آليات وسبل مكافحة الجريمة الإلكترونية

ليندة بوسيف
أستاذة باحثة
المدرسة الوطنية العليا للصحافة وعلوم الإعلام

الكلمات المفتاحية: الجريمة، الجرم الإلكتروني، سمات الجريمة الإلكترونية، أنواع الجرم الإلكتروني، الوسائل الإلكترونية، طرق الوقاية من الجرائم الإلكترونية.

Le Résumé

Avec l'avènement d'internet qui permet à chacun un accès libre et sans aucune entrave et cela grâce à la croissance incessante de la révolution numérique.

Nous sommes devenus confrontés à de multiples problèmes et dangers**,** découlant naturellement de tout développement civilisationnel ou avancée technique, source de plusieurs phénomènes, telle la cybercriminalité qui a pris une ampleur majeure, mettant même en péril la sécurité nationale de certaines nations.

Cela étant, l'obligation de sévie contre l'émergence de plusieurs délits liés à ce phénomène est indispensable, nécessitant même la mise en place d'un arsenal juridique adéquat avec ces nouveaux fléaux aussi inouïs qu'étranges.

La sensibilisation contre la cybercriminalité et ses dangers est également incontournable d'où cet article relatant sa nature, les raisons de sa propagation et la manière d'y prévenir ces phénomènes numériques.

المقدمة:

في ظل التطور الحاصل الذي تشهده الثورة المعلوماتية والالكترونية والانتشار الواسع للشبكة العنكبوتية وفتح أبوابها التي كانت مغلقة عن المعلومة وكشف ستار أحداثها، دق ناقوس الخطر على هذه الشبكة حيث اصبحت دون حارس وبدون قيود أو حدود لردع الاعمال السيئة التي كانت ولا زالت مصدرها البشر.

وكنتيجة لهذا الانتشار الحاصل في مجال العلوم والاكتشافات التقنية، ظهر بما أصطلح بالجرائم الالكترونية التي أتت لتنبه المجتمعات على عظيم خطرها، فظهر محترفوها ينهبون ويخربون ويهددون أمن دول عديدة.

مما ادى بهذه الدول إلى أخذ موقف صارم للحد من هذه الظاهرة الخطيرة، فتوجب عليهم معرفة ماهية الجريمة الالكترونية، وما هو الغرض من انتشارها وكيفية الوقاية منها.

لهذا وجب علينا طرح الانشغال التالي:

ما هي الآليات والسبل التي يمكن استغلالها من أجل التصدي للجريمة الالكترونية ؟

نحن نعلم أن كل نشاط يقام بطريقة غير مشروعة وغير قانونية يعتبر جريمة، إذن فهو عمل مخالف للقوانين العرفية والوضعية المتعارف عليها والمعمول بها.

عبر مختلف دول العالم، هذا النشاط غذا استخدمت فيه وسائط تقنية علمية أصبح الفعل جريمة الكرتونية.

فما هي الجريمة الالكترونية ؟

تعتبر الجريمة الالكترونية ذلك السلوك الغير مشروع المتعلق بالمعالجة الآلية للبيانات ونقلها كون التقنية فيها تكون إما وسيلة تستخدم في ارتكاب الفعل أو البيئة والوسط الذي يحدث فيه الجرم، وأن يكون الهدف أو الغاية لارتكاب الفعل المجرم[1] أي أن الوسيط يكون آلة تقنية كجهاز كمبيوتر من خلال الاتصال بالأنترانت ويكون هدفها اختراق الشبكات أو تخريبها أو التحريف أو التزويد أو السرقة أو الاختلاس. ويشمل السلوك الانحرافي في جريمة بأركانها المادية والمعنوية ولا عبره فيها بالباعث على ارتكابها[2] . فهي متعلقة كذلك ببعض الأجهزة التقنية الأخرى كالجيل الثالث للهواتف النقالة واستخدام الانترانت فيها الذي حول العالم إلى قرية صغيرة باعتباره وسيلة اتصال عالمية تعتمد على برامج معلوماتية حديثة في ضبط مختلف البيانات والمعطيات المعلوماتية الدقيقة.

فالجريمة الالكترونية إذن هي كل فعل ضار يأتيه الفرد أو الجماعة عبر استعماله لأجهزة الكترونية، ويكون لهذا الفعل اثر ضار على غيره من الافراد[3] فهي إذن تستهدف القضاء على التكنولوجيا الحديثة عبر الوسائط الالكترونية، ومع غزو الانترنت دول العالم اصبح من الصعوبة ضبط مكان وكشف هذه الجرائم.

نظرا لكونها عابرة للحدود لادين ولا وطن لها، وتتم بسرعة فائقة دون رقيب أو حسيب ودون رقابة من أي دولة مما أدى إلى ارتكاب كافة صور النشاط الإجرامي المتعارف عليها عبر الانترانت حتى القتل، والدليل عن ذلك الرجوع إلى مؤلفتا الجريمة الالكترونية السطو على برامج الحاسوب بغرض سرقة البيانات وقاعدة المعطيات المعلوماتية حتى السرية منها واستخدامها في التجسس أو تلك المتعلقة بالقرصنة والسطو على الأموال إلى جانب ظهور ما اصطلح عليه بالإرهاب الالكتروني وتهديد الأمن القومي للدول، وكذا جرائم الآداب العامة والمساس بالأخلاق من خلال الإباحية الالكترونية التي تجسدها المواقع الجنسية الإباحية.

جل النظريات والدراسات المنجزة تتفق حول نقطة اساسية تتمثل في الغاية المادية البحتة التي يسعى إلى تحقيقها المجرم الالكتروني، من سطو على الأموال، إلى الاعتداء على البيانات السرية وتدمير البرامج المعلوماتية لأية

دولة لتهديدها في أمنها القومي وسلامة أراضيها ولعل أبرز مثال على ذلك اقتحام موقع وزارة الدفاع الأمريكي، لتعود في صورة حديثة على شاكلة ما يعرف بإرهاب المستقبل الذي اصبح هاجسا حقيقيا يهدد سلامة وأمن المجتمع الدولي، عن طريق التهديد بتدمير اساليب وإستراتيجية الدفاعات الامنية والاقتصادية للدول وعوائدها المالية باستخدام الخطط التخريبية والفيروسات لتدمير مختلف البرامج المعلوماتية وإتلاف مختلف البيانات الخاصة بتقنية الرقمية في حفظ وتخزين البرامج المعلوماتية لأية دولة ومهما كانت درجة سريتها[4].

سمات الجريمة الالكترونية :

إن الجريمة الالكترونية تتسم بعدة سمات تجعل من الصعوبة التنبؤ بها سواء مكانيا أو زمانيا، وكذلك عدم معرفة مرتكبها ويمكن تحديد البعض منها فيما يلي:

1- سهولة ارتكاب الجريمة بعيدا عن الرقابة الأمنية.
2- تنطوي على سلوكيات غير مألوفة في المجتمع.
3- سهولة إتلاف الادلة من قبل الجناة.
4- صعوبة التحكم في تحديد حجم الضرر الناجم عنها قياسا بالجرائم التقليدية.
5- كون مرتكبها من بين فئات متعددة يجعل التنبؤ بهم أمرا صعبا[5].

6- جريمة عابرة للحدود لا تعترف بعنصر المكان ولا الزمان فهي تتميز بالتباعد الجغرافي، واختلاف التوقيت بين الجاني والمجني عليه.

من الواضح اننا أمام جريمة معقدة وخطيرة، والثورة الرقمية الهائلة ساعدت المجرم كثيرا، سواء بالتخفي وغيابه عن مسرح الجريمة منذ البداية، أو عدم ترك أي أثر يقودنا إلى معرفته ومعرفة أنواع جرائمه.

فما هي تصنيفات وأنواع الجرائم الالكترونية ؟

تصنيفات وأنوع الجرائم الالكترونية :

تنقسم الجرائم الالكترونية حسب ما يلي :[6]

1) تقسيم الجرائم حسب دور الحاسوب في الجريمة

أولا : الجرائم التي تستهدف عناصر (السرية والسلامة ووفرة المعطيات والنظم)

- الدخول غير القانوني (غير المصرح به)، حيث يقوم الشخص باختراق الشبكات والحواسيب التي ترتبط بشبكة الانترنت، وذلك باختراق نظام الأمن في الشبكة و الدخول إلى الجهاز والكشف عن محتوياته.
- الاعتراض غير القانوني.
- تدمير المعطيات (يكون هذا الأمر بعد اختراق الشبكة وقيام الشخص بمسح البيانات أو تشويهها أو تعطيل البرامج المخزنة وجعلها غير قابلة للاستخدام.

- اعتراض النظم.
- اساءة استخدام الأجهزة.

ثانيا : الجرائم المرتبطة بالحاسوب وتضم:

- التزوير المرتبط بالحاسوب.
- الاحتيال المرتبط بالحاسوب.

ثالثا : الجرائم المرتبطة بالمحتوى، وتضم طائفة واحدة وفق هذه الاتفاقية، وهي الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية.

رابعا : الجرائم المرتبطة بالإخلال بحق المؤلف وقرصنة البرمجيات.

2) تقسيم الجرائم الالكترونية حسب نوع المعطيات ومكان الجريمة، ونجد فيه :

1- الجرائم التي تمس بقسمة معطيات الحاسوب.
2- الجرائم التي تمس بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة.
3- الجرائم التي تمس بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (جرائم قرصنة البرمجيات).

3) تقسيم الجرائم الالكترونية حسب الأشخاص والأموال ويضم هذا التقسيم طائفتين مهمتين وهما:

1- الجرائم غير الجنسية التي تستهدف الاشخاص.
2- الجرائم الجنسية وتشمل القتل بالحاسوب.

أما الطائفة الثانية وتضم جرائم الأموال وكذلك :

- جرائم الاحتيال والسرقةFraud and theft crimes
- جرائم المقامرة Gambling
- جرائم التزوير crimes of fraud
- جرائم الحاسوب المضادة للحكومة.

أنواع المجرمين من مرتكبي الجرائم الالكترونية :

- إما يكونوا مجرمين محترفين.
- إما أن يكونوا من الهواة، ويطلق عليهم صغار نوابغ الكمبيوتر.

خصائص المجرم الالكتروني :

يتميز المجرم الالكتروني بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين وهي[7] :

1- المهارة :

لا بد أن يتمتع المجرم بقدر كبير من المهارة التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في المجال التكنولوجي، او بمجرد التفاعل الاجتماعي مع الآخرين، وهذه ليست قاعدة في أن يكون للمجرم الالكتروني كل هذا القدر من العلم وهذا ما أثبته الواقع العلمي أن جانب من أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب هذا النوع من الجرائم.

2- المعرفة :

يمكن للمجرم الالكتروني أن يكون تصورا كاملا لجريمته ويرجع ذلك إلى أن الذي تمارس فيه الجريمة الالكترونية هو نظام الحاسب الأولى، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة وذلك قبل تنفيذ الجريمة.

3- الوسيلة:

ويراد بها الإمكانيات التي يحتاجها المجرم الالكتروني لإتمام جريمته.

4- السلطة :

وتتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات وأيضا قد تكون السلطة عبارة عن حق الجاني في الدخول إلى الحاسب الآلي وإجراء المعاملات، كما أن السلطة قد تكون شرعية وغير شرعية في حالة سرقة شفرة الدخول الخاصة بشخص آخر.

الأسباب الدافعة لارتكاب الجرائم الالكترونية [8] :

1- الولع في جميع المعلومات وتعلمها.
2- حب المغامرة والإثارة.
3- دوافع الشخصية: فغالبا ما يرتكب المبرمج جرائم الكترونية نتيجة إحساسه بالقوة والذات، وبقدرته على اقتحام النظام فيندفع تحت تأثير الرغبة القوية في تحقيق الذات.
4- تحقيق مكاسب مالية.

5- الفضول لدى الكثيرين.

6- صعوبة اكتشاف الدليل الرقمي.

الصعوبات والمشكلات العلمية والإجرائية للحد من الجريمة الالكترونية:

1- صعوبة إثبات وقوع الجريمة.

2- صعوبة تحديد المسؤول جنائيا عن الفعل الإجرامي.

3- صعوبة إلحاق العقوبة بالجاني المقيم بالخارج.

4- صعوبة التواصل إلى الجاني.

5- القصور في القوانين الجنائية القائمة.

6- افتراض العلم بقانون جميع دول العالم.

