمة الفيدرالية بقيام أحد المبرمجين العاملين في شركة Omega Engineering في Bridgeport Jersey بابتكار قنبلة منطقية، انفجرت بعد 20 يوما حاذفة لكل البرمجيات الإنتاج والتصميم للشركة ومعطلة تسهيلات لها لدعم والتجديد وقدر الضرر الكلي بـ 10 مليون دولار بسبب طرده منها بدافع الانتقام(عثمان قاسم داود اللامي، 2010، ص214-215).

الفيروسات: البرامج و الدودية وأحصنة طروادة، عبارة عن "برامج ضارة تسبب الضرر للحواسيب وللمعلومات الموجودة فيه أو قد تسبب إبطاء سرعة الإنترنت".

وكان أول ظهور عام 1983 حيث تقشى فيروس في برنامج Xun، ويرى "العبيدي" أن أول مكتشف للفيروس يعد أحد المبرمجين، الذي قام بحماية معلومات حاسوبه من عمليات النسخ والتقليد والتكبير يقوم بتخريب النسخ المقلدة عن برنامجه أو معلوماته(عثمان قاسم داود اللامي، 2010، ص216-217).

فحسب خبير اسباني في محاربة الفيروسات يوجد حاليا في عالم الإنترنت حوالي 45 ألف فيروسا معلوماتيا، وقد قدر عدد الفيروسات النشطة شهريا ما بين 600 و800 فيروسا، ومن

أشهرها: مليسا، تشرنوبيل، وفيروس الحب، لقد تسبب هذا الفيروس ذو الاسم المغربي (I love you)، والذي بلغ ذروته انتشاره من خلال البريد الإلكتروني(فضيل دليو، 2002، ص20). ويعتبر "مل" المراهق الكندي (الذي اشتهر باسم Mafiaboy خير مثال على ذلك، فقد استطاع في فبراير 2000 أن يتسلل إلى عمل المئات من مواقع الويب، وتسبب بذلك في خسارة ملايين الدولارات لشركات مثل Yahoo. Cnn. Buy. Com ولقد تم اكتشافه من طرف الشرطة الفيدرالية الأمريكية (FBI) التي قدمته للمحاكمة في ماي 2000، وتسبب في خسارة تسعة مليار فرنك، كما ذهبت ضحيته في أمريكا حوالي 95 بالمائة من الشركات، والتي قدرت مؤخرا خسارتها بـ 56 مليار دولار(فضيل دليو، 2002، ص21).

انتحال الشخصية Impersonation: يحدث خطر انتحال الشخصية عن طريق قيام المهاجم بسرقة مفتاح التشفير السري، أو اقتناص الاسم وكلمة السر، خلال مرورهما بالشبكة أو بالتسجيل بعض الرسائل المارة بالشبكة، وإعادة إرسالها في وقت لاحق Replay"(حسن طاهر داود، 2004، ص102).

الطعن والقدف عبر الإنترنت(بهاء شاهين، 1999، ص73):

التجسس: حيث يتم التجسس على الموظفين فقد جاء في مسح ميداني أجرته حديثا الجمعية الأمريكية لإدارة أن نسبة 63% من أرباب العمل، يمارسون نوع من الرقابة أو التجسس على موظفيهم وتشمل هذه الممارسات تحري ملفات الكمبيوترية، وسجلات ترددهم على شبكة الإنترنت(أحمد نافع المداححة، محمد عبد الدبس، 2012، ص191).

الإباحية الإلكترونية: ففي بريطانيا اكتشفت الشرطة بمحض الصدفة منزلا بمدينة "سانت ليونارد" يدار لأعمال منافية للأداب في أكتوبر 1997، وقد ألقت الشرطة القبض على ستة عشر رجلا بتهمة إنتاج وتبادل الصور الإباحية الخاصة بالأطفال، وكان جهاز الكمبيوتر يحتوي على آلاف الصور الخليعة، والتي يصعب الوصول إليها دون معرفة كلمة السر Pass Word(شريف درويش اللبان، 2005، ص130).

المساعدة على الانتحار: وفرت شبكة الإنترنت خدمة خاصة للانتحار، لتسهيل عملية قتل النفس لكل من يرغب في ذلك، نظر دفع المقابل المادي لذلك، وقد ساعدت هذه الخدمة امرأة واحدة على الأقل في الإقدام على الانتحار، كما أرسلت طرود بريدية من أقراص "سيانيد البوتاسيوم" القاتلة لسبعة أشخاص طلبوها عن طريق الإنترنت.

واكتشفت الشرطة اليابانية هذا الموقع في 15-12-1998، وقد تبين أن الشخص الذي يديره صيدلي يمتلك ترخيص بمزاولة المهنة، وكانت الشرطة تبحث عن شخص طلب كبسولات "سيانيد البوتاسيوم" عن طريق الموقع، الذي كتب فيه باللغة اليابانية أنه مخصص للأشخاص الذين لا يعرفون طريقة الحصول على العقار الصحيح للانتحار، ويعرض الموقع الكبسولة الواحدة بمبلغ يتراوح بين 258 و 430 دولار(شريف درويش اللبان، 2005، ص131).

