خصائص الجريمة الإلكترونية ومجالات استخدامها

تاريخ استلام المقال: 2017/10/05 تاريخ قبول المقال للنشر 2018/01/10

د/ رحموني محمد أستاذ محاضر (أ)
جامعة أحمد دراية – أدرار
البريد الالكتروني: ramouni4@yahoo.fr

ملخص:

مما لاشك فيه أن تطور وسائل الاتصال الإلكتروني بمختلف أنواعه صاحبه تطور في الجريمة يتماشى وهذا التطور التكنولوجي، وبذلك أصبحت الجريمة الإلكترونية لا تقل خطورة عن الجريمة العادية، إذ تعد جريمة ذات طابع خاص تستهدف معنويات وليست ماديات محسوسة، إلا أن آثارها قد تكون معنوية، كما تكون مادية محسوسة أيضاً.

وتتشابه الجريمة الإلكترونية مع الجريمة التقليدية في أطراف الجريمة، وتختلف عنها في أداة ومكان الجريمة، حيث أن الأداة في الجريمة الإلكترونية عالية التقنية، والمجرم في الجريمة الإلكترونية لا يحتاج إلى التنقل الحركي لمكان وقوع الجريمة، بل يقوم بالفعل الإجرامي عن بعد باستخدام خطوط وشبكات الاتصال، وبالتالي فإن هذه الجريمة أضحى خطرها يطال أمن الأفراد والأموال والبلاد.

الكلمات المفتاحية:

الجريمة الكترونية، أنظمة المعالجة الآلية للمعطيات، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، جرائم عابرة للحدود، مهارة وتقنية، المعاملات المالية، الاحتيال، تحويل، غسيل، إرهاب، تجسس، جريمة منظمة.

Abstract

Obviously, the development of electronic means of communication of various types has been accompanied by an evolution in crime which goes in line with this technological development. Electronic crimes are no less serious than ordinary crimes. Electronic crimes are both similar to traditional crimes and differs from it in the tool and place. The tool in cybercrime is

highly technical and the cybercrime does not require the physical mobility to the crime scene.

مقدمة:

غير خاف أن التطور المستمر لوسائل الاتصال والتواصل الإلكتروني بشتى أنواعه ووسائله صاحبه تطور في الجريمة أيضاً، حيث أصبحت الجريمة تتمشى وفق التطور التكنولوجي وتستغله، فظهرت الجريمة الإلكترونية التي لا تقل خطورة عن الجريمة العادية، فهي جريمة ذات طابع خاص تستهدف معنويات وليست ماديات محسوسة، إلا أن آثارها قد تكون معنوية، كما تكون مادية محسوسة أيضاً.

فهذه الجريمة بطبيعتها مخالفة لنظام المجتمع حيث ترتكب ضد أفراد أو جماعات بدافع جرمي و نية الإساءة لسمعة الضحية أو لجسدها أو عقليتها، سواءً كان ذلك بطريقة مباشرة أو غير مباشرة، و أن يتم ذلك بواسطة الكومبيوتر واستخدام وسائل الاتصالات الحديثة مثل الإنترنت (وغيرها من مستجدات تطور الاتصال الالكتروني التكنولوجي.

ومن حيث الأساس فإن الجريمة الإلكترونية تتشابه مع الجريمة التقليدية في أطـــراف الجريمة من مجرم ذي نزعة لارتكاب الجريمة[1]، وضحية الذي قد يكون شخـــص طبيـــعي أو معنوي، إلا أن الاختلاف يتجلى في أداة ومكان الجريمـة، وهنـا يكمـن الاختـلاف بـين الجريمـة العاديـة التقليديـة والجريمـة الإلكترونية، حيث تكون الأداة في الجريمة الإلكتـــرونية عالية التقـــنية، كما أن المجرم لا يحتاج إلى التنقل الحركي لمكان وقوع الجريمة، بل يقوم بالفعل الإجرامي عن بعد –من حيث الزمان والمكان– باستخدام خطوط وشبكات الاتصال بين الجاني ومكان وقوع الجريمة.

[1] - مع الوضع في الحسبان أن المجرم الإلكتروني يتميز بجملة من الصفات تختلف عن المجرم العادي في الجرائم التقليدية العادية.

