ندوة علمية حول الأمن الإلكتروني

المحور الثامن: الجرائم الالكترونية

من اعداد : شبايكي نزهة

السنة الأولى دكتوراه

تخصص : عقود و مسؤولية

كلية الحقوق جامعة الجزائر 01

مقدمة :

لقد صاحب الثورة الصناعية و خاصة في مجالي الاتصالات و البحوث العلمية المتنوعة ثورة معلوماتية ، كان لها الأثر الكبير على حياة الناس العامة و الخاصة .و لتبادل هذه المعلومات استخدمت وسائط عديدة لنقلها و تداولها بين الدول فكانت الانترنت الوسيلة الرائدة في هذه الوسائط معتمدة في ذلك على الحاسوب ،حيث أصبح هذا الأخير بمثابة العمود الفقري لأنشطة الإنسان في كافة المجالات و الأمكنة لدى جميع الدول المتقدمة و النامية.

و قد تنتج عن التطور التكنولوجي في الوقت الراهن وجود علاقة قوية بين استخدام الحاسوب و ارتكاب بعض الجرائم المستحدثة ،و سواء كان هذا الأخير محلا للجريمة أو وسيلة لها ،فإن الجوهري في الأمر أن انتشار الوسائل المعلوماتية نتيجة لثورة المعلومات أصبح يزيد من فرص انتشار هذا النوع من الجرائم المستحدثة.

و يؤكد الخبراء أن الجرائم الالكترونية تزداد كلما توغل العالم في استخدام الانترنت و قد حققت هذه الجرائم خسائر فادحة بالاقتصاد الأمريكي ،كما لم ينج العالم العربي من هذه الجرائم و إن كانت الخسائر ليس على المستوى نفسه .

ولهذا كان من الضروري التصدي لهذه الجرائم و مكافحتها بغية الحد منها .ومن هنا نطرح الإشكالية التالية:

ماهي الجريمة الالكترونية ؟ و كيف السبيل إلى معالجتها ؟

المبحث الأول :ماهية الجريمة الالكترونية

تعتبر الجريمة الالكترونية من اخطر الجرائم التي عرفتها الدول لذا ينبغي تحديد مفهومها ،و ذلك من خلال تعر يفها و بيان خصائصها و هذا في المطلب الأول ،ثم ينبغي معالجة أنواعها و أنواع الجناة فيها و هذا في مطلب ثاني .

المطلب الأول :تعريفها و خصائصها

تعددت الجهود الرامية لوضع تعريف جامع مانع للجريمة الالكترونية لكن الفقه لم يجتمع على وضع تعر يف محدد لها، فقد ذهب جانب من الفقه إلى تناولها بالتعريف على نحو ضيق و جانب أخر عرفها على نحو موسع .

التعريف الضيق للجريمة الالكترونية :

ذهب الفقيه (MERWE) إلى أنها هي الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي .

فيما عرفها (ros blat)بأنها كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي و إلى تحويل طريقه .

التعريفات الموسعة لمفهوم الجريمة الالكترونية :

ذهب جانب من الفقه إلى تعريف الجريمة الالكترونية بأنها عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسب و شبكات الاتصال الخاصة به التي يحميها قانون العقوبات و يفرض لها العقاب .

كما يرى جانب من الفقه بأنها سلوك إجرامي يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر .[1]

و ذهب بعض الخبراء إلى تعريفها بأنها سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و نقلها [2].

و تحمل الجريمة الالكترونية عدة مسميات منها الجريمة السايبرية ،جريمة التقنيات العالية ،و جرائم الحاسوب و الانترنت .

خصائص الجريمة الالكترونية :تتميز الجرائم الالكترونية بالخصائص التالية :

1 –صعوبة إثباتها :فمعظم الجرائم الالكترونية تم اكتشافها بالصدفة و بعد وقت طويل من ارتكابها لافتقارها إلى الدليل المادي التقليدي كالبصمات .[3]

2 – عابرة للدول :إذ أنها لا تعترف بالحدود الجغرافية للدول و لا بالمكان و لا بالزمان ،فاغلب الجرائم المرتكبة عبر شبكة الانترنت يكون الجاني فيها في دولة ما و المجني عليه في دولة أخرى ،و قد يكون الضرر المترتب عن الجريمة ليس واقعا على المجني عليه داخل إقليم دولة الجاني .