تجارة البويضات البشرية: لقد ساهمت شبكة الإنترنت في "تسويق المنتجات وترويج لها، عن طريق التجارة الإلكترونية، إلا أن الأمر تعدى تلك التجارة إلى تجارة غير شرعية عرفت بـ "تجارة بويضات البشرية"، التي ظهرت في بعض الأوساط الطبية في الغرب، وأثارت جدل

حول هذا النوع من التجارة، والتي بدأت تنتشر على نطاق واسع من خلال شبكة الإنترنت، وقد كشفت إحدى الدراسات الجامعية أن هذه التجارة أخذت بالتوسع، نتيجة النمو الذي حدث في عيادات الخصوبة المنتشرة هناك، والتي يتعامل معها الأزواج الذين لم ينجبوا أطفالاً بالطرق العادية، لقد أصبح بعض الطالبات في بعض جامعات العالم الكبرى والتي تتمتع بسمعة طيبة في التعليم، هدفاً للراغبين في شراء بويضات وتطلب بعض الإعلانات المنتشرة في المجالات العلمية، بويضات فتيات يتمتعن بعيون زرقاء، وبشرة بيضاء وصحة جيدة، ولا يتعاطين المخدرات، وذلك من أجل ولادة أطفال أصحاء" (أحمد نافع المداحه، محمد عبد الدبس، 2012، ص 190)

الجرائم المالية:

-السطو على أرقام البطاقات الائتمانية(منير الجنيهي، ممدوح الجنيهي، 2006، ص239).
-القمار عبر الإنترنت.
-تجارة المخدرات عبر الإنترنت.

تهريب أموال عصابات المخدرات: تستخدم شبكة الإنترنت كأداة لتهريب الأموال المجمعة من تجارة المخدرات، والتي يطلق عليها اسم الأموال القذرة، ويشير تقرير أعدته منظمة الأمم المتحدة وصندوق الدولي أن (28,5) مليار دولار من الأموال القذرة تهرب سنوياً إلكترونياً عبر شبكة الإنترنت لتخترق وتورط (67) دولة من بينها أمريكا وبعض الأقطار العربية والإسلامية، وقد تعرضت هذه الدول إلى انتقادات حادة من قبل الهيئة الدولية لمكافحة الجرائم الاقتصادية.(خالد عبده الصرايرة، 2007، ص98).

ونشأ مصطلح غسيل الأموال عام 1931، لدى محاكمة رئيس عصابة المافيا "ألفونس كابوني" الشهير باسم "الكابوني" عندما حاولت عصابة إبراز المصدر القانوني لأموال الطائفة المحصلة بطريقة غير قانونية (ابتزاز، سرقة، دعارة، قمار، مخدرات)(فضيل دليو، 2002، ص22).
أوضح تقرير أعدته الأمم المتحدة وصندوق النقد الدولي إلى أن 28.5 مليار دولار من الأموال القذرة تطير سنوياً عبر الإنترنت لتخترق حدود بعض الدول في أنحاء مختلفة من العالم لغسلها(أحمد نافع المداحه، محمد عبد الدبس، 2012، ص190).

إن غسل الأموال Money laundering أو ما يعرف بالغسل الإلكتروني للأموال Electronic money، وما أثر على القوانين السرية للحسابات في هذا الصدد، قامت بعض البنوك بفتح مواقع لها على الإنترنت ومارست غسيل الأموال، إلا أنها تم اكتشافها بعد ذلك، فحسب تقرير المكتب الأمريكي لتقويم التكنولوجيا أنه بين 1% من التحويلات تنطوي على غسيل أموال، وتبعا لهذا يقدر أن أكثر من 300 مليون دولار يتم غسلها سنوياً(السيد أحمد عبد الخالق، 2008، ص178).

جريمة الإرهاب الإلكتروني: إنه "العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان دينه أو نفسه أو عرضه، أو عقله، أو ماله بغير حق بشتى صنوفه وصور الإفساد في الأرض، وبالتالي فلكي ننتع شخصاً ما بأنه إرهابياً على الإنترنت، وليس فقط مخترقاً، فلا بد وأن تؤدي الهجمات التي

يشنّها إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل تحدث أذى كافياً من أجل نشر الخوف والرعب" (<http://diae.net/16243.04-01-2016.15:00> h). كان أول استخدام لكلمة الإرهاب الإلكتروني في فترة الثمانينات في دراسة "Barrycollin" التي خلص فيها إلى صعوبة تعريف ظاهرة الإرهاب التكنولوجي بدقة. (صابرو شعبي، 2015، ص108-109).

وهناك من يرى أن الإرهاب الإلكتروني هو إرهاب معلوماتي Cyberterrorism، حيث ذهب مركز حماية البنية التحتية الوطنية الأمريكية NIPC إلى عدّ الإرهاب المعلوماتي عبارة عن "فعل إجرامي يمارس بواسطة الحاسوب، أو أدواته، فيفضي إلى نشر العنف، والموت، مع إثارة الهلع" (حسن مظفر الرزوي، 2007، ص214).

إن جرائم الفضاء الرقمي خلقت ما عرف بـ "أعداء الإنترنت"، الذين تم تصنيفهم إلى: -المتطفلون: (الهواة) Hackers فالمتطفل هو الشخص الذي يشعر بالفخر لمعرفته بأساليب عمل النظام أو الشبكات، بحيث يسعى للدخول عليها بدون تصريح وهؤلاء الأشخاص عادة لا يتسببون بأي أضرار مادية.