والجدير بالذكر، أن التعرض لمفهوم وتعريف الجريمة الإلكترونية وخصائصها يعد أمر ذا أهمية بالغة، وهذا بالنظر لما تنطوي عليه هذه الجريمة من مخاطر اقتصادية وأمنية واجتماعية والثقافية.

ومن هذا المنطلق نطرح تساؤلا مفاده: ما المقصود بالجريمة الإلكترونية؟ وما مجالات استخدامها؟ ذلك ما تحاول هذه الدراسة الإجابة عنه من خلال مطلبين؛ الأول منهم يعالج مفهوم الجريمة الإلكترونية وخصائصها، أما الثاني فيتعرض إلى المجال الذي تحويه هذه الجريمة.

المطلب الأول: تعريف الجريمة الإلكترونية وخصائصها

مما لا شك فيه أن الجريمة بالمفهوم الوسع تعني كل مخالفة لقاعدة من القواعد تنظم سلوك الإنسان في الجماعة، أو هي سلوك إجرامي من خلال ارتكاب فعل يجرمه القانون، أو الامتناع عن فعل أمر به القانون، وعلى العموم فالجريمة هي ذلك السلوك المضاد للمجتمع والذي يضر بصالحه، هذا بوجه عام، فإذا ما تم هذا النشاط أو الفعل بواسطة الوسائل التكنولوجية الحديثة الممثلة في الكمبيوتر وباستخدام شبكات الاتصال الإلكترونية عبر وسائط تقنية علمية يمكن وصف النشاط أو الفعل حينئذ بالجريمة الإلكترونية، وقد أخذ تحديد مفهوم الجريمة الالكترونية زخما واسعا، كما أن هذه الجريمة تتصف بجملة من الخصائص، ذلك ما تتعرض إليه الدراسة في النقاط الجزئية التالية:

الفرع الأول:تعريف الجريمة الإلكترونية

للوقوف على مفهوم الجريمة الإلكترونية يقتضي منا الحال التعرض إلى التعريف الفقهي لهذه الجريمة (أولاً)، ومن ثم تبيان التعريف التشريعي (ثانياً).

أولاً: التعريف الفقهي للجريمة الإلكترونية

لم يتوصل الفقه إلى تعريف جامع مانع للجريمة الإلكترونية، وبالتالي تعددت التعريفات بشأنها وفق المنظور الذي تبناه الفقيه، في هذا الإطـــار يشير

الفـقيه " فان دير هلست وونيف" إلى أن:((هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة ... وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية وكلها تعكس فجوات مهمة في التعريف[1].))

ويعزى تباين التعريفات بشأن الجريمة الإلكترونية بالنظر إلى الزاوية التي تبناها الفقيه، فهناك جانب من الفقه يرى تعريفها بالنظر إلى وسيلة ارتكابها أو موضوعها أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها أو استنادا لمعايير أخرى حسب القائلين بها[2]، كما يعتمد في تعريفها على العناصر المتصلة بآليات ارتكابها أو بيئة ارتكابها أو صفات مرتكبيها، ذلك ما نبينه في الآتي:

1- تعريفات تقوم على موضوع الجريمة أو نمط السلوك محل التجريم:

تعرف الجريمة الإلكترونية في هذا الإطار على أنها: " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه[3]." وتضيف هدى قشقوش للتعريف السابق- وهذا ما تبناه أشهر فقهاء هذا الاتجاه مثل الفقيه Rosenblatt- طابع السلوك غير المشروع في الجريمة الإلكترونية بقولها: " كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات[4]." وتعرف الجريمة الإلكترونية أيضاً بأنها "نمط من أنماط الجرائم المدونة في

1 - محمد حجازي، جرائم الحاسبات والانترنت (الجرائم المعلوماتية)، المركز المصري للملكية الفكرية، القاهرة، مصر، 2005، ص 08.

2 - عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت ، دار الفكر الجامعي، مصر، طبعة 2009، ص 12.

3 - محروس نصار غايب، الجريمة المعلوماتية، مقال منشور على الموقع الإلكتروني، www.iasj.net/iasj?func=fulltext&aId=28397 أطلع عليه بتاريخ: 2017/03/12 الساعة 00:17.

4 - هدى حامد قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، مصر، الطبعة الأولى ، 1992 ، ص22 .

قانون العقوبات طالما كان مرتبطا بتقنية المعلومات[1]. أو هي الجريمة الناتجة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدًا من الناحية التقنية مثل تعديل الكومبيوتر[2].