3- **جرائم ناعمة** : إذا كانت الجرائم التقليدية تتطلب استخدام العنف لارتكابها كجرائم الإرهاب ،القتل ،السرقة ، فإن الجرائم الالكترونية لا تحتاج إلى العنف ،فنقل بيانات من كمبيوتر إلى أخر أو السطو الالكتروني على أرصدة بنك لا يتطلب أي عنف .

---

[1] د.عبد العال الديربي ،ا.محمد صادق إسماعيل ،الجرائم الالكترونية دراسة قانونية قضائية مقارنة مع احدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية و الانترنت ،المركز القومي للإصدارات القانونية ،القاهرة ،الطبعة الأولى ، ،ص 40 – 41.

[2] عبد الصبور عبد القوي على مصري ،الجريمة الالكترونية ،دار العلوم للنشر و التوزيع ،القاهرة الطبعة الأولى 2008 ،ص 22.

[3] WWW.startimes.com الجرائم الالكترونية ، في 24أفريل2016،الساعة الثالثة.

بـل تعتمـد علـى الدراسـة الذهنيـة و التفكيـر العلمـي المـدروس القـائم علـى معرفـة تقنيـة بالحاسـب الآلي .[1]

4 –سهولة إخفاء الجريمة : فالجرائم الواقعة على الكمبيوتر أو بواسطته هي جرائم مخفية.

كمـا أن هـذه الجـرائم لا تتـرك أثـرا لهـا بعـد ارتكابهـا ،فليسـت هنـاك أمـوال أو مجـوهرات مفقـودة ،و إنما هي أرقام تتغير في السجلات .[2]

المطلب الثاني :أنواع الجرائم الالكترونية و مرتكبوها

أولا :أنواع الجرائم الالكترونية :

تعـددت أراء الدارسـين القـانونيين للجـرائم الالكترونيـة ، فهنـاك مـن يصـنفها بحسـب الفئـات مثـل جـرائم ترتكـب علـى نظـم الحاسـب الآلـي ،و جـرائم ترتكـب بواسـطته ،و هنـاك مـن يصـنفها بحسـب الأسلوب المتبع فيها .

و عموما يمكن تقسيمها إلى ثلاث أنواع رئيسية :

أ – الجرائم الخاصة بأمن المعطيات المعالجة أليا :

و هـي تتعلـق بالشخصـيات و البيانـات المتصـلة بالحيـاة الخاصـة ،و تشـمل جـرائم الاعتـداء علـى المعطيـات السـرية المحميـة قانونـا و غيـر المصـرح بتـداولها ،و المعلومـات و البيانـات التـي تمـس الخصوصية .

ب – الجرائم الخاصة بقيمة المعلومات و البيانات المعالجة أليا :

و هـــي تنقســـم بـــدورها إلـــى جـــرائم واقعـــة علـــى ذات المعلومـــات كجـــرائم الإتـــلاف و التشـــويه و التخريـب ،و السـطو علـى بـرامج الحاسـوب و قواعـد البيانـات ،و جـرائم أخـرى واقعـة علـى مـا تمثلـه

---

[1] صـغير يوسـف،الجريمة المرتكبـة عبـر الإنترنيـت ،رسـالة ماجيسـتر فـي القـانون الـدولي للأعمـال ،كليـة الحقـوق والعلوم السياسية ،تيزي وزو،2013،ص16 .

[2] د.عبد العال الديربي ،ا. محمد صادق إسماعيل ، المرجع السابق ،ص 55-57.

المعلومات و البيانات المعالجة أليا ،و التي تستهدف الحصول على مال غير شرعي عن طريق الغش و النصب و الاحتيال بالحاسب الآلي .

ج – جرائم متعلقة بحقوق الملكية الأدبية و الفكرية لبرامج الحاسوب و نظمه كجرائم قرصنة البرمجيات و الحاسب ،و تشمل نسخ البرامج و إعادة إنتاجها و تداولها بدون ترخيص ،و الاعتداء على العلامات التجارية و براءات الاختراع و كل ما يدخل ضمن إطار الملكية الفكرية [1] مثال على ذلك :قدر الاتحاد الأوربي للملكية الفكرية إجمالي الخسائر التجارية بسبب أعمال القرصنة في مصر على الكتب و المطبوعات و برامج الكمبيوتر و الأعمال الفنية بحوالي 5.84 مليون دولار .[2]