-المخربون (المحترفون) Carckers هو الشخص الذي يحاول الدخول إلى أنظمة الكمبيوتر دون تصريح وهؤلاء الأشخاص عادة ما يتسببون في أضرار مادية بعكس المتطفلين.

-الفيروسات: هو برنامج يكرر نفسه على نظام الحاسوب عن طريق دمج نفسه في البرامج الأخرى، وتأتي الفيروسات في أشكال وأحجام مختلفة (ربحي مصطفى عليان 2015، ص279-280).

-المخادعون: "وهؤلاء يتمتعون بقدرات فنية عالية، باعتبارهم عادة من الأخصائيين في نظم المعلومات، ومن أصحاب الكفاءات، وتتصب معظم جرائمهم على شبكات تحويل الأموال، ويمكنهم التلاعب بحسابات البنوك أو فواتير الكهرباء والتليفون أو تزوير بطاقات الإئتمان، وهذه الفئة من المجرمين لها موهبة خاصة في الاستحواذ على ثقة الناس".

-لصوص نظم المعلومات: هم "أشخاص يقتحمون نظم المعلومات، بالتعدي المادي عليها، وعلى البرامج المتحكمة في تشغيلها، للحصول على خدمات أو أهداف غير مشروعة" (ربيعة قندوشي، 2012، ص107-108).

-الأوساط المهنية: الوسطاء مجموعة من الأشخاص ينحصر دورهم في تمكين المستخدم من الدخول على الشبكة والاطلاع على ما يريد، ولذلك فمنهم من ينقل الخدمة ومنهم من يمكن المستخدم من الوصول إلى المواقع، ومنهم من يخزن المعلومات أو ينتجها، وينشط في مجال الوساطة العديد من الأطراف مثل:

-متعهد الوصول: شخص طبيعي أو معنوي يقوم بدور فني لتوصيل المستخدم إلى شبكة، وذلك بمقتضى عقود اشتراك تضمن توصيل العميل إلى مواقع التي يريدها.

-متعهد الإيواء: شخص طبيعي أو معنوي، قد يكون شركة تجارية أو أحد أشخاص قانون العام، مثل الجامعات والمؤسسات العامة يعرض إيواء صفحات الويب على حساباته الخاصة (ربيعة قندوشي، 2012، ص108-109).

ويتسبب الإنترنت أيضا في وصول مستخدمين آخرين غير مرغوب فيهم إلى المعطيات والملفات الموجودة على الشبكات المحلية، وهي مشكلة تعيق انتشار الإنترنت، لأن الخوف من تجسس المشتركين في الإنترنت، ومن التخريب، وسرقة الهوية الذاتية وفقدان سرية المراسلات، كل ذلك أدى إلى الحذر من الاقتراب من الخدمات المباشرة التجارية(عبد الحافظ محمد سلامة، وائل أبو مغلي، 2002، ص78-79).

ويقول بعض المحللين أن كثيرا من القرصنة " يتسابقون في نشر البرامج المقرصنة عبر مواقع الدردشة بواسطة لوحة مفاتيح الحواسيب، للتباهي فقط بقدراتهم في سرعة كسر نظام حماية النسخ، ويقدم البعض الآخر هذه البرامج كخدمة مجانية بحجة أن تكاليفها، خاصة أن طلاب المدارس والجامعات ومستخدمي الدول الفقيرة، يشكلون الغالبية العظمى من مستخدمي البرامج المقرصنة في العالم"(فضيل دليو، وآخرون، 2002، ص14-15).

رأى " حسين عبد الجبار " أن للإنترنت أضرار كثيرة ومتنوعة، جملها في: الأضرار العقيدية، الأضرار الأخلاقية: مثل المواقع الإباحية، الأضرار الاجتماعية: مواقع المخدرات، الأضرار الاقتصادية: مثل غسيل الأموال(حسين عبد الجبار، 2008، ص87-88).

إدمان الإنترنت: في مسح أجري في أواخر عام 1995 تم تقدير 9,5 مليون مستخدم للإنترنت في الولايات المتحدة فقط، يقضون في المتوسط 6,6 ساعة أسبوعيا على الإنترنت، وقد وردت التقارير عن حالات إدمان الإنترنت Internet addiction حيث يقضي بعض مستخدم الشبكة 18 ساعة يوميا في الاتصال المباشر معها، لينفقوا بذلك مئات الدولارات في مقابل فواتير التليفونات الشهرية(شريف درويش اللبان، 2005، ص40-42).

غياب التشريعات القانونية: مع التوسع في " صناعات تكنولوجيا المعلومات وانتشار تطبيقاتها في المجالات المختلفة وتبادل المعلومات عبر الحدود، ظهرت الحاجة إلى وضع العديد من التنظيمات والتشريعات واللوائح التوحيد القياسي، ومن أهم الجوانب التي يجب تغطيتها تشريعا هي تلك المتعلقة بالملكية الفكرية وحماية الأسرار الصناعية والتجارية"(السعيد مبروك إبراهيم، 2014، ص95-96).

وقد أدى غياب القوانين التي تنظم العمل الإعلامي في البيئة الالكترونية، والاهتمام بضبط وتقنين الجوانب التقنية والفنية لهذه البيئة، أكثر من الاهتمام بالتنظير لحقوق المهنية، وقبة عدد العاملين في بعض المواقع، وقلة القيود المفروضة على العمل الإعلامي، إلى عدم إمكانية تحديد صبغة طبيعة الحقوق التي يتمتع بها الإعلاميون في هذه بيئة، وتراجع الاهتمام بصياغة تشريعات ومواثيق تنص على حقوقهم، كما أدى غياب الجمعيات والاتحادات التي تهتم بسن التشريعات ومواثيق تنص على حقوق الإعلاميين في البيئة الالكترونية(السيد بخيث، 2011، ص122).