مكافحة الجرائم الالكترونية :

للحد من الجرائم الالكترونية لابد على جل الدول والافراد المساهمة قدر الإمكان للتصدي لها وهذا عن طريق[9]:

1- الاستدلال الذي يتضمن التفتيش والمعاينة والخبرة التي تعود إلى خصوصية الجريمة الالكترونية عبر الانترنت.

2- تقديم الجهود الدولية والداخلية لتجسيد القوانين للوقاية من هذه الجريمة المستحدثة، فأما الدولية فتتمثل في جهود الهيئات والمنظمات الدولية والتي تتمثل في :

- توعية الناس لمفهوم الجريمة الالكترونية وأنه الخطر القائم ويجب مواجهته والحرص على ألا يقعوا ضحية له.
- ضرورة التأكد من العنوانية الالكترونية التي تتطلب معلومات سرية خاصة كبطاقة ائتمانية أو حساب بنكي.
- عدم الافصاح عن كلمة السر لأي شخص والحرص على تحديثها بشكل دوري واختيار كلمة السر غير مألوفة.
- عدم حفظ الصور الشخصية في الكمبيوتر.
- عدم تنزيل أي ملف او برنامج من مصادر غير معروفة.
- الحرص على تحديث أنظمة الحماية مثل استخدام برامج الحماية مثل MacafeeNorton ..... إلخ.
- تكوبن منظمة لمكافحة الجريمة الالكترونية.
- تتبع تطورات الجريمة الالكترونية وتطوير الرسائل والأجهزة والتشريعات لمكافحتها.
- تطوير برمجيات آمنة ونظم تشغيل قوية التي تحد من الاختراقات الالكترونية وبرمجيات الفيروسات وبرامج التجسس مثل: مضادات التجسس وهي

برامج تقوم بمسح الحاسب للبحث عن مكونات التجسس وإلغائها مثل : Lavasoft.

خاتمة :

في ظل التطورات الكثيرة في مجال العلوم واستحداثها، تطورت أدوات وسبل الجريمة الالكترونية بشكل أكثر تعقيدا وأشد ضررا فقد مست مختلف المجالات الاجتماعية والاقتصادية والسياسية، لذا يأت لزاما وضع الحلول الجذرية لمعالجة هذه الظاهرة التي هي وليدة هذا التطور والحد من تفشيها في الأوساط المجتمعية، ولا يمكن الشروع بذلك بغياب القوانين الرادعة لتطبيق الأحكام المشرعة ضد المنفدية، وقبل هذا كله تفعيل أساليب التوعية و التهذيب لدى مستخدمي شبكة الاتصالات العالمية (الانترنت) وحثهم على استخدام الأمثل لهذه التقنيات والتي من المفترض وجدت لخدمة الإنسان وليس لمضرته.

الهوامش :

1عبد الصبور عبد القوي، الجريمة الالكترونية والجهود الدولية. دار النشر والتوزيع المصرية، ط1 ،مصر 2011.

2 يونس خالد عرب مصطفى : جرائم الحاسوب، دراسة مقارنة، رسالة ماجيستر مقدمة إلى الجامعة الاردنية 1994.

3 أمير فرج يوسف : الجرائم المعلوماتية على شبكة الانترنت دار المطبوعات الجامعية الإسكندرية 2001.

4 منيرة بنت فهد الحمدان، الجرائم الإلكترونية، عندما تصبح التقنية وسيلة للإجرام، دار الجزيرة، الأردن، 2007، ص 65.

5DR.Francillon les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France REV . Int pen 1999. Vol 64 p 296.

6 مقالات أمن المعلومات – الكاتبة – سمية بنت عبد الرحمن بنت سليمان الحمدات.

الجريمة الالكترونية للمؤلف. مصطفى عمارة، مجلة المعلوماتية العدد 29 شهر تموز 2012.

7 رماح الدلمقوني، أنواع الجرائم الإلكترونية، دار الموجز، البحرين، 2017، ص 38.

8 منى الأشقر، القانون والأنترنت، تحدي وتكييف الضبط، بيروت، ص 70.

9 أمير فرج يوسف : الجرائم المعلوماتية على شبكة الانترنت ط1،دار المطبوعات الجامعية الإسكندرية 2001.