الآثار الاقتصادية للجرائم الالكترونية

م.د نادية صالح مهدي الوائلي
كلية العلوم السياحية / جامعة كربلاء

الملخص

في ظل واقع يتسم بالتغيرات المتلاحقة في جميع جوانب الحياة الاقتصادية والسياسية والاجتماعية والثقافية ، برز على الساحة الاقتصادية متغير جديد ارتبط بثورة تكنولوجيا المعلومات والاتصالات ألا وهو الامن الالكتروني والذي يعد نتاجاً لتطبيقات التقنيات الحديثة وما رافقها من خطر التجسس على المعلومات والجرائم الالكترونية التي باتت موازية من ناحية الخطورة للجرائم التي يتم ارتكابها بالطرق التقليدية ، إذ باتت تهدد الاقتصاديات العالمية والنامية على حد سواء وأصبحت ترصد لها المبالغ الهائلة والجهود والخبرات من اجل تلافي خسائرها الفادحة ، وهذا ما اثر في مسيرة العجلة الاقتصادية في معظم المؤسسات الانتاجية من إذ التأخير في العمل او سرقة المشاريع والأفكار الجديدة نتيجة استخدام برامج ووسائل التجسس على الحواسيب الشخصية او تحويل حسابات شخصية في البنوك بصورة غير مشروعه من شخص لأخر وهذا ما يستوجب الوقوف عند هكذا موضوع ومعرفة مدى تأثيره في الجانب الاقتصادي .

Abstract

In light of the reality characterized by changes successive in all aspects of economic , political, social and cultural rights, has emerged in the economic arena a new variant has been associated with a revolution of information technology and communications , namely electronic security , which is the product of the application of modern technologies and the concomitant risk of spying on information and cyber crime , which has become a parallel hand seriousness of the crimes that are committed by traditional methods , where is now threatening the global economies and developing countries alike , and became the monitors have enormous sums , efforts and experiences in order to avoid losses heavy , and this is what the impact on the progress of the economic wheel in the most productive enterprises in terms of the delay in the work or the theft of projects and ideas as a result of the use of the new programs and the means to spy on personal computers or converting bank accounts illegally from one person to another and this is what requires the subject to stand at so and find out the extent of its impact on the economic side .

المقدمة ..

في ظل عالم متغير ومتجدد دخلت تكنولوجيا المعلومات والاتصالات في واقع حياتنا اليومية وأصبح جزء مهم لا يتجزأ من مفردات الواقع وقد أصبح الحاسوب من ابرز ملامح هذا التغير ودخوله في شتى مجالات الحياة فلا يكاد يخلو أي مكتب أو جهاز حكومي من هذا الجهاز وقد ساهم الحاسوب بإحداث نقلة في حياة المجتمع وتسهيله العديد من المعوقات والصعوبات واختصاره للجهد والوقت وقد ساعد ذلك ظهور الانترنت مما سرع من وتائر انجاز الإعمال .

وكما أدخلت تكنولوجيا المعلومات والاتصالات بعدا جديدا للحياة وللتعاملات أدخلت أيضا بالنسبة لمرتكبي الجرائم بعدا أخر هو البعد الالكتروني وأصبحت الجرائم ألان تتم عن طريق الانترنت وقد أصبحت جرائم السرقة والاختلاس وتدمير البيانات كلها من الجرائم المعروفة ، وقد ظهر مصطلح جديد لهذه العمليات جميعا يدعى (Cyber crime) ، وقد حدثت بالفعل

عمليات سرقة واختلاس وبيع وهمي نتيجة الاختراقات لأنظمة الحماية على الحواسيب العاملة في بنوك وبورصات ومؤسسات حكومية .

ومن هذا المنطلق تم التطرق الى هذا الموضوع لما له من اهمية على الواقع الاجتماعي والاقتصادي وحتى السياسي لما يحتويه من تداخلات وتأثير مباشر على مجريات العمل في العديد من الانشطة إذ ارتأينا التعريف بمفهوم الامن الالكتروني والجريمة الالكترونية فضلاً عن عناصر الجريمة الالكترونية وأسبابها وأساليبها والآثار الاقتصادية الناجمة عن هذا النوع من الجرائم.

مشكلة البحث ..

يعالج البحث الاشكالية الاتية ..

يواجه الامن الالكتروني مشاكل وعقبات والمتمثل بالجريمة الالكترونية وسرقة المعلومات واختراق المواقع الامر الذي يشكل تهديدا كبيرا لسريه وامن المعلومات على الصعيدين الدولي والإقليمي .

فرضية ألبحث ..

ينطلق البحث من فرضية مفادها ..

يرتبط الامن الالكتروني ارتباطا وثيقا بتطور تكنولوجيا ألمعلومات والاتصالات ، اذ ان ثورة تكنولوجيا المعلومات والاتصالات هي ذات منظور ثنائي الابعاد الجانب الايجابي منها متمثل على الصعيدين المحلي والعالمي بالتطورات الحديثة ، اما الجانب السلبي فيتجسد بما افرزته من اختراقات وتجاوزات على الحقوق المادية والفكرية .

هدف البحث ..

يهدف البحث إلى التعريف بالأمن الالكتروني والجريمة الالكترونية وتحديد عناصره وأسبابه وتأثيره على الجانب الاقتصادي لغرض الوقوف على الجوانب التي يتضمنها هذا الموضوع بدقة وموضوعية.

منهجية البحث ..

تم استخدام اسلوب المزج بين المنهج الوصفي و التحليأتي كونهما الاكثر انسجاما مع تحقيق هدف البحث.

هيكلة البحث ..

لغرض تحقيق هدف البحث واثباتا للفرضية فقد تمت دراسته على النحو الاتي :

اولا..مفهوم الامن الالكتروني والجريمة الالكترونية.

ثانيا ..عناصر الامن الالكتروني.

ثالثا .. اسباب الجريمة الالكترونية .

رابعا .. اسباب الجريمة الالكترونية.

خامسا .. الاثار الاقتصادية الناجمة عن الجرائم الالكترونية .

سادسا..التشريعات ضد الجرائم الالكترونية.

سابعا ..الجرائم الالكترونية في المملكة المتحدة والتشريعات اللاسيما بها .

ثامنا .. الجرائم الالكترونية مجرد قرصنة ام جرائم منظمة.

تاسعا .. الوقاية من الجرائم الالكترونية.

اولاً – مفهوم الأمن الاليكتروني والجريمة الاليكترونية ..

الأمن الاليكتروني عبارة عن مجموعة من المبادئ والممارسات التي تستهدف تعليم كيفية حماية الحاسوب وأصول المعلومات من التهديدات الكامنة على شبكة الانترنت.

ويمتد الأمن وسياسات الأمن أبعد من المفاهيم التقليدية للدفاع المادي ومنع الدخول على الحاسب والبرامج المضادة للفيروسات (Firewalls) وكلمات السر، فقد يشتمل الأمن على سياسات أخرى أو جوانب من السياسات، مثل السياسات التي تطبق على الموظفين والتحكم في الدخول على الشبكات والحصول على المعلومات والرقابة على وسائل الإعلام وتوزيعها، ومواجهة الكوارث واستمرارية العمل، ويزيد حجم ومجال المؤسسة التجارية من تعقيد بعض من تلك السياسات، ولكن يجب أن تنظر المؤسسات التجارية كافة، بغض النظر عن حجمها إلى الأمن نظرة شاملة ومن خلال القواعد والأنظمة والأدوار الوظيفية[1].

إما بالنسبة للجريمة الاليكترونية يمكن تعريفها [2]:

حسب تعريف الشرطة البريطانية هو استعمال شبكة الحاسوب لعمل إجرامي.

إما تعريف الإتحاد الأوروبي : أي مخالفة جرمية ترتكب ضد أو باستعمال شبكة الحاسوب.

أي ان الجريمة إلكترونية تتم باستخدام التقنية الحديثة ، سواءً كان ذلك باستخدام جهاز حاسوب أم أي جهاز إلكتروني أخر حديث، ولولا ذلك لا يمكن وقوعها.

ثانياً – عناصر الامن الاليكتروني.

يشتمل الامن الاليكتروني على مجموعة من العناصر الأساسية والتي يجب توفرها والتي نذكر منها الأتي :

(أ) سرية المعلومات (Data Confidentiality): و يشمل هذا الجانب جميع التدابير اللازمة لمنع الاطلاع غير المصرح لمقتحمي الحواسيب على المعلومات الحساسة أو السرية. عن أمن المعلومات، ومن أمثلة المعلومات التي يُحرص على سريتها (المعلومات الشخصية، والموقف المالي لشركة ما قبل إعلانه، والمعلومات العسكرية)[3].

(ب) سلامــة المعلومات (Data Integrity): إن ما يهمنا هنا هو اتخاذ التدابير اللازمة لحماية المعلومات من التغيير . وهناك أمثلة كثيرة لهذا المطلب: فقد تنشر جهة ما قوائم أسماء المقبولين ممن تقدموا بطلبات للعمل لديها، وكما نرى جميعاً فإننا عندما نتحدث عن أمن هذه القوائم نعني حمايتها من التغيير، إذ من المحتمل أن يقوم شخص ما بحذف بعض الأسماء وإدراج أسماء أخرى بدلاً منها، مسبباً كثيراً من الإرباك للناس والحرج للجهة المعنية. أو ممكن تغيير مبلغ التحويل من 100 دولار إلى 1000000 دولار.

(جـ) ضمان الوصول إلى المعلومات والموارد الحاسوبية (Availability): إن الحفاظ على سرية المعلومات وسلامتها أمر مهم و لا ريب، لكن هذه المعلومات تصبح غير ذات قيمة إذا كان من يحق لـه الاطلاع عليها لا يمكنه الوصول إليها أو أن الوصول إليها يحتاج وقت طويلاً. ويتخذ المهاجمون وسائل شتى لحرمان المستفيدين من الوصول إلى المعلومات، ومن هذه الوسائل حذف المعلومات نفسها أو مهاجمة الأجهزة التي تخزن المعلومات فيها وشلها عن العمل [4].

ثالثاً– أسباب الجرائم الاليكترونية :

أ– أسباب أو دوافع اقتصادية : يعد الدافع الاقتصادي حافزا مهما يدفع (الهاكرز – Hackers) لارتكاب جرائم من هذا النوع من خلال سرقة أرقام بطاقات إنترنت والسطو على حسابات مصرفية وتصل إلى معارك ضارية تجسد تنافسا تجاريا بين الشركات الكبرى في محاولة للإيقاع بالمنافس أو القضاء عليه ، ويعد هذا النوع من الاختراقات هو الأخطر على الأفراد

والشركات على حد سواء والأكثر انتشارا، وكثيرا ما تطالعنا الصحف ووسائل الإعلام الأخرى بأخبار محاولات سرقة بطاقات الائتمان للعديد من الأفراد ممن اعتادوا التسوق من خلال الشبكة. [5].

ب – أسباب سياسية وأمنية :وفي هذا الجانب تكثر القصص والحوادث في السعي للحصول على الأسرار العسكرية والأمنية، والتي تشير إلى انتهاج بعض الحكومات نهج التجسس على الأفراد والجماعات المعادية لها، لإحباط محاولاتها ومعرفة خططها الآنية والمستقبلية، ومن طريف القصص ما حدث في الولايات المتحدة الأمريكية عندما تم القبض على مجموعة من الهاكرز المحترفين، وبعد عدة جولات من المفاوضات تم تجنيدهم لصالح وكالة الاستخبارات الامريكية (CIA) لاستغلالهم بمهام أمنية.

ج– –أسباب ودوافع أخرى :ويمكن ايجازها في جانبين اثنين[6]:–

الأول.. يكون دافعه الأساسي التباهي والفخر لإثبات الذات ,وذلك لعدم وجود أي دافع اقتصادي أو سياسي, وهي كثيرا ما تحصل على أيدي الهواة وطلاب الجامعات والمبهورين بإمكانيات التقنية الحديثة .

أما الجانب الآخر .. فان يتمثل في محاولة إيجاد نوع من الرقابة الأخلاقية أو الاجتماعية أو الدينية من بعض المجموعات التي تبعا لعقيدتها تتبنى فكرة (الإصلاح) التي تستنبط منها قوانينها وأعرافها، فنلاحظ أن الكثير من الهاكزر نذروا طاقاتهم على سبيل المثال لتدمير المواقع التي تقدم خدمات وعروضا غير اخلاقية.

وقد أوضح الخبراء إن هناك العديد من الثغرات التي من الممكن إن تستغل في تسهيل النفاذ إلى المواقع التي يتم سرقتها أو تخريب البيانات التي تتضمنها في الجدول (1) أدناه الأماكن التي يمكن القلق من ناحيتها والتي تتعلق بصورة لاسيما بالبنية التحتية التكنولوجية التي من الممكن إن تستغل للاختراق مثلا التطبيقات او البرامج التي يتم استضافتها من الانترنت نسبة النفاذ اليها (48 %) [7] .

جدول (1) مواطن الضعف التي يمكن استغلالها من قبل مجرمي الانترنت

ت	نقاط الضعف	نسبة النفاذ
1	التطبيقات او البرامج التي يتم استضافتها من الانترنت	% 48
2	البيانات التي تنقل من الاجهزة المحمولة (الموبايل)	% 43
3	الاتصالات من والى الانترنت	% 40
4	العاملون المحليون في المواقع	% 34
5	الصيانة مع الاطراف المتعاقدة	% 34
6	الاميل (E- Mail)	% 33
7	شبكات الربط الاسلكية	% 23
8	الخدمات	% 19
9	طلبات تحميل البرامج	% 15
10	طلبات تحديث البرامج	% 9

الجدول من اعداد الباحثة بالاعتماد على: E- Crime Survey 2009 , The 7th Annual e-Crime Congress ,2009 , p 22

رابعا – أساليب الجريمة الاليكترونية .

1- صناعة ونشر الفيروسات : إذ تعد هذه الجرائم الأكثر تأثيرا وانتشارا معتمدة في أكثر الأحيان على شبكة الانترنت التي أصبحت تدخل في إعمالنا وبيوتنا وحياتنا اليومية وتؤدي الى تحقيق بعض أهداف الجريمة الالكترونية كحذف المعلومات أو تعديلها أو نقلها إلى أجهزة أخرى وإحداث خسائر اقتصادية ومادية كبيرة وتعطيل الأجهزة وعمل المؤسسات بكافة أنواعها[8].

2 – حصان طروادة : وهو البرنامج الذي يقوم على توفير مدخل للمخترقين إلى أجهزة تحتوي معلومات غير مصرح لهم بالدخول إليها ولا يتطلب استخدام هذا النوع من البرامج إلى خبرات تقنية لحقيق الهدف، ويكثر استخدام هذا الأسلوب على مواقع الانترنت بإذ يقوم المخترق بتعديل او تغيير المعلومات الموجودة في الموقع بما يخدم هدفه.

3 – إيقاف عمل الخادمات (Serves) : من خلال إغراق أجهزة الخادمات في المؤسسات (لاسيما تلك المرتبطة في الانترنت) بعدد هائل من طلبات التشبيك مما يؤدي إلى إيقاف عملها وتحقق الخسائر التي يهدف إليها القائم بهذا العمل

4- انتحال الشخصية : وهي جريمة العصر والتي تقوم على مبدأ انتحال شخصية أخرى والقيام بممارسات وإعمال غير مشروعة او استخدام هوية الشخص الضحية لتحقيق استفادة مادية بطريقة تجعل من الصعب اكتشاف الفاعل الحقيقي[9].

5- الابتزاز والتغرير: باستخدام أساليب عدة مما ذكر وعادة ما يكون الضحية من قليأتي الخبرة او المعرفة الالكترونية أو من الأطفال او النساء وتستخدم أيضا لهذا الهدف مواقع المواعدة على الانترنت او البرامج الحوارية

6- تشويه السمعة : وذلك بنشر معلومات حصل عليها المجرم بطريقة غير مشروعة او معلومات مغلوطة وتهدف إلى كسب مادي او سياسي او اجتماعي معين.

7- النصب والاحتيال : كبيع السلع أو الخدمات الوهمية أو سرقة معلومات بطاقات الائتمان واستخدامها وتوفر الانترنت مجالا واسعا للقيام بهذه الإعمال إذ إن الإطار الوهمي الذي يمكن ان تغلف فيه الانترنت من يقوم بهذه العملية تسمح له بالاختفاء في إي وقت يشاء وبعد قيامه بالجريمة

جدول (2) بعض اساليب الجرائم الالكترونية حسب احصاءات عام 2012

ت	نوع الجريـــــــمة	النسبه المئوية%
1	التسوق والمزادات عبر الانترنت	% 39
2	الاحتيال بطلب رسوم الاشتراك مقدما	% 11
3	البرامجيات وخدمات الكمبيوتر الاخرى	% 7.5
4	الحجوزات والتذاكر	% 6.1
5	بطاقات الائتمان المصرفي	% 4.5
6	تزوير الصكوك الكترونيا	% 2.3
7	التلاعب بتاريخ العقود والصفقات	% 2.8
8	وسائل اخرى	% 26.8
	المجـــــــــموع	% 100

الجدول من اعداد الباحثة بالاعتماد على ..

Mike McGuire، Cyber crime: A review of the evidence ,Chapter 2: Cyber-enabled crimes - fraud and theft Home Office Research Report 75 , England , 2013 , p 13

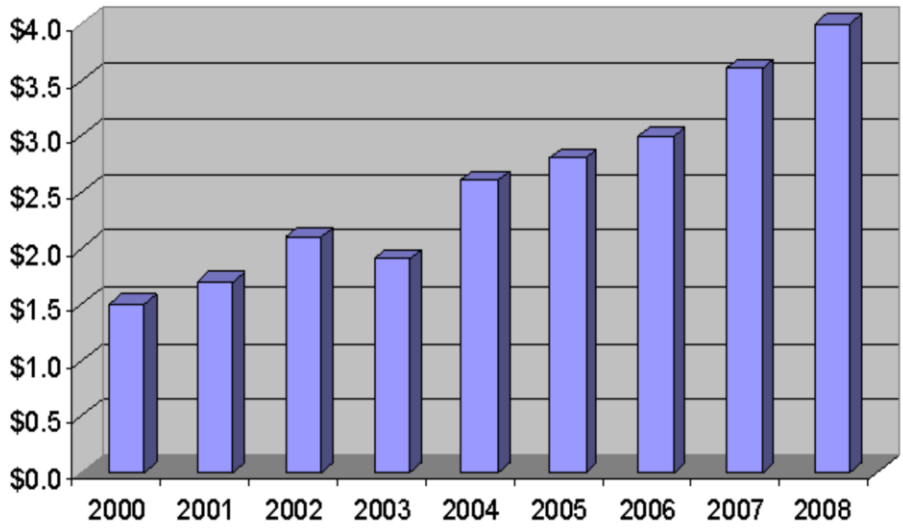
خامسا .. آلاثار الاقتصادية الناجمة عن الجرائم الاليكترونية .

1- إن جرائم الكمبيوتر و الانترنت تنتج من إذ أثرها الاقتصادي خسائر فادحة تقدر بمبالغ طائلة تفوق بنسب كبيرة الخسائر الناجمة عن جرائم المال التقليدية مجتمعة و لو أخذنا على سبيل المثال بريطانيا ، التي تعد الدولة الآخرة في حجم الخسائر التي تلحقها جراء جرائم الكمبيوتر بعد الولايات المتحدة فانه ، وعلى لسان وزير التكنولوجيا البريطاني Lord Reay أعلن في عام 1992أن الجرائم التي تتعرض لها أجهزة و أنظمة الحاسوب كالتطفل التشغيأتي hacking و الفيروسات Viruses تضر بأعمال أكثر من نصف الشركات الصناعية و التجارية في بريطانيا بتكلفة سنوية بما يقارب (1,1 بليون جنية إسترليني) [10].

2- أما في الولايات المتحدة الأكثر تضررا من جرائم الكمبيوتر ، فأن التقرير الصادر عن معهد (Ponemo Institute) والمعني بدراسة جرائم الانترنت للعام 2013 يشير إلى ان المؤسسات المصرفية وحدها تكبدت خسائر بلغت (11.56) مليون دولار من جراء انتهاكات الهاكرز للمواقع اللاسيما بالبنوك وتحويل الحسابات او تعطيلها [11].

3- و في دراسة أجريت عام 1984م في كندا و نشرت نتائجها مجلة (الكمبيوتر و الحماية) الأمريكية عام 1984م ، ظهر أن صافي معدل الخسارة الناجمة عن السطو المسلح (جريمة تقليدية) على البنوك 3200 دولار للحالة الواحدة و أن نسبة القبض على مرتكبيها تصل إلى 95% بينما يصل معدل الخسارة الناجمة عن اختلاس أموال البنوك بدو استخدام الكمبيوتر مايقارب (23500) دولار للحالة الواحدة ، فإذا استخدم الحاسوب في ارتكاب الجريمة فان معدل الخسارة يرتفع بشكل حاد ليصل إلى 430000 دولار و تنخفض نسبة فرص ضبط الجناة من 95% إلى 5% أما فرص الضبط و الملاحقة القضائية معا فتنخفض إلى أقل من 1% [12].

شكل (1) الخسائر الناجمة عن الجرائم الاليكترونيةفي الولايات المتحدة للمدة من (2000 – 2008) مليار دولار



المصدر من اعداد الباحثة بالاعتماد على :

Cyber source online fraud report 2009, Latin America , 2009 , p14

4- منذ منتصف الثمانينات ثمة حجم خسائر كبير تتكبده كبرى شركات المال و البنوك و المؤسسات في الدول المتقدمة ، الاقتصادية و العسكرية و العلمية جراء جرائم الكمبيوتر ، كإفشاء البيانات السرية المعالجة في نظم الحاسوب و الاتجار بالمعلومات و تدمير نظم التشغيل و جرائم الفيروسات و قرصنة البرامج ، و غيرها . و الأمر الذي بات مؤكدا ، أن جرائم الكمبيوتر أكثر خطورة من الجرائم التقليدية، و تخلف حجما كبيرا من الخسارة ، و تشيع القلق و تهدد مستقبل سوق المال و تمس حق للأفراد في المعلومات ، إلى جانب خطرها على السيادة الوطنية .

5- ومن دراسة مسحية شملت لجنة التدقيق بالمملكة المتحدة أواخر الثمانينات عن غش الحاسوب و إساءة استخدام الحاسوب ، شملت (6000) من المؤسسات التجارية و الشركات في القطاع الخاص ، تبين أن ما يقرب من نصف هذه حالات (الاحتيال بواسطة الحاسوب) – كما تسميها الدراسة المذكورة ، قد اكتشفت مصادفة ، و أن خسائر هذه الحالات تقدر بنحو (2,5) مليون جنيه إسترليني ليست إلا (جبل جليد عائم يختفي جزؤه الأكبر تحت سطح الماء) و في دراسة مسحية لإدارة الصحية و خدمات الإنسان (HHS) في الولايات المتحدة الأمريكية عام 1983م ظهر أن الحوادث العرضية مصادقة (مثل الفضول أو الشكوى أو الانتقام من المبلغ ضده (الفاعل) أو الأنشطة غير العادية للجناة و تحديدا الاتفاق غير العادي) كانت هي العادي) كانت هي العامل المنبه لاكتشاف 49% من حالات غش الحاسوب ، أن التدقيق الداخلي و الخارجي كان المنبه لاكتشاف 29% ، بينما كانت الرقابة الشاملة (الرقابة على الانتهاكات الأمنية للحاسوب) المنبه لاكتشاف 25% من هذه الحالات[13] .

سادسا .. التشريعات ضد الجرائم الاليكترونية

تعد السويد أول دولة تسن تشريعات لاسيما بجرائم الحاسب الآلي والانترنت، إذ صدر قانون البيانات السويدي عام (١٩٧٣ م) الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي فضلاً عن شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشروع عليها.

وتبعت الولايات المتحدة الأمريكية السويد إذ شرعت قانونا لاسيما بحماية أنظمة الحاسب الآلي (١٩٧٦ –١٩٨٥)، وفي عام (١٩٨٥) حدّد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية وهي :جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحاسب الآلي، دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب . وفي عام (١٩٨٦) صدر قانونا تشريعاً يحمل الرقم (١٢١٣) عرّف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الدستورية اللازمة لتطبيقه، وعلى اثرذلك قامت الولايات الداخلية بإصدار تشريعاتها اللاسيما بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي[14]

وتأتي بريطانيا كثالث دولة تسن قوانين لاسيما بجرائم الحاسب الآلي إذ أقرت قانون مكافحة التزوير والتزييف عام (١٩٨١) الذي شمل في تعاريفه اللاسيما بتعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى . وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والانترنت إذ عدّلت في عام (١٩٨٥) قانونها الجنائي بإذ شمل قوانين لاسيما بجرائم الحاسب الآلي والانترنت، كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسوبية وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي .وفي عام (١٩٨٥) سنّت الدنمارك أول قوانينها اللاسيما بجرائم الحاسب الآلي والانترنت والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي أو التزوير أو أي كسب غير مشروع سواء للجاني أو لطرف ثالث أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها أو تغييرها أو الاستفادة منها[15].

وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية إذ أصدرت في عام (١٩٨٨ (القانون رقم) ١٩ – ٨٨) الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها .أما في هولندا فلقاضي التحقيق الحق بإصدار أمره بالتصنت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة، كما يجيز القانون الفنلندي لمأمور الضبط القضائي حق التنصت على المكالمات اللاسيما بشبكات الحاسب الآلي، كما تعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام.

وفي اليابان قوانين لاسيما بجرائم الحاسب الآلي والانترنت ونصت تلك القوانين على انه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق أو إفشاء كلمات السر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته.

كما يوجد في المجر وبولندا قوانين لاسيما بجرائم الحاسب الآلي والانترنت توضح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها، وتعطي تلك القوانين المتهم الحق في عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الأكواد اللاسيما بالبرامج [16].

سابعا .. الجرائم الالكترونية في المملكة المتحدة والتشريعات اللاسيما بها

لقد تزايد النشاط الإجرامي فيما يتعلق الجريمة الاليكترونية وفي المملكة المتحدة وحسب تقرير الجريمة الاليكترونية لوحظ زيادة في معدلات الجريمة ، فهناك نوعان مختلفان من الجريمة بالنسبة للملكية الفكرية او الجريمة الاليكترونية الأولى تتعلق بالتزوير ولأخرة القرصنة وقد سارع في معدلات الجريمة السرعة الكبيرة في التطور التكنولوجي واكتشاف طرق جديدة وبرامج يمكنها النفوذ إلى الحواسيب اللاسيما بالشركات الكبرى او حتى البرامج التي تساعد في تغيير العلامات التجارية وتزييفها وهذا ما يلقي على عاتق السلطات المختصة والإفراد على حد سواء عبء إضافي من إذ انه لا يتم التعرف على محتوى وصحة ما يتم التعامل معه إلا بعد فوات الأوان[17] .

ومن ضمن التشريعات التي تم التنويه عنها فيما يخص الجريمة الاليكترونية ضمن (قانون منع الفساد العام) والتي تم نشرها ضمن تقرير (2009 IP Crime Report – 2008) والذي يشتمل قانون عائدات الجريمة للعام 2002 والذي أعطى صلاحيات اكبر في الاقتصاص من المجرمين والحق في مصادرة ملكيتهم في المملكة المتحدة والجدول (3) يوضح حجم المبالغ التي تم استعادتها للمدة 2003 – 2008[18] .

جدول (3) حجم المبالغ التي ضبطت في إطار قانون عائدات الجريمة للمدة من (2003 – 2008) مليون جنيه إسترليني

العام	المبلغ
2004 – 2003	54.5
2005 – 2004	84
2006 - 2005	96
2007 – 2006	125.36
2008 – 2007	135.7

الجدول من اعداد الباحثة بالاعتماد :

, Minister of State for Higher Education and David Lammy , 2008 - 2009 IP Crime Report Intellectual Property,USA, 2009, p 42.

من الجدول السابق يتضح إن المبالغ التي تم ضبطها خلال المدة من عام 2003 ولغاية 2008 هي في تزايد مستمر وهذا ما يدل على تزايد معدلات الجريمة الاليكترونية في المملكة المتحدة ، إذ ارتفعت من (54.5) مليون جنيه إسترليني للعام 2003 – 2004 لتصل إلى (135.7) مليون جنيه إسترليني للعام 2007 – 2008 .

وبالنسبة للأشخاص الذين يحترفون هذا النوع الإجرامي فهم في تزايد مستمر أيضا رغم القوانين الرادعة لهم وقد تم تقسيم هؤلاء إلى فئتين وهما الأولى تختص بالعلامات التجارية أي يعملون على طبقة معنية وهي الماركات العالمية وتركيز اهتمامهم في سرقة الشركات المعروفة والتحاليل على الناس باسم هذه الشركات إما الفئة الآخرة مختصة بسرقة براءات الاختراع والجدول (4) يوضح أعداد الذين تم إلقاء القبض عليهم للمدة من عام (2002 – 2008)

جدول (4) إعداد الذين تم القبض عليهم بالجرائم الاليكترونية في المملكة المتحدة

للمدة من (2002 – 2008)

العام	فئة العلامات التجارية	فئة براءات الاختراع	مجموع الفئتين
2002	331	71	402
2003	404	85	489
2004	493	98	591
2005	748	160	908
2006	932	243	1175
2007	893	367	1260
2008	1200	402	1602

الجدول من إعداد الباحثة بالاعتماد على :

Stefan Fafinski,the cost of sybercrime adetica report in partnership with the office of cyber security and information assurance in the cabinet office , United Kingdom, 2009, p 20.

وفي بداية عام 2009 تم مداهمة مصنع في غرب لندن في بريطانيا تم اكتشاف انه يقوم بتزييف الأقراص الليزرية من خلال سرقة حقوق الطبع ويقوم بطبع أقراص غير مرخصة إضافة إلى عمليات غسيل الأموال

وتم مصادرة ملايين الأقراص التي كانت معدة للبيع [19] .

وقد نشرت منظمة التعاون والتنمية للعام 2008 تقريرها عن الآثار الناجمة عن القرصنة والتزوير على المجتمع كما موضح في الجدول (5) .

جدول (5) الآثار الناجمة عن القرصنة والتزوير الاليكتروني في المجتمع للعام 2008

ت	المجموعة	الاثار
1	الثلاثية الأسيوية	بيع أقراص الفيديو الرقمية المقلدة في لندن
2	الجماعات الايرلندية	بيع لعب الأطفال ، البطاريات ،الأدوات الكهربائية ،والعقاقير البيطرية في ايرلندا الشمالية
3	المجموعة الإسرائيلية مع أصول روسية	بيع المنتجات المقلدة في اليابان
4	الايطالية وعصابات أوربا الشرقية	استيراد الاسطوانات المدمجة المقرصنة في ايطاليا
5	المافيا الروسية	مبيعات الأقراص المدمجة المقرصنة في لندن

الجدول من إعداد الباحثة بالاعتماد على

The Economic Impact of Counterfeiting and Piracy, OECD, June 2008

ثامنا .. الجرائم الاليكترونية مجرد قرصنة ام جرائم منظمة ..

يتبادر إلى الذهن فور التحدث عن الجريمة المنظمة عصابات المافيا كون تلك العصابات من أشهر المؤسسات الإجرامية المنظمة .وقد سارعت عصابات المافيا بالأخذ بوسائل التقنية الحديثة سواء في تنظيم أو تنفيذ إعمالها، ومن ذلك إنشاء مواقع لاسيما بها على شبكة الإنترنت لمساعدتها في إدارة العمليات وتلقي المراسلات واصطياد الضحايا وتوسيع إعمال وغسيل الأموال، كما تستخدم تلك المواقع في إنشاء مواقع افتراضية تساعد المنظمة في تجاوز قوانين بلد محدد بإذ تعمل في بلد أخر يسمح بتلك الأنشطة.

ويوجد على الشبكة (٢١٠) موقع يحتوي اسم نطاقها على كلمة مافيا، في حين يوجد (٢٤) موقعا يحتوى على كلمة مافيا، كما وجد(٤) مواقع للمافيا اليهودية [20].

وقد خصص بعض هذه المواقع للأعضاء فقط ولم يسمح لغيرهم بتصفح تلك المواقع في حين سمحت بعض المواقع للعامة بتصفح الموقع وقامت مواقع أخرى بوضع استمارة تسجيل لمن (يرغب في الانضمام إلى العصابة من الأعضاء الجدد) .

والجريمة المنظمة ليست وليدة التقدم التقني وأن كانت استفادت كثيرا منه فا" الجريمة المنظمة وبسبب تقدم وسائل الاتصال والتكنولوجيا والعولمة أصبحت غير محددة لا بقيود الزمان ولا بقيود المكان وأن ما أصبح انتشارها على نطاق واسع وكبير وأصبحت لأتحدها الحدود الجغرافية ، كما استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة في وسائل الإنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بيسر وسهولة [21].

باتت قضية الأمن الإلكتروني تُشكل هاجسًا متزايدًا لدى دوائر صنع القرار الأمريكي، وداخل الأروقة البحثية الأمريكية منذ أن تعرضت مصالح وهيئات حكومية كبرى لضربات إلكترونية موجعة عام 2007 كان في مقدمتها وزارات الدفاع والخارجية والأمن القومي والتجارة، فضلاً عن وكالة الفضاء الأمريكية (ناسا) وجامعة الدفاع الوطني.

كما جرى اختراق البريد الإلكتروني لوزير الدفاع الأمريكي الأسبق والحالي روبرت جيتس. إذن الحرب الإلكترونية باتت حقيقة واقعة لا جدال فيها. فعمليات القرصنة والتجسس تطورت من مجرد هجمات عشوائية إلى جرائم منظمة بفعل مجموعات غير رسمية تستهدف الإنترنت التجاري مثلما حدث مع (Commercial Internet) إستونيا في إبريل ومايو

2007أو حتى مجموعات رسمية تمثل دولة بعينها تستهدف قدرات سياسية أو اقتصادية أو عسكرية، وفي هذا الإطار تبدو كل من الصين وروسيا مصدر تهديد جدي للقوة الأمريكية [22].

وفي الآونة الأخيرة اهتمت مراكز الأبحاث الأمريكية بجانب المؤسسات التكنولوجية الأمريكية بتلك القضية. وفي إطار هذا الاهتمام نشرت مؤسسة التراث البحثية الأمريكية مقالة أعدها جيمس جاي كارافانو وإريك سايرز في ديسمبر /كانون الأول 2009 بعنوان بناء قيادة أمنية إلكترونية للقرن« هدفت إلى الوقوف » الحادي والعشرين على طبيعة هذا التهديد الأمني الجديد، وتقديم توصياتها لإدارة أوباما لتعزيز أمنها الإلكتروني .بحسب موقع تقرير واشنطن [23].

وقد ركزت الحكومة الامريكية الجديدة برئاسة اوباما على الامن الاليكتروني وذلك لما يمثله من تحديًا يتمثل في الرغبة في الحفاظ على الأمن الإلكتروني ووضع استراتيجية تضع في الاعتبار الجوانب المحلية والعالمية للقضية لاسيما مع تزايد اعتماد الأمريكيين على شبكة الإنترنت في إجراء معاملاتهم البنكية والاستثمارية فضلاً عن الاتصالات الإلكترونية ومتابعة الأخبار، وبين خوف من الوقوع في فخ انتهاك الخصوصية بما يعد تعديًا على الحريات المدنية للمواطنين الأمريكيين. واليوم أصبح السؤال الملح هو :ما الطريقة المثلى للتعامل مع هذا الخطر غير المرئي العابر للحدود الذي يكاد يكون غير مكلف بالنسبة إلى فاعله، لكنه يضرب الجهة المستهدفة في مقتل؟.

المثير في الأمر أن أمريكا التي تشكو الآن من خطر الحرب الإلكترونية واحتمال تعرضها لضربة قوية تشل حركتها هي التي بدأت هذه الحرب عام 1991 عندما شن سلاح الجو الأمريكي حربًا إلكترونية في حرب الخليج الآخرة عبر استهداف قدرات الأنظمة الدفاعية العراقية وتدمير البنية التحتية للاتصالات.

وبالرغم من أن تنفيذ هجوم إلكتروني لا يقتضي المركزية بمعنى أن الهجوم قد ينفذ من قبل عدة جهات في دول مختلفة في التوقيت ذاته، إلا أن الفضاء الإلكتروني يظل معتمدًا على وجود شبكة من خوادم الكمبيوتر(Servers) وكابلات الألياف البصرية ونظام ضخم من الكابلات يمر عبر محيطات العالم ومن ثم يمكن طرح إمكانية فرض عقوبات على الدول التي تستضيف منفذي هذه الهجمات إذا رفضت التحرك ضدهم[24].

وكما تشير المطبوعات العسكرية الصينية فإن جيش التحرير الشعبي الصيني شن هجمات إلكترونية متكررة على شبكة عسكرية أمريكية هي شبكة (C4ASR) وقد رصدت وزارة الدفاع الأمريكية خططًا صينية لتطوير وتحسين قدراتها القتالية الإلكترونية.

وفقَ تقريرٍ للبنتاجون عن القدرات العسكرية للصين صدر عام 2006 ، فإن الجيش الصيني يحاول ضمان توفر المعدات والخبرات المدنية في الكمبيوتر لتساعده في تدريباته وعملياته، كما يستعين الجيش الصيني بالأكاديميين ومعاهد وشركات تكنولوجيا المعلومات لدمجهم في وحدات دعم للجيش في العمليات العسكرية، لكن هذا لا يعني أن الولايات المتحدة هي وحدها المستهدفة من الصين فحسب صحيفة (دير شبيجل) الألمانية فإن الصين مارست عمليات القرصنة الإلكترونية على أنظمة الكمبيوتر اللاسيما بالمستشارة الألمانية (أنجيلا ميركل) فضلاً عن أنظمة ثلاثة وزراء آخرين هم وزراء الخارجية والاقتصاد والأبحاث منذ نحو عام، لكن السفارة الصينية في برلين نفت الاتمهماًت ووصفتها بأنها (افتراض غير مسؤول دون وجود دليل)[25].

تاسعا ..الوقاية من الجرائم الاليكترونية ..

هناك العديد من الوسائل الوقائية التي من الممكن ان تخفف من خطر التعرض للسرقة او الاحتيال على شبكة الانترنت هذه الوسائل على قدر ما هي بسيطة إلا أنها غاية في الأهمية والتي يمكن إدراجها في أدناه[26]:

1- تجنب استعمال اسمك الحقيقي أو أي معلومات شخصية قد تستغل ضدك، وإذا رغبت في مزيد من الخصوصية والحماية قم بشراء بريد الكتروني مدفوع من احد مزودي الخدمة لاستخدامك الرسمي .

2- عدم عرض اسمك أو بريدك الإلكتروني الشخصي في الأماكن العامة على النت، مثل المنتديات أو الأدلة أو المواقع الاجتماعية، وإذا اضطررت فقم باستخدام بريد الكتروني آخر (ثانوي)، فقد تتعرض لهجمات تصيّد Phishing أو إغراق برسائل Spam

3- ضبط إعدادات الماسنجر لمنع استقبال الرسائل من أناس لا تعرفهم، وذلك منعاً لاستقبال رسائل سبام عبر الماسينجر IM Spam (Spim).

4- تحاشي ذكر أي معلومات لاسيما مثل أرقام الحسابات أو كلمات السر أثناء المحادثة، فقد يتم اعتراضها من قبل برامج التجسس على الشبكةSniffers ، فبرامج الحماية تحمي بياناتك أثناء وجودها في جهازك، وليس أثناء انتقالها خارجه إلى الشبكة [27] .

5- دعم جهازك ببرامج وتأكد من احتوائه على مضاد فيروسات ومضاد للسبام والبرمجيات الضارة وجدار نار ومضاد للتصيّد وتقنيات إسناد وتعرّف مبكر للهجمات والملفات الضارة .

6- التأكد من عدم تشغيل الانترنت آلياً مع بدء تشغيل الجهاز والنظام، واحرص على إغلاق الجهاز وفصل خط الاتصال سواء كان هاتفيا أو رقميا DSL في حال عدم استخدامك له.

7- التحديث المستمر لنظام التشغيل باستمرار وكذلك برنامج الحماية .

8- عدم فتح أي ملفات أو بريدا إلكترونيا قبل مسحه من برنامج مضاد الفيروسات، ولا تفتح ملفات أو بريدا إلكترونيا من شخص غير معروف، وإذا قمت بذلك فاحذر من فتح الروابط أو الوصلات داخلها .

9- الحذر عند مشاركة الملفات، وارفض تماماً استقبال الملفات ذات الامتدادات

(.exe. .scr. .lnk. .bat. .vbs. .dll. .bin. .cmd)

الاستنتاجات ..

تم التوصل الى الاستنتاجات الاتية ..

1- ترتبط الجريمة الالكترونية بالتطورات التي افرزتها ثورة تكنولوجيا المعلومات والاتصالات الحديثة.

2- لا ترتبط الجريمة الالكترونية بفئة معينة من الافراد وإنما تعتمد على القابلية على التعامل مع التقنيات الحديثة .

3- احدثت الجريمة الالكترونية اثار سلبيه في اغلب الاقتصاديات التي اصبحت تحت طائلة هذا النوع الجديد من الجرائم .

4- نوعية الانتهاكات او الجرائم تكون على معلومات (Information's) ذات قيمة مادية وفكرية عاليه .

5- اغلب الجرائم الالكترونية تعتمد على عدم توخي الحذر والاستخدام غير المتقن لشبكة المعلومات الدولية (الانترنت) من قبل الافراد .

التوصيات ..

1- احد اهم عوامل تفادي مثل هذه الجرائم هي الاستخدام الامن للأجهزة الحديثة او ذات التقنية العالية من خلال استخدام برامج حماية من التجسس والتعامل بحذر مع المعلومات المستلمة وغير مؤكد مصدرها .

2- تفعيل العمل على برامج حماية الملكية الفكرية التي تسُهم بشكل كبير في ترصين دور اصحاب براءات الاختراع والحفاظ على حقوقهم من السرقات التي تغلف بغطاء قانوني.

3- احد اهم طرق الاختراق هي ترك الحسابات اللاسيما بالمستخدم بدون اغلاق امن لذلك لتوخي الحذر يجب التأكد من الاغلاق الامن لحسابات الويب كالاميل او الفيس بوك باستخدام (log out) فالإغلاق غير الامن احد اهم المنافذ للهكرز .

4- تجنب فتح أي اميل او صورة يكون حجمها صغير جدا لان اغلب الفايروسات وبرامج الهاكرز تكون بهكذا احجام .

5- في حالة التسوق على الانترنت يجب التأكد من المواقع اللاسيما بالماركات المعروفة على الانترنت كمواقع تسوق لان اغلب حالات السرقة وتحويل الاموال تكون عن طريق مواقع مزيفه.

المراجع ..

1- Steve Wozniak , THE ART OF DECEPTION , Controlling the Human Element of Security KEVIN D. MITNICK , USA, 2002 , p 203.

2- Revision of the Computer Misuse Act: Report of an Inquiry by the All Party Internet Group , 2004 , p 7.

3- Janet Williams , Association of Chief Police Officer of England, Wales & Northern Ireland , 2009 , p 5.

4- خالد بن سليمان الغثبر و محمد بن عبد الله القحطاني،امن المعلومات بلغة ميسرة،الرياض ، ط1، 2009 ، ص 22.

5- Bryan Krekel , Capability of the People's Republic of China to Conduct Cyber arfare and Computer Network Exploitation . USA, 2009 , p 16.

6- - خالد بن سليمان الغثبر و محمد بن عبد الله القحطاني، مصدر سابق ، ص 23.

7- Michael B. Mukasey , Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition , 2001, p24.

8- قراصنة الانترنت تعددت الوسائل وتنوعت الغايات ، اسواق العرب عالم المبتكرات والتكنولوجيا والمحركات ،2009 ، ص 7.

9- E- Crime Survey 2009 , The 7th Annual e-Crime Congress ,2009 , p 22.

10- Daniel Chávarri , Current and future trends on e-crime , 2008 , p 6.

11- Thomas A. Johnson , Electronic Crime Scene Training , Overview Discussion and Questions , National Cyber Crime Training Partnership , The California Sciences Institute , 2009 , p 9.

12- عبد الصادق عبد الجليل عبد الصادق ، جرائم المعلومات ، http:// www.ict.sd

13- Cyber Source online Fraud Report 2009 . , p 14.

14-Network Security The Bad, The Good, and The Quiz Technology for the Rest of Us: What Every Librarian Should Understand about the Technologies that Affect Us , The Ohio State University , 2004 , p 15.

15 - ITU TOOLKIT FOR CYBERCRIME LEGISLATION , Developed through the ,American Bar Association's Privacy & Computer Crime Committee Section of Science & Technology Law With Global Participation , 2009 , p27.

16- James X. Dempsey , Cyber and Electronic Crime –ID Theft and Child Online Protection Background Paper: Balancing Privacy and Safeguards , Center for Democracy and Technology , 2007 , p 7.

17- Paul Wright and William Fone , Designing and Managing Networks to Aid the Capture and Preservation of Evidence to support the Fight Against e-Crime , 2009, p 5.

18- The Economic Impact of Counterfeiting and Piracy, OECD, June 2008 , p 63.

19 Thomas M. Robertson ,2008 CRIME LEGISLATION UPDATE , An Outline of Recently Passed Legislation , 2009 , p 10.
20- E- Crime Survey 2009 , The 7Th Annual E- Crime Congress in partnership with KPMG , Swiss, 2009 , p 24.
21- eCrime – hinter den Kulissen , Carsten Stiebens ,eSafe PreSales Consultant , Aladdin Germany, 2009, p 23.
22- http://www.antiphishing.org/events/2009_gm.html.
23- 2004 E-CrimeWatch Survey™ Summary of Findings , CSO magazine in operation with the U.S. Secret Service & CERT, 2004, p 19.
24 – القرصنة من مجرد هجمات عشوائية الى جرائم منظمة ، الامن الاليكتروني هاجس متزايد لدى ادارة اوباما ، مجلة اسواق العرب ، 2009 ، ص 9.
25 - Electronic Crime Committee 2008 Annual Report , 2008 , p 20.
26- Bill Fone and Paul Wright , CRIMINAL ACTIVITY IN CYBERSPACE, DETECTION PREVENTION AND SOCIAL RESPONSIBILITIES , 2007. p 5.
27 - Personal
Internet Security: Follow –up , Science and Technology Committee , 4th Report of Session 2007–08 , p 12.