ففي الصين التي يتجاوز معدل القرصنة فيها نسبة 95 بالمائة، ويحصل على أحدث الألعاب أو أنظمة التشغيل وعلى غرار الصين تتغاضى معظم دول العالم المستهلكة للبرمجيات عن قرصنة البرمجيات وتعرض عن سن القوانين المضادة لهم، بل يوجد منها من ذهب إلى ما هو أبعد من ذلك بنسبة لقوانين تبيح قرصنة البرمجيات، مثل الأرجنتين، لأنها تعتبر العكس وتصب في مصلحة الدول المنتجة للبرمجيات وعلى رأسها أمريكا(فضيل دليو، وآخرون، 2002، ص17).

إن شبكة الإنترنت تقلل من مشاهدة التلفزيون قراءة الصحف لدى الشباب، حيث أشارت الدراسة التي أجرتها الدكتورة " نجوى عبد السلام" على أن هناك علاقة معنوية بين مستوى التعليم واستخدام الإنترنت بدافع التسلية والترفيه، فكلما زاد المستوى التعليمي قل استخدام الإنترنت لتسلية والترفيه، وأن هناك علاقة مؤكدة بين مستوى التعليم واستخدام الإنترنت بدافع تكوين الصداقات، فكلما زاد المستوى التعليمي قل استخدام الإنترنت في تكوين الصداقات(خالد عبده الصرايرة، 2007، ص96).

المواد غير الملائمة للصغار UnsuitableMaterial for Minors: يوجد مستوى عال من الاهتمام فيما يتعلق " بالمواد التي تشمل على موضوعات تتعلق بالجنس، بينما ينصب الاهتمام في حالات أخرى على أمور تتصل بالعنف والإرهاب وتعاطي المخدرات، التي تعتبر من الآراء عن مدى ملائمة مواد معينة للأطفال والشباب، وعلى الأخص عندما يتعلق فحوى المواد المعروضة على موضوعات الجنس والعري"(محمد محمد الهادي، 2001، ص235).

ثالثاً. الآليات المنتهجة للحد من مخاطر الإنترنت في ظل متطلبات الأمن المعلوماتي:

إن ظهور الجرائم عبر الإنترنت خلقت ضرورة لما يسمى بـ " الأمن المعلوماتي"، حيث يعد الهاجس الأمني من أهم العوائق والتحديات في وجه تطبيق الحكومة الالكترونية، من هنا يجب ألا يغيب عن فكر القائمين على المشروع موضوع الأمن في كافة مراحل المشروع، خاصة في مراحل التصميم والتطبيق، ويتطلب توافر أمن المعلومات الأمور التالية:

-ضرورة تعيين مسئول مختص في مجال أمن وسرية المعلومات، يهتم بتقديم المعلومات الأمنية لكافة مراحل المشروع.

-تقترح ضرورة إجراء تقييم مستمر للتطبيقات للتأكد من توفر أعلى درجات الاحتياطات الأمنية.
-ضرورة الاهتمام بكافة أنواع الأمن المعلوماتي المادي والمنطقي وتطبيق كافة الخطوات الضرورية في كل المراحل.

-ضرورة تنفيذ الندوات والدورات التدريبية المستمرة لكافة العاملين، وذلك لإبقاء معلوماتهم حول المخاطر الأمنية حديثة.

-ضرورة عمل خطط للطوارئ واختبار تلك الخطط في الظروف الاعتيادية(خالد ممدوح إبراهيم، 2008، ص382-383).

وتستدعي الحكومة الالكترونية وجود إدارة الكترونية تسيّر لها أمورها ونشاطاتها، حيث أن الإدارة الالكترونية يقصد بها "البيئة التي تحقق فيها خدمات المواطنين واستعلاماتهم وتحقق فيها الأنشطة الحكومية للدائرة المعنية من دوائر الحكومة ذاتها، أو فيما بين الدوائر المختلفة باستخدام شبكات المعلومات والاتصال عن بعد"(نادية سلامي، 2015، ص186).

ضرورة إيجاد منظومة تشريعية للممارسة الإستخداماتية للإنترنت: سعت الكثير من الدول المتقدمة إلى إصدار تشريعات بهدف حماية المستجدات المعلوماتية المعاصرة، ومن أهم هذه القوانين:

-قيام الولايات المتحدة الأمريكية عام 1993 بإصدار قانون يقض بالسيطرة على حقوق النشر في المجال الإلكتروني، وإعطاء الحماية القانونية لهذه الأعمال، وضمنت قوانينهم قانون حق النشر،

وشجعت الحقوق الإبداعية في المجال التقني، حيث يمكن الحصول على حق النشر بشكل آلي وبمجرد أن يصبح العمل مثبت بشكل مادي، وبذلك لا يمكن لأي أحد أن ينسخ أو يوزع أو يعرض العمل دون السماح المالك بذلك (السعيد مبروك إبراهيم، 2014، ص96).