2- تعريفات تقوم على وسيلة ارتكاب الجريمة:

من هذا التصور تتحقق الجريمة الإلكترونية باستخدام الكومبيوتر كأداة رئيسية لارتكابها، فالأستاذ جون فورستر يعرفها بأنها فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة [3]، وهذا ما ذهب إليه أيضاً الفقيه تايديمان Tiedeman حيث أشار إلى أنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب." ويصف هذه الجريمة مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها " الجريمة التي تلعب فيها البيانات الكومبيوتر والبرامج المعلوماتية دورا رئيسيا[4]."

أما منظمة التعاون الاقتصادي والتنمية OECD فقد عرفتها بأنها " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[5].

3- تعريفات على أساس صفات شخصية لمرتكب الفعل (المعرفة التقنية المعلوماتية):

ومنها التعريف الذي وضعته وزارة العدل الأمريكية في دراسة أعدها معهد ستانفورت للأبحاث واعتمدتها هذه الوزارة في دليلها لعام1979 والذي يعرفها

---

[1] - محروس نصار غايب، الجريمة المعلوماتية، مرجع سابق، ص 11.

[2] - نفس المرجع، ص 12.

[3] - Tom forester, Essential problems to High-Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989, P. 104

[4] - نفس المرجع، ص 13.

[5] - عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية ، بيروت، لبنان،2003، ص3.

بأنها: " أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها[1]." ومنها أيضا ما جاء به الفقيه David Thomson بأنها أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب[2].

ويرجح اعتماد هذا التعريف على اعتبار أنه اتسع ليشمل مختلف التصورات والاحتمالات المرتبطة بالجريمة الإلكترونية، كما أنه لا يغفل طابعها الفني والتقني، مما يعطي المجال الأوسع لما تنتجه التكنولوجيا العلمية مستقبلا في هذا المجال.

4- تعريفات تعتمد معيار محل الجريمة ووسيلة ارتكابه (الكمبيوتر) :

وفي هذه الحالة يعد جهاز الكومبيوتر الضحية والوسيلة، ولتفصيل ذلك نورد التعريفات التالية:

وفق هذا المنظور يعرف الفقيه Smedinghoff الجريمة الإلكترونية بأنها: " أي ضرب من النشاط الموجه ضد أو المنطوي على استخدام نظام الحاسوب." وفي ذات الاتجاه ذهب كل من الفقيهان Robert J. Lindquist و Jack Bologna فيعرفانها بأنها "الجريمة التي يستخدم فيها الحاسوب كوسيلة لارتكابها أو يمثل إغراء بذلك أو جريمة يكون الكومبيوتر نفسه ضحيتها." أما الفقيه Masse فيضيف إلى ذلك الهدف من اقتراف الجريمة الالكترونية وهو الحصول على الربح، فيعـــرفها بأنها" تلك الاعتداءات التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح[3]."

وخلاصة القول، أن الجريمة الالكترونية حسب هذا المعيار تقع بواسطة جهاز الكومبيوتر وعليه، وإن كان غرض البحث عن الربح وارد في ارتكابها،

1 - هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة . أسيوط ، مصر، ص5 و مايليها .

2 - نفس المرجع، ص 34.

3 - محروس نصار غايب، الجريمة المعلوماتية، مشار إليه، ص 13.

إلا أنه ليس العنصر الأهم؛ فقد يكون الهدف إثبات الذات والريادة من قبل الفاعل، أو بغرض الإضرار بالغير... وغيرها من الأسباب.

ثانياً: التعريف التشريعي للجريمة الإلكترونية

من المعلوم أن المشرع الجزائري وإلى وقت قريب أغفل تنظيم مجال الجريمة الإلكترونية قانونا، إلا أنه ما فتئ أن تدارك ذلك الفراغ القانوني من خلال سن قواعد قانونية لمواجهة هذه الجريمة، وذلك ما تجلى في القانون رقم 04-15 المتضمن تعديل قانون العقوبات، الذي نصت أحكامه في القسم السابع مكرر على المساس بأنظمة المعالجة الآلية للمعطيات، ثم تلاه بالقانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما.