و فيما يلي تورد بعض أنواع الجرائم التي ترتكب عن طريق الانترنيت :

1- **قيادة الجماعات الإرهابية عن بعد** :إذ يمكن من خلال شبكة الانترنت بث الأفكار المتطرفة ،سواء كانت سياسية أو دينية و التي تسيطر على وجدان الأفراد و تفسد عقائدهم، و تستغل معاناتهم في تحقيق مآرب خاصة تتعارض مع مصلحة المجتمع.[3]

2- **السطو على أموال البنوك** :إن المصارف و البنوك هي الهدف المفضل لقراصنة الانترنت الذين يتلاعبون في كشوف و حسابات العملاء و نقل الأرصدة من حساب لأخر.

3- **أسلوب التجسس** : حيث يقوم قراصنة الحاسب الآلي باستخدام البرامج التي تتيح لهم ،الاطلاع على البيانات و المعلومات الخاصة بالشركات و المؤسسات التجارية العاملة على شبكة الانترنت و بالتالي يتمكنون من الحصول على ما يريدون من معلومات و منها تلك المتعلقة ببطاقات الدفع الالكتروني المستخدمة في التجارة الالكترونية عبر هذه الشبكة.

---

[1] . Eljaraimeliliktounia .BlogSpot .com في24 أفريل 2016،على الساعة الثالثة والنصف.

[2] www.startimes.com الجريمة الالكترونية .

[3] الشحات إبراهيم محمد منصور :الجرائم الالكترونية في الشريعة الإسلامية و القوانين الوضعية ،دار الفكر الجامعي ،الطبعة الأولى ،2011 ،ص 143.

4- **غسيل الأموال القذرة** :تعد شبكة الانترنت نوعا جديدا من التكنولوجيا الالكترونية التي تتعامل مع الأوراق النقدية و السماح بإيداع و انتقال أرصدة الأموال من شخص لأخر عبر الدول على مستوى العالم و دون الحاجة إلى المرور عبر البنوك ،مما يتيح لعصابات الجريمة المنظمة استخدامها في غسيل الأموال دون الوقوع في أيدي القائمين على تنفيذ القانون.[1]

5- **جرائم الاحتيال و السرقة** :و تشمل التلاعب بالمعطيات و النظم و استخدام الكمبيوتر للحصول على أو استخدام البطاقات المالية للغير دون ترخيص و الاختلاس عبر الكمبيوتر أو بواسطته و سرقة معلومات الكمبيوتر ، و قرصنة البرامج و سرقة أدوات التعريف و الهوية عبر انتحال هذه الصفات أو المعلومات داخل الكمبيوتر .

6- **جرائم التزوير** :و تشمل تزوير البريد الالكتروني ،الوثائق و السجلات و تزوير الهوية.

7- **جرائم المقامرة** :تشمل تملك و إدارة مشروع مقامرة على الانترنت و تسهيل مشاريع القمار ،و تشجيعها ،و استخدام الانترنت لترويج الكحول و مواد الإدمان للقصر. [2]

8- **الجرائم الجنسية** :تسهل الانترنت ارتكاب الجرائم ذات الصبغة الجنسية كما تتيح لمستخدميها مكنة تخطي القيود المحلية المفروضة عليهم ،و بالتالي يمكنهم الاطلاع على المواد التي فرضت الرقابة شروط معينة بالنسبة للحد الأدنى للسن المسموح له الاطلاع عليها ،كالأقلام التي لا يسمح بمشاهدتها إلا الكبار و أيضا الصور التي تحذف من المطبوعات و المشاهد المعروضة لتناولها موضوعات خارجة عن حدود القيم و التقاليد.[3]

كما تحرض القاصرين على أنشطة جنسية غير مشروعة ،إضافة إلى إغوائهم من أجل ارتكابها ،أيضا التحرش الجنسي بالقاصرين عبر الكمبيوتر و الوسائل التقنية ،و نشر و تسهيل المواد الفاحشة عبر الانترنت بوجه عام و للقاصرين تحديدا [4].