ولا بد من الإشارة إلى نقطة قانونية هامة ألا وهي أنه برغم حرية الكلام المطلق التي كفلها الدستور والتي لا يجوز بموجبها لأية سلطة حكومية تقييد هذه الحرية، إلا أنه قد يكون هناك قيد على هذه الحرية فحالة اتفاق الأطراف المعنيين على ذلك، وإذا نشر هذه الأكاذيب بالقول والكلام فإن ذلك قدفا ونشر الأكاذيب الملققة كتابة في مجال الأعمال يسمى قانونا " التشهير التجاري" وإذا نجم عن هذا التشهير الإضرار بمصالح الشخص المشهر به وبأعماله، فقد يتعرض للمحاكمة ودفع تعويض عن الإضرار المادية والأدبية التي تكون قد لحقت بالطرف المشهر به (بهاء شاهين 1999، ص62-64).

إن المواد القانونية تختلف من دولة إلى أخرى، حيث أن " بعض المواد قد تكون غير قانونية في إحدى الدول قد تحمل وتخزن على الإنترنت، ويمكن الوصول إليها في دول أخرى، تكون فيها هذه المواد قانونية، وحتى لو وجد اتفاق في التشريعات ببعض المواد الخاصة " بأدب الأطفال الإباحي" Pornography مثلا، إلا أن القوانين المتعددة التي ترتبط بهذا الموضوع قد تختلف جوهريا، مما يجعل إقامة الدعاوي أو القضايا أو حتى التعاون الدولي في هذا الموضوع صعبا للغاية" (محمد محمد الهادي، 2001، ص234).

أما الدول صاحبة المصلحة المادية في محاربة قرصنة البرمجيات، ممثلة في " الدول الثمانية الأكثر تصنعا، فقد قررت توحيد جهودها الدفاعية لحماية اقتصادها، مدرجة (قضية محاربة قرصنة البرمجيات) ضمن خطة شاملة لمحاربة سلبيات إنترنت، قد انعقدت من أجلها قمة طارئة في منتصف ماي 2000، ولن تختم دون ذكر نوع البيانات التي يتم تبادلها في إنترنت بشكل غير قانوني، إنها لا تنحصر في برامج الحواسيب الشخصية المختلفة، بل تنوعت السلع التي يتبادلها رواد السوق السوداء، لتشمل كلا من الملفات الموسيقية وأفلام الفيديو، وأصبحوا أخيرا يقومون بترويج محاكيات (emulators) للأنظمة الحاسوبية المختلفة، وقرصنة برامج هذه الأنظمة، مثل محاكيات أنظمة (Sega Nintendo Play station neogeo) للألعاب وتحويل ألعابها، التي يباع معظمها على شكل "كارتريج" إلى صيغة رقمية وترويجها في إنترنت" (فضيل دليو، وآخرون، 2002، ص18).

تحقيق أمن النشر الإلكتروني: ويمكن حفظ حقوق المؤلفين الفكرية عن طريق تقنية تعرف إدارة الحقوق الرقمية RightManagement Digital، وهي تقنية تهدف إلى تمكين الناشرين من النشر المأمّن للممتلكات الفكرية كالكتب بشكل رقمي عبر شبكة الانترنت أو عبر أي وسيط الكتروني كالأقراص المكتنزة ووسائط التخزين Removablemedia (أحمد نافع المدادحة، 2011، ص42).

وتمكن هذه التقنية من تشفير Encryption المواد الرقمية digital Materials المراد نشرها والتحكم بالنفاذ إلى المواد الرقمية عن طريق السماح للزبائن بالنفاذ إلى هذه المواد بعد دفعهم لتكاليف معينة (أحمد نافع المدادحة، 2011، ص43).

الوقاية من الاعتداء على المعلومات: هناك خمس أنواع أساسية لخدمات الأمن تستهدف حماية ميدان معلومات، وهي:

خدمات (وسائل) حماية التعريف Identification and Authentication: هذه الخدمات "تهدف التثبيت من الهوية إلى تحديدا عندما يقوم شخص ما بالتعريف عن نفسه، فإن هذه الخدمات تهدف إلى التثبيت من أنه هو الشخص نفسه، وبهذا فإن التعريف يعد الوسائل التي تحمي من أنشطة التخفي والتتكر(أحمد نافع المدادحة، 2011، ص163-164).

وسائل السرية Data and message confidentiality: هذه خدمات "تحمي من الإفشاء للجهات غير المصرح لها الحصول عليها، والسرية تعني بشكل عام إخفاء المعلومات من خلال تشفيرها على سبيل المثال أو من خلال وسائل أخرى كمنع التعرف على حجمها، أو الجهة المرسله إليها".

خدمات حماية التكاملية وسلامة المحتوى Data and message Integrity: تهدف إلى "حماية مخاطر تغيير البيانات خلال عمليات إدخالها أو معالجتها أو نقلها، وعملية التغيير تعني بمفهوم الأمن هنا الإلغاء أو التحرير أو إعادة تسجيل جزء منها أو غير ذلك، وتهدف هذه الوسائل أيضا إلى حماية أنشطة تدمير المعطيات بشكل كامل أو إلغائها دون تحويل".

خدمات منع الإنكار Non repudiation: وهذه الخدمات تهدف منع الجهة التي قامت بالتصرف من إنكار حصول نقل البيانات أو النشاط من قبلها.(أحمد نافع المدادحة، 2011، ص164-165).

كذلك لابد من القيام بمجموعة من الأمور للتحقيق الأمن المعلوماتي، من بينها:
-ضرورة بث الوعي الاجتماعي، فإنه الوقود الفاعل لنجاح الإشاعة، قلة الوعي الاجتماعي، وفقدان بعد النظر للخبر، ومنه لابد من نوعية الأسرة بأهمية التربية الدينية للأبناء، فالتربية الدينية ترسخ في الإنسان مبادئه الأخلاقية وعقائده الإسلامية.

-توعية الشباب بالجانب السلبي لاستخدام الرسائل الاتصالي (الهاتف، الإنترنت) عن طريق وسائل الإعلام المختلفة(رحيمة الحبيب عيساني، 2015، ص173).

كما أن هناك العديد من البروتوكولات التي تستخدم وتطبق في شبكة الإنترنت من أجل ضمان حماية المعلومات وسريتها، وتحقيق أمن الإنترنت، نذكر منها:

بروتوكول S-HTTP: هو نسخة أمنية من بروتوكول HTTP ويستخدم للاتصال مع مواقع الويب.

يعمل بروتوكول بين طبقة TCP-IP وبروتوكول HTTP، فعندما يطلب بروتوكول HTTP إرسال المعلومات إلى مخدم آخر، يقوم بإرسال الطلب إلى بروتوكول S-HTTP ليتحقق أمن المعلومات مشفرة وصحيحة قبل إرسالها إلى بروتوكول TCP/IP ليقوم بنقلها.

بروتوكول SSL (طبقة الداخل الأمانة): تستخدم المتصفحات " بروتوكول SSL أو Secure Socket Layer لتشفير المعلومات التي تنتقل من المتصفح ومخدم الويب، حيث يتم استخدام بروتوكول SSL في عمليات التسوق الإلكتروني، وتبادل المعلومات الحساسة، فعندما يظهر مفتاح أو قفل في أسفل شاشة المتصفح، فهذا يدل على أن المتصفح قد أقام اتصال مشفر وامن مع

المخدم، وأنه بالإمكان الآن إرسال المعطيات الحساسة بأمان" (ناصر خليل، 2008، ص222-223).

بروتوكول العقود الإلكترونية الأمانة SET: هو " اختصار لـ Secure Electronic Transactions وهو بروتوكول يضمن أمن العقود الإلكترونية والصفقات التجارية على الإنترنت، تم تطوير هذا بروتوكول بدعم من شركات Master card و Netcape Visa و IBM، ويستخدم بروتوكول SET نظام الأقفال والمفاتيح، بالإضافة إلى رقم حساب معتمد لكل من الزبون و الشركة، التي تزاو أعمال التجارة الإلكترونية".

يقوم بروتوكول العقود الإلكترونية الأمانة " بتشفير المعلومات المتبادلة على الإنترنت بين الزبون والشركة بطريقة سرية، ويوفر سهولة في إجراءات الدفع، وسرية العقود، والأهم من ذلك يضمن أمن عملية الدفع بكاملها" (ناصر خليل، 2008، ص224-225).

اكتشاف التطفل وسوء الاستخدام: في حين " يهدف التحكم بالدخول والترشيح لمنع الأنشطة غير المصرح بها، والأنشطة الضارة بالمعلومات، نجد أن اكتشاف التطفل وسوء الاستخدام يهدف لاكتشاف النشاط الضار في بدايته" (ذياب البدانية، 2002، ص390).

ويؤكد خبراء التقنية والمعلوماتية على أن الانترنت هو "عالم من الآثار الخفية، وفي مسح أجرى عام 1999 في مركز معلومات الخصوصية الإلكترونية (EPIC) وهي منظمة غير حكومية، ورد أن أكثر من أربع مائة موقع هم أكثر شعبية ورواجا على الانترنت، تحبذ مخبرين مسربين وقطاع طرق إلكترونيين للحصول على صور وتفاصيل كاملة عن مستخدمي الشبكة، كما يجري في محيط الشبكة العديد من عمليات السطو والقرصنة الإلكترونية، إذ يستخدم المحتالون وسائل الكترونية مختلفة" (مجد الهاشمي، 2004، ص257).

كما يمكن أن نقوم بإجراءات أخرى لحماية المعلومات على الشبكة، تمكن من تحقيق الأمن المعلوماتي، وتتمثل تلك الإجراءات في:

-المسؤولية الفردية والعمل الفردي: إذ لابد من نشر الوعي بأهمية حماية المعلومات الخاصة بالفرد، فقد يحتاج المبتدئون باستخدام الحاسب الآلي، أو الذين لا يعرفون قضايا الخصوصية، إلى تنمية هذا الوعي بالتعلم (مؤيد أحمد عبد الرحمن، 2014، ص33-34).

-المسؤولية الرسمية الحكومية: لابد من التدخل الرسمي لحماية خصوصية المعلومات، بالقدر الذي يكفل الحماية التامة لمعلومات الآخرين (مؤيد أحمد عبد الرحمن، 2014، ص35).

ضرورة إيجاد قواعد لتعامل الأخلاقي مع الإنترنت: حيث لابد من العمل على إيجاد وتنشئة المواطن الإنترنتي الصالح (Good netizen، Good Internet citizen)، حيث قدمت إحدى جمعيات أخلاقيات الحاسوب Youshalluseacomputer to harmother people عشر وصايا في التعامل الأخلاقي مع الشبكة، وجاءت الوصية الأولى في التحذير من استخدام الإنترنت من أجل إلحاق الأذى بالآخرين، وهي كالتالي: " لا تستخدم حاسبك في إيذاء الآخرين، وتسوق هنا نموذج في استخدام الحاسوب في إيذاء الآخرين، ولقد استخدم أحد الطلاب في إحدى الجامعات الغربية، البريد الإلكتروني في جامعته ووجه عليه قنبلة إلكترونية، نفذت عبر الشبكة وكانت على شكل 25000 رسالة إلكترونية تم إرسالها دفعة واحدة، مما أدى إلى انهيار نظام

البريد الإلكتروني وما يتصل به من أعمال وأنشطة، قدرت الأضرار الناجمة عن الجريمة بعشرات الآلاف من الدولارات، وحوكم الطالب بعد إقرار المحكمة بأنه مذنب، ونفذ عليه حكم السجن ودفع غرامة مالية (أحمد نافع المدادحة، محمد عبد الدبس، 2012، ص193-194).

خاتمة:

ساهمت الانترنت في تسهيل إيصال المعلومات إلى الجمهور في أي وقت ودون وجود الحواجز الجغرافية، إلا أنها جعلت المجتمعات تعيش تهديدات ومخاطر جديدة على غرار سرقة المعلومات والتجسس الإلكتروني الذي لم يطل فقط الأفراد بل حتى سيادة الدول، إضافة إلى بروز تجارة جديدة كتجارة الالكترونية التي تستهوي قراصنة الانترنت لتهدد خصوصية الأفراد والحياسة على بطاقاتهم الائتمانية، مما بدأ الحديث عن ضرورة الحفاظ على الأمن الإنترنت أو المعلوماتي الذي برز في المجتمع المعلوماتي والمجتمع المعرفي، ومنه البحث عن بدائل واليات قانونية وأخلاقية كقيلة بالحد من تهديدات التي تشكلها شبكة الانترنت، وكذا بروز دراسات حول التربية الإنترنتية التي تغرس الوعي لدى الأفراد في كيفية التعامل مع وسيلة الوسائل، خاصة وأنها تتوجه إلى التشكل لدى كل فئات المجتمع على حد سواء، في ظل الإلحاح الشديد للاستخدام الأفضل لهذه الوسيلة.

قائمة المراجع:

1. الموسوعة العربية العالمية (1999)، مؤسسة أعمال للنشر والتوزيع، ط2، م03، الرياض، السعودية.
2. النقري معن (2003)، التكنولوجيا والاتصالات والإنترنت في تقارير التنمية الإنسانية الدولية العرب والعالم، مطبعة اليازجي، دمشق، سوريا.
3. اللبان شريف درويش (2005)، تكنولوجيا الاتصال: المخاطر والتحديات والتأثيرات الاجتماعية، ط1، الدار المصرية اللبنانية، القاهرة، مصر.
4. الصرايرة خالد عبده (2007)، النشر الإلكتروني وأثره على المكتبات ومراكز المعلومات، ط1، دار كنوز المعرفة، عمان، الأردن .
5. الرزو حسن مظفر (2007)، الفضاء المعلوماتي، ط1، مركز دراسات الوحدة العربية، بيروت، لبنان.
6. بدران عباس (2010)، الحرب الإلكترونية: الاشتباك في عالم المعلومات، مركز دراسات الحكومة الإلكترونية، بيروت، لبنان.
7. داود اللامي عثمان قاسم، أميرة سنكرولي البياتي (2010)، تكنولوجيا المعلومات في منظمات الأعمال: الاستخدامات والتطبيقات، ط1، مؤسسة الوراق، د ب.
8. دليو فضيل، وآخرون (2002)، التحديات المعاصرة: العولمة، الإنترنت، الفقر، اللغة: فعاليات اليوم الدراسي الأول لمخبر علم اجتماع الاتصال، جامعة منتوري، قسنطينة.
9. حسن يوسف يوسف (2011)، التجارة الإلكترونية وأبعادها القانونية الدولية، ط1، المركز القومي للإصدارات القانونية، القاهرة.
10. حسين عبد الجبار (2008)، اتجاهات الإعلام الحديث والمعاصر، ط2011، دار أسامة للنشر، عمان، الأردن.
11. طاهر داود حسن (2004)، أمن شبكات المعلومات، مركز البحوث للمملكة العربية السعودية، الرياض، السعودية.

12. أبو معال عبد الفتاح(2006)، أثر وسائل الإعلام على تعليم الأطفال وتنقيفهم، ط1، دار الشروق، عمان، الأردن.
13. ناصر خليل(2008)، التجارة والتسويق الإلكتروني، ط1، دار أسامة للنشر، عمان، الأردن.
14. مجد الهاشمي(2004)، تكنولوجيا وسائل الاتصال الجماهيري، ط1، دار أسامة للنشر، عمان، الأردن.
15. مجمد جمال راسم (2006)، الاتصال والإعلام في الوطن العربي في عصر المعلومات، الدار المصرية اللبنانية، القاهرة، مصر.
16. محمد صالح أحمد(دس)، الإنترنت والمعلومات بين الأغنياء والفقراء، مركز البحوث العربية والأفريقية، دب.
17. محمد فتحى عبد الهادي(2007)، المكتبات والمعلومات في عالم جديد، ط1، الدار المصرية اللبنانية، القاهرة، مصر.
18. محمد محمد الهادي(2001)، تكنولوجيا الاتصالات وشبكات المعلومات مع معجم شارح المصطلحات، القاهرة، المكتبة الأكاديمية، القاهرة، مصر.
19. محمود عباس طارق(2003)، المكتبات الرقمية وشبكة، ط1، القاهرة، المركز الأصيل للنشر والتوزيع.
20. مؤيد أحمد عبد الرحمن(2014)، تقنية المعلومات Information technology، ط1، دار دجلة ناشرون وموزعون، الأردن.
21. سلامة عبد الحافظ محمد ، وائل أبو مغلي(2002)، تطبيقات الحاسوب في المكتبات ومراكز المعلومات، ط1، دار صفاء للنشر والتوزيع، عمان، الأردن.
22. سمير أحمد محمد(2009)، التسويق الإلكتروني، ط1، عمان، دار الميسرة للنشر والتوزيع، عمان، الأردن.
23. إبراهيم حمادة بسيوني(2008)، دراسات في الإعلام وتكنولوجيا الاتصال والرأي العام، ط1، عالم الكتب، القاهرة، مصر.
24. عبد الخالق السيد أحمد(2008)، التجارة الإلكترونية والعولمة، مصر، المنظمة العربية للتنمية الإدارية.
25. فتحى محمد(2003)، الإنترنت شبكة العجائب: أهم أحداث القرن العشرين وأفاق المستقبل، دار الطائف للنشر والتوزيع، القاهرة، مصر.
26. فتحى عبد الهادي محمد(2001)، النشر الإلكتروني وتأثيره على مجتمع المكتبات والمعلومات: أبحاث ودراسات المؤتمر العلمي الثاني لمركز بحوث نظم وخدمات المعلومات، المكتبة الأكاديمية، القاهرة، مصر.
27. قندوشي ربيعة(2012) ، الإعلان الإلكتروني، دار هومة للطباعة والنشر والتوزيع، الجزائر.
28. ربحي مصطفى عليان(2015)، المكتبات الإلكترونية والمكتبات الرقمية، ط2، دار صفاء للنشر والتوزيع، عمان، الأردن.
29. رشاد غنيم السيد (2008)، التكنولوجيا والتغير الاجتماعي، ط1، دار المعرفة الجامعية، مصر.
30. خالد ممدوح إبراهيم(2008)، لوجيستيات التجارة الإلكترونية، ط1، دار الفكر الجامعي، الإسكندرية، مصر.
31. شاهين بهاء (1999)، الإنترنت والعولمة، ط1، القاهرة، عالم الكتب، القاهرة، مصر.

32. شمو علي محمد(دس)، الاتصال الدولي والتكنولوجيا الحديثة: الإنترنت القمر الصوتي الرقمي والملتيميديا، ط1، مكتبة ومطبعة الإشعاع الفني، الإسكندرية، مصر.
33. ذياب البدائية(2002)، الأمن وحرب المعلومات، ط1، دار الشروق، عمان، الأردن.
34. الجنيهي منير، ومدوح الجنيهي(2006)، البنوك الإلكترونية، دار الفكر الجامعي الإسكندرية، مصر.
35. بوراس زهرة، بوشارب أحمد(2014)، مدى نجاعة العمل الإداري في الجزائر باعتماد نظام الحكومة الالكترونية، المجلة الجزائرية للعولمة والسياسات الاقتصادية، ع5، الجزائر.
36. سلامي نادية(2014)، الإدارة الالكترونية كأساس لترقية الخدمة العمومية في الجزائر: الدور والتحديات، مجلة الحقوق والعلوم السياسية، ع04، الجزائر.
37. عيساني رحيمة الحبيب(2015)، دور الانترنت وتطبيقاتها في نشر الشائعات، لمجلة الباحث الإعلامي، ع28، الجزائر.
38. شعنبي صابرو(2015)، الإرهاب الإلكتروني: الإشكال والدوافع، مجلة العلوم الاجتماعية والإنسانية، ع10، جامعة تبسة، تبسة، الجزائر.
39. الدباس ريا أحمد(2010)، خدمات المعلومات في المكتبات التقليدية والالكترونية، ط1، دار البداية ناشرون، عمان، الأردن.
40. السيد بخيث(2011)، أخلاقيات العمل الصحفي The Ethics of journalism، ط1، دار الكتاب الجامعي، الإمارات العربية المتحدة.
41. السعيد مبروك إبراهيم(2014)، أخصائي المكتبات بين المهنة والرسالة، ط1، دار العلم والإيمان للنشر والتوزيع، مصر.
42. المدادحة أحمد نافع (2011)، النشر الالكتروني وحماية المعلومات، ط1، دار صفاء للنشر والتوزيع، عمان، الأردن.
43. المدادحة أحمد نافع، محمد عبد الدبس(2012)، تكنولوجيا المعلومات والشبكات في المكتبات ومؤسسات التعليم، ط1، مكتبة المجتمع العربي للنشر والتوزيع، عمان، الأردن.
44. Michel Grenie(1997), Dictionnaire de la micro-informtique, Larousse-Bordas, paris.
45. <http://arabic.Tebyan.net/index.aspx?pid=44602>, 29-03-2016, 11 :4
46. <http://diae.net/16243> h. 15:0004-01-2016.