ومما تجب الإشارة إليه، أن مصطلح نظام المعالجة الآلية للمعطيات تعبير ذا طابع فني تقني يصعب على القانوني إدراك مغزاه ببساطة، فضلا عن أنه تعبير متطور يخضع للتطورات السريعة و المتلاحقة في مجال فن الحاسبات الآلية[1]

ولذلك؛ فالمشرع الجزائري على غرار الكثير من التشريعات لم يعرف نظام المعالجة الآلية للمعطيات، وأوكل بذلك هذه المهمة لكل من الفقه[2] والقضاء.

ولمزيد من التفصيل نتطرق إلى تعريف ذلك من خلال القانونين 04-15، و09-04 على التوالي:

[1] - علي عبد القادر القهوجي , الحماية الجنائية لبرامج الحاسب الآلي , منشأة المعارف , الإسكندرية , مصر، 1999، ص 120.

[2] - وعلى سبيل الاستشهاد والمقاربة، فقد ذهب الفقه الفرنسي في تعريفه للنظام المعلوماتي إلى أنه: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة البرامج والمصطلحات وأجهزة الإدخال والإخراج وأجهزة الربط والتي يربط بينها مجموعة من العلاقات التي عن طريقها تحقق نتيجة معينة وهما معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية، راجع في ذلك عطاء الله فشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، راجع في ذلك الموقع الإلكتروني، http://iefpedia.com/arab/wp-content/uploads/2010/04/.doc أطلع عليه بتاريخ: 2017/03/11 الساعة 19:53.

أ- تعريف الجريمة الإلكترونية في التشريع الجزائري في القانون 04-15[1]

بالرجوع إلى قواعد القانون 04-15 من المادة 394 مكرر إلى المادة 394 مكرر2 نجد أنه حدد مفهوم المساس بأنظمة المعالجة الآلية للمعطيات، حيث حددها في المادة 394 مكرر بالآتي:

- الدخول والبقاء بالغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك.

- حذف أو تغيير لمعطيات المنظومة إذا ترتب عن الدخول أو البقاء غير المشروع بغرض تخريب نظام اشتغال المنظومة.

أما المادة 394 مكرر1 فقد أشارت إلى ما يلي:

- إدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها.

وبالنسبة للمادة 394 مكرر 2 فقد بينت المساس بأنظمة المعالجة الآلية للمعطيات من الآتي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

[1] - القانون رقم 04-15 المؤرخ في 10 نوفمبر، يعدل ويتمم الأمر 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71 لسنة 2004.

ب- تعريف الجريمة الإلكترونية في التشريع الجزائري في القانون 09-04[1]

حددت المادة (02) منه الجريمة الإلكترونية بقولها: " يقصد في مفهوم هذا القانون بما يأتي:

- الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

- منظومة معلوماتية:

أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

- معطيات معلوماتية:

أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

الفرع الثاني: خصائص الجريمة الإلكترونية ومرتكبيها

تتميز الجرائم الإلكترونية بجملة من الخصائص لا تتوافر في الجرائم العادية، وكذلك الأمر بالنسبة لمرتكبيها فإن لهم عدة خصائص تميزهم عن المجرمين العاديين، نبين ذلك في التالي:

أولاً: خصائص الجريمة الإلكترونية

تتسم الجريمة الإلكترونية بجملة من الصفات أو الخصائص نبينها في الآتي:

1 - القانون 09-04 المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47 لسنة 2009.

1- صعوبة اكتشاف الجريمة الإلكترونية:

توصف الجرائم الإلكترونية بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة، كإرسال فيروسات، وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم[1].

وبالتالي فإن هذه الجرائم وفي الغالب لا تترك اثر لها بعد ارتكابها، كما يصعب الاحتفاظ الفني بآثارها إن وجدت، وهذا كله يصعب من مهمة المحقق العادي في التعامل معها، حيث يستخدم فيها وسائل فنية غير عادية تعتمد التمويه في ارتكابها والتضليل في التعرف على مرتكبيها، وفي كل الأحوال تحتاج مواجهة هذه الجريمة إلى خبرة فنية عالية متخصصة لإثباتها.

2 – الجريمة الإلكترونية عابرة للحدود (الزمان والمكان):

المقصود بذلك أن هذا النوع من الجرائم لا يعتد بالحدود الجغرافية للدول ولا بين القارات، فمع انتشار شبكة الاتصالات بين دول العالم وأقاليمه أمكن ربط أعداد لا حصر لها من أجهزة الكمبيوتر عبر مختلف دول العالم بهذه الشبكة، حيث يمكن أن يكون الجاني في بلد والمجنى عليه في بلد آخر، وهكذا فالجرائم الالكترونية تقع في أغلب الأحيان عبر حدود دولية كثيرة[2].

ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمال الإجرامية التي يعمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، وهو ما يعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا، إذ أن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم

[1] - محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، مصر، 2009، ص 31.

2 - عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، ص 42

التواجد المادي لحصول الجريمة الإلكترونية في مكان الجريمة، ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء، فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الكمبيوتر الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصا آخر موجود في بلد ثالث[1].

3- جرائم هادئة:

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل والسرقة وغيرها من الجرائم، فالجرائم الالكترونية لا تحتاج أدنى مجهود عضلي بل تعتمد على الدراسة الذهنية، والتفكير العلمي المدروس القائم عن معرفة تقنية الكمبيوتر[2].

وذلك يعود لكون هذا النوع من الجرائم عبارة عن معطيات وبيانات تتغير أو تعدل أو تمحى من السجلات المخزنة في ذاكرة الحاسبات ، إلا أن البعض يشبهها بجرائم العنف مثل ما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة الأمريكية (FBI) نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف[3].

3- جرائم صعبة الإثبات:

يعد إثبات الجريمة الإلكترونية من الصعوبة بمكان، حيث يصعب تتبعها واكتشافها، فهي لا تترك أثراً يقتفى، حيث تعتبر مجرد أرقام، فمعظم الجرائم

1 - نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الأولى، 2005 ص 52.

2 - عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، مشار إليه، ص 46.

3 - مفتاح بوبكر المطردي، الجريمة الإلكترونية والتغلب على تحدياتها، مقال مقدم إلي المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان، المنعقد في 23-25 / 9 / 2012، ص 31 نقلا عن:
Computer Hackers : Tomorrows Torrortsts , Dgnamics , News For And Aboutmembers Of the American Society For Industrial Security, Varyl Febrauary , 1990 , p.7.

الالكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أنها تفتقر إلى الدليل المادي التقليدي كالبصمات مثلاً[1].

ومن جهة أخرى، فإن تعقبها يتطلب خبرة فنية يصعب تواجدها لدى المحقق العادي للتعامل معها، زيادة على ذلك يعمد مرتكب الجريمة الإلكترونية إلى ممارسة التمويه عند ارتكابها والتضليل والتحايل بغاية عدم التعرف على مرتكبيها.

ثانياً: خصائص مرتكبي الجريمة الإلكترونية

يتميز مرتكب الجريمة الإلكترونية بصفات خاصة تميزه عن غيره من مرتكبي الجرائم الأخرى، وذلك من حيث الآتي:

1- المجرم الإلكتروني ذكي ومتخصص:

في الغالب يتميز المجرم الإلكتروني بالذكاء، حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية الإلكترونية، حيث يستطيع المجرم الإلكتروني أن يكون تصور كاملا لجريمته حتى لا يتمكن ملاحقته وتتبع أفعاله الإجرامية من خلال الشبكات أو داخل أجهزة الكومبيوتر، فالمجرم الإلكتروني عادة يمهد لارتكاب جرائمه بالتعرف على كافة الظروف المحيطة به، لتجنب ما من شأنه ضبط أفعاله والكشف عنه[2].

كما أنه يتمتع بقدرة ومهارة تقنية يستغلها في اختراق الشبكات وكسر كلمات المرور أو الشفرات بغاية الحصول على البيانات والمعلومات الموجودة في أجهزة الكومبيوتر ومن خلال الشبكات[3].

1 - رستم هشام، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، دبي، الإمارات العربية المتحدة، العدد(2)، 1999، ص 11.

2- طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي (النظام القانوني لحماية المعلوماتي)، دار الجامعة الجديدة، القاهرة، مصر، الطبعة 2009، ص 177.

3- محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة، عمان، الأردن، ص 14.

2-المجرم الإلكتروني شخص سوي واجتماعي:

يتميز بأنه إنسان اجتماعي، فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به ، بل على العكس من ذلك نجده إنسان متوافق مع مجتمعه[1] ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو بغاية إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يتم تشغيله بها، أو بدافع الحصول على الأموال، أو بهدف الانتقام.