---

[1] **الشحات إبراهيم محمد منصور ،المرجع السابق ،ص 145.**

[2] **عبد الصبور عبد القوي علي مصري ،المرجع السابق ،ص 27-28.**

[3] **الشحات إبراهيم محمد منصور ،المرجع السابق ،ص147.**

[4] **عبد الصبور عبد القوي علي مصري ،المرجع السابق ،ص 26.**

10 – جريمة نشر و صناعة الفيروسات :الفيروس برنامج يكرر نفسه على نظام الكمبيوتر عن طريق دمج نفسه في البرامج الأخرى ،و هو قد يقضي على الكمبيوتر ،و قد يأتي في مختلف الأشكال و الأحجام ،و بعضها لا يسمى فيروسا مثل الدودة worms و أحصنة طروادة [1] و هذا الأخير يتمثل في إدخال أوامر على نحو غير مشروع إلى الكمبيوتر بهدف تحقيق أغراض إجرامية ،و عادة ما توجد برامج حصان طروادة في برامج الأعمال كبرامج معالجة النصوص و برامج إدارة قواعد البيانات.[2]

و الهدف من وراء انتشار صناعة الفيروسات و رواجها هو السطو و انتهاك و سرقة المعلومات المخزنة في قواعد و بنوك المعلومات ،بغرض التخريب و المتاجرة بها او استغلالها بطرق غير شرعية ،من خلال نقلها من الأجهزة المخزنة بها إلى أجهزة أخرى.[3]

ثانيا :أنواع الجناة في الجرائم الالكترونية

أما اعن مرتكبي الجرائم الالكترونية فيمكن تقسيمهم إلى 03 أنواع :

1- الموظفون العاملون بمراكز الكمبيوتر و هم يمثلون الغالبية العظمى من مرتكبي تلك الجرائم.

2- الموظفون الساخطون على مؤسساتهم و هم يقومون باستخدام الكمبيوتر لمسح بعض المعلومات الخاصة بالشركة أو المؤسسة.

3- الهاكرز أو كرا كرز الذين يستغلون الكمبيوتر من أجل التسلية لاستخدام شبكة الانترنت لتحقيق المزيد من الأرباح ،و نجد جماعة الجريمة المنظمة يسعون لاستخدامها لتنفيذ عمليات غير مشروعة و لعل التطور المستمر للانترنت و توفر السرية جعل من الانترنت جهازا مثاليا لتنفيذ الجرائم بعيدا عن أعين الأجهزة الأمنية.[4]

---

[1] **نفس المرجع ،ص 48.**

[2] **عبد العالي الديربي ،ا .محمد صادق إسماعيل ،المرجع السابق ،ص 80.**

[3] **Eljarime liliktounia .blog.spot.com.**

[4] **عبد الصبور عبد القوي علي مصري ،المرجع السابق ،ص 25.**

المبحث الثاني :مكافحة الجريمة الالكترونية و الصعوبات التي تعترضها

سعت مختلف الدول إلى مكافحة الجرائم الالكترونية نظرا لما خلفته من خسائر وأضرار وهذا على المستوى الدولي والمحلي وهو ما سنتعرض إليه في المطلب الأول، إلا أن هناك العديد من الصعوبات التي تعترض سبل مكافحة هذه الجريمة وهو ما سنناقشه من خلال المطلب الثاني.

المطلب الأول :مكافحة الجريمة الالكترونية

تعددت الجهود الدولية والإقليمية في سبيل مكافحة الجريمة الإلكترونية، وعلى الرغم من قلتها إلا أنها تعتبر هامة في هذا المجال، إضافة إلى الجهود التي بذلتها مختلف الدول في تشريعاتها الداخلية للحد من هذه الجريمة.

أولا: على المستوى الدولي والإقليمي.

1- جهود منظمة الأمم المتحدة: توصلت هذه الأخيرة في مؤتمرها الثامن حول منع الجريمة ومعاملة المجرمين إلى إصدار قرار خاص بالجرائم المتعلقة بالحاسوب، كما عقدت اتفاقية خاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية سنة 2000، أين أكدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، إضافة إلى ذلك عمدت اللجنة الاقتصادية والاجتماعية لغربي آسيا التابعة للمجلس الاقتصادي والاجتماعي على عقد ورشة عمل حول التشريعات السيبرانية وتطبيقها في منطقة الاسكوا عام 2008، أيضا عقدت منظم الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية بالبرازيل سنة 2010 ناقشت فيه الدول الأعضاء مختلف التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما في ذلك الجرائم الحاسوبية.[1]

2- المنظمة العالمية للملكية الفكرية: حيث اهتمت في مجال المعلومات بتوفير الحماية القانونية للبرامج المعلوماتية وقواعد البيانات، وذلك بواسطة الاتفاقيات العالمية خاصة "التربس"

[1] صغير يوسف، المرجع السابق،ص 93،94،95

و"برن" اللتان حثتا الدول الأعضاء على تطوير تشريعاتها خاصة تشريعات حق المؤلف، وأيضا وضع عقوبات على كل أعمال تزوير في العلامات التجارية والقرصنة المرتكبة في إطار تجاري.[1]

3-الاتحاد الأوروبي: و اقتناعا بالحاجة إلى تحقيق سياسة جنائية تم توقيع الاتفاقية الأوربية بشأن جرائم الكمبيوتر بتاريخ 2001/11/23 بغرض حماية المجتمع الأوربي من جرائم الكمبيوتر و ذلك من خلال التقريب بين التشريعات القانونية الجزائية و تمكين وسائل التحقيق الفعالة فيما يتعلق بهذه الجرائم ،و فتح الباب أمام اكبر عدد ممكن من الدول لكي تصبح أطرافا في الاتفاقية.[2]

ثانيا: على المستوى العربي.

تعتبر مصر من أوائل الدول الحريصة على محاربة الجرائم الالكترونية حيث قامت وزارة الداخلية بإنشاء إدارة خاصة لمكافحة جرائم شبكات حواسيب النظم المعلوماتية و تختص الإدارة بالمتابعة اليومية للشبكات العاملة لضبط الحالات الخارجة عن القانون ،و حسبما أكد المسؤولون أن هذه الإجراءات تتخذ فور اتجاه المخالفين و يتم تدمير المواقع إذا ثبت إضرارها بمصلحة الأمن القومي أو الآداب العامة.[3]

كما أعلنت السلطات المختصة بالمملكة العربية السعودية أنها ستفرض عقوبات بالحبس لمدة عام واحد و غرامات لا تزيد عن 500 ألف ريال لجرائم القرصنة المرتبطة بالانترنت و إساءة استخدام كاميرات الهواتف المحمولة ،كما أصدرت المملكة تشريعا وطنيا في هذا الخصوص مؤخرا تحت مسمى نظام مكافحة جرائم المعلوماتية ،الذي أصبح قيد التطبيق ،كما اقترح الباحثون إنشاء شرطة معينة بالمعلومات و الانترنت في السعودية تسمى شرطة الانترنت تهتم بتطهير الانترنت و حجب المواقع الإرهابية و المواقع الضارة على المجتمع.[4]

ثالثا: على المستوى الداخلي

---

[1] **صغير يوسف، المرجع السابق،ص 98**

[2] **د.عبد العال الديربي ،احمد صادق إسماعيل ،المرجع السابق ، ص 204.**

[3] **Eljarime liliktounia .blog.spot.com**.

[4] **د.عبد العال الديربي، أ محمد صادق إسماعيل،نفس المرجع،ص125-128.**

واكب المشرع الجزائري مختلف التطورات التشريعية التي تم سنها من أجل تنظيم المعاملات التي تتم من خلال الوسائط الإلكترونية، خاصة التي تهدف إلى الحد من الاستخدام غير المشروع لها، وتجلى ذلك من خلال المحاولات التالية:

1- مكافحة الجريمة المرتكبة عبر الإنترنت في قوانين الملكية الأدبية والفنية: اتجه المشرع الجزائري إلى الاعتراف صراحة بوصف المصنف المحمي لمصنفات الإعلام الآلي، وذلك من خلال تعديله للأمر 73-14 بموجب الأمر 97-10 المتعلق بحق المؤلف والحقوق المجاورة، حيث واكب المشرع التطورات الحاصلة في المجال المعلوماتي بأن أخضع المعلوماتية لقانون الملكية الفكرية موسعا بذلك من سلطة القاضي في تقرير العقوبة، وذلك ضمانا وحماية لحق المؤلف ومالك الحق المجاور.

2- مكافحة الجريمة المرتكبة عبر الإنترنت في قانون العقوبات: تدارك المشرع ولو نسبيا الفراغ القانوني في مجال الإجرام المعلوماتي بموجب القانون 04-15 المتضمن تعديل قانون العقوبات حيث جرم بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات وهي جريمة التوصل أو الدخول غير المصرح به، جريمة التزوير المعلوماتي، جريمة الاستيلاء على المعطيات، جريمة إتلاف وتدمير المعطيات، جريمة الاحتيال المعلوماتي، أنشطة الإنترنت المجسدة لجرائم المحتوى الضار والتصرف غير القانوني. [1]

و مع ازدياد رقعة استخدام وسائل الإعلام التقنية الحديثة و تعدد أشكال الجرائم الالكترونية في بلادنا سن المشرع الجزائري قانون للحد من الجرائم الالكترونية ،و زكى هذا المسعى مؤتمر أوراق العمل الوطني الأول في 2008/03/28 المنعقد بعين الدفلى ،و الذي تبنى دراسة توحي بتشريع يعاقب مجرمي الانترنت.

كما تسعى السلطات الأمنية الجزائرية إلى الاستعانة بالمرصد الفرنسي لمتابعة جرائم الانترنت من خلال إيجاد مرصد جزائري شبيه للتحكم في هذه الجرائم و فرض غرامات.

و يشار بأن بعثات من الدرك و الشرطة أرسلت إلى عواصم عدة لتلقي دورات تدريبية لتولي مهمة تطبيق القانون المرتقب .كما صادق مجلس الوزراء بالجزائر مؤخرا على مشروع قانون

[1] صغير يوسف، المرجع السابق،ص 103،110

مكافحة الجرائم الالكترونية الذي ينص على حملة إجراءات تحدد آليات الرقابة على الانترنت و محاربة الجنح المرتبطة بالشبكة الافتراضية ،كما يفرض دفتر الشروط و رخص جديدة لممولي الانترنت و إلزام هذه الشركات بالحفاظ على المراسلات الالكترونية لمدة سنة ،كما ستجبر مقاهي الانترنت على التجهيز بكاميرات مراقبة إضافة إلى حملات تفتيش تقوم بها مصالح الأمن[1].

المطلب الثاني: صعوبات مكافحة الجريمة الإلكترونية

رغم الجهود المبذولة للحد من الجرائم الإلكترونية إلا أن هذه الجهود تصطدم بعدة صعوبات وعراقيل تتمثل فيمايلي:

أولا: صعوبة اكتشاف الجريمة الإلكترونية.

ويرجع ذلك إلى عدة اعتبارات:

1- فقدان الآثار التقليدية للجريمة فهذه الجرائم لا تخلف آثارا مادية كتلك التي تخلفها الجريمة العادية حيث أنها تتم دون أن يشعر بها القائمون على تشغيل الأجهزة المعلوماتية .

2- فرض الجناة لتدابير أمنية حيث يعمدون إلى إخفاء جرائمهم وإزالة آثارها عن طريق التلاعب بقواعد البيانات والقوائم في جهاز الكمبيوتر والبرامج، كما قد يقوم هؤلاء المجرمين بإخفاء هويتهم أو انتحال شخصية أخرى حتى لا يمكن التعرف عليهم في حالة اكتشاف الجريمة.

3- التكتم عليها من قبل الجهات المجني عليها والتي غالبا ما تكون مصرف أو مؤسسة مالية، وهذا لتوقي الخسائر التي يتوقع تحققها نتيجة هذا الإبلاغ بسبب نقص ثقة العملاء في هذه المؤسسات.

4- نقص خبرة سلطات الاستدلال حيث تواجه عملية استخلاص الدليل في الجريمة الإلكترونية نقص الخبرة لدى رجال الضبط القضائي أو أجهزة الأمن بصفة عامة، وكذلك لدى أجهزة

---

[1] الجرائم الالكترونية www.startimes.com.

العدالة الجنائية، وذلك فيما يتعلق بثقافة الحاسب الآلي والإلمام بعناصر الجريمة الإلكترونية وكيفية التعامل معها وهذا في البلدان العربية لأن تجربتها في مجال الاعتماد على الحاسب الآلي جاء متأخرا عن الدول المتقدمة. [1]

ثانيا: الإثبات في الجرائم الإلكترونية.

تتسم هذه الجرائم بأنها غير مرئية في العديد من حالاتها إذ تعتمد التعاملات فيها على نبضات الكترونية لا يمكن قراءتها إلا بواسطة الحاسوب، والبيانات التي يمكن استخدامها ضد الفاعل يمكن محوها في لمح البصر.

ومن هنا نجد معوقات خاصة بأدلة الجريمة منها:

1- انعدام الدليل المرئي.

2- سهولة محو الدليل أو تدميره في فترة زمنية يسيرة.

3- صعوبة الوصول إلى الدليل.

4- مكان ارتكاب الجريمة والذي يكون عن بعد حيث لا يتواجد الفاعل في مسرح الجريمة، ومن ثمة تباعد المسافات بين الفعل والنتيجة، وهذه المسافات قد تمتد إلى النطاق الإقليمي لدولة أخرى مما يضاعف صعوبة كشفها. [2]

وعموما هناك بعض التدابير التي يمكن اتخاذها لتفادي وقوع الجرائم الإلكترونية تتمثل في الآتي:

- رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الانترنت إذ يستلزم التدخل الحكومي و الدولي نظرا للخطورة الجسيمة للأمر.

- الاعتماد على أساليب و تقنيات متطورة ،للتمكن من الكشف عن هوية مرتكب الجريمة و الاستدلال عليه بأقل وقت ممكن.

---

[1] **صغير يوسف،المرجع السابق، 116،121**

[2] **د الشحات ابراهيم محمد منصور ،المرجع السابق،ص 191،193.**

- الحرص على الحفاظ على سرية المعلومات الخاصة بالعناوين الالكترونية كالحسابات البنكية ،و البطاقات الائتمانية و غيرها.

- عدم الكشف عن كلمة السر نهائيا و تغييرها بشكل مستمر و اختيار كلمات سر صعبة.

- تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي و أجهزة الحاسوب .

- تجنب تحميل أي برنامج مجهول المصدر .

- استمرارية تحديث برامج الحماية الخاصة بأجهزة الحاسوب .

- تأسيس منظمة خاصة لمكافحة الجرائم الالكترونية و الحد منها .

- المسارعة في الإبلاغ للجهات الأمنية فور التعرض لجريمة الكترونية.

- مواظبة التطورات المرتبطة بالجريمة الالكترونية و الحرص على تطوير وسائل مكافحتها .

- الحرص على استخدام كلمات سرية للوصول إلى البرامج الموجودة على جهاز الحاسوب.

- عدم ترك جهاز الحاسوب مفتوحا.

- فصل اتصال جهاز الحاسوب بشبكة الانترنت في حال عدم الاستخدام.

- إعداد حملة موسعة لنشر الوعي الثقافي بين الشباب من الجنسين و توفير عدد من البرامج التدريبية لتفعيل استخداماتهم في مجال يعود بالنفع عليهم و على أمتهم

خاتمة :

إن الجريمة الالكترونية ليست حكرا على بعض الدول دون الآخر إذ أن الواقع الذي يفرضه التقدم التكنولوجي يؤكد أن هذه الجريمة آخذة في الانتشار في ربوع الأرض ، و لهذا نجد ثمة جهودا كبيرة تبذل لمحاربتها بكافة أشكالها ،و لكن نظرا لما تتميز به هذه الجرائم من ميزات جعل من الصعب الكشف عنها و تحديد الدليل المادي الذي يدين مرتكبها ،لذلك يتوقع أن يستمر هذا النوع من الجرائم و يتطور مع مرور الوقت إلى ما هو اخطر و اعقد .وعلى هذا فإن وجود إستراتيجية فعالة لدى الدول تحارب هذه الجرائم هي الوسيلة الضامنة لتقليلها و محاولة التحكم بها دون أن ننسى دور الأفراد في محاربتها عن طريق تبصيرهم بايجابيات و سلبيات استخدام الانترنت.

قائمة المراجع:

أولا: الكتب

1- الشحات محمد ابراهيم منصور: الجرام الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، دار الفكر الجامعي، الطبعة لأولى، 2011.

2- عبد الصبور عبد القوي علي مصري: الجريمة الإلكترونية، دار العلوم للنشر والتوزيع، القاهرة، الطبعة الأولى، 2008.

3- عبد العال الديربي، محمد صادق اسماعيل: الجرائم الإلكترونية دراسة قانونية قضائية مقارنة، المركز القومي للاصدارات القانونية، الطبعة الأولى، 2012.

4- محمد علي العريان: الجرائم المعلوماتية، دار الجامعة الجديدة للنشر،الإسكندرية، 2004.

ثانيا: الرسائل الجامعية

1- صغير يوسف: الجريمة المرتكبة عبر الإنترنت، رسالة ماجيستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، تيزي وزو،2013

ثالثا: المواقع الإلكترونية

www.startimes.com consulté à 24 avril à 15 :00

www.eldjarimeiliktounia.blospot.com consulté à 24 avril à 15 :30