المطلب الثاني:مجالات استخدام الجريمة الإلكترونية

يتسع نطاق مجال الجريمة الإلكترونية ليشمل جميع مناح حياة المجتمع وأفراده، بداية من التدخل في حياته الخاصة وصولاً إلى أمنه، فنطاق الجريمة الإلكترونية تطال حياة الأشخاص الخاصة، كما تطال أيضاً أو تقع على أموال الأفراد والمؤسسات، وأخرى تطال أمن الدولة وسلامتها، ذلك ما يعالج في النقاط الجزئية التالية:

الفرع الأول: جريمة إلكترونية تطال حياة الأشخاص الخاصة

من المتعارف عليه أن المشرع في مختلف النظم القانونية يسن قوانين بغرض حماية الأشخاص من كل اعتداء قد يطالهم، وبظهور العالم الإلكتروني أصبحت حياة الأشخاص الخاصة في خطورة نتيجة توافر إمكانية السطو والاطلاع على أدق تفاصيل المعلومات عنهم والاستخدام السيئ لها، ذلك ما يفصل في التالي:

أولا: التهديد والمضايقة

يقصد بالتهديد والمضايقة زرع الخوف في نفس الإنسان من ضرر قد يلحق به شخصياً أو بمن تحت رعايته أو بمن لهم صلة به أو بماله ...[2] حيث يقوم

1 - عبد الصبور عبد القوي علي، الجريمة الالكترونية الطبعة الأولي دار العلوم للطباعة والنشر، القاهرة، مصر، 2007،

2 – محمد عبيد الكعيبي، مشار إليه، ص 88.

المجرم الإلكتروني بإرسال رسالة الكترونية للمجني عليه تنطوي على ما يرعبه كيفما كان شكله أو مضمونه، وذلك رغبة منه في التحكم في الضحية أو ابتزازه أو لأي سبب آخر.

ثانياً: انتحال شخصية الغير والاستدراج

يتم ذلك من خلال استخدام المجرم الإلكتروني لشخصية الضحية أو المجني عليه بغرض الاستفادة من سمعته أو سلطته أو ماله أو غيره من الأسباب، فقد تتم بواسطة انتحال شخصية المجني عليه أو انتحال شخصية المواقع، ويكثر استخدام هذه النمط في الوسط التجاري[1].

أما الاستدراج فغالب ضحاياه هم صغار السن، حيث يوهمون من قبل المجرم الالكتروني برغبته في تكوين صداقة عبر الشبكة تتحول إلى لقاء واقعي بينهما[2]، وقد تتم الجريمة في إقليم الدولة الواحدة، وقد تكون مخترقة حدود الدولة أي أن المجرم الإلكتروني في دولة والضحية موجود بدولة أخرى.

ثالثاً: نشر الإباحة

يقصد بنشر الإباحة كل إرسال أو نشر عمل إباحي أو بإعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية أو اتصل بالدعارة أو الأعمال الإباحية[3].

ويتم ذلك من خلال المواقع الإلكترونية الموجودة على الشبكة، والتي تستخدم بغرض الإثارة الجنسية من خلال قيام المجرم الإلكتروني بنشر صور

---

[1] – عمرو موسى، الجرائم المعلوماتية (جرائم الحاسب الآلي في مصر وفي الدول العربية)، المكتب الجامعي، الإسكندرية، مصر، 2006، ص102.

[2] – عمرو موسى، الجرائم المعلوماتية، مشار إليه، ص102.

[3] – أحمد محمد اللوزي و محمد عبد المجيد الذنيبات، الجريمة الإباحية الإلكترونية كما نظمها قانون جرائم أنظمة المعلومات الأردني، مجلة دراسات، كلية علوم الشريعة والقانون، الجامعة الأردنية، مجلد 42، العدد03، 2015، ص 853.

جنسية فاضحة وأفلام جنسية، وكثيرا ما تستهدف الأطفال والشباب لأن هذه الفئة أقل تحصيناً[1].

رابعاً: جريمة إلكترونية ماسة بشخص الإنسان وكرامته

تعد من الجرائم الإلكترونية واسعة الانتشار عبر الشبكات، حيث تستخدم أسلوب القذف والسب وتشويه السمعة وغيرها من الأفعال اللاأخلاقية، بغرض المساس بشرف الشخص أو النيل من كرامته، وقد يكون عبر خطوط الاتصال أو عبر البريد الإلكتروني أو عبر صفحات الويب، أو عبر غرف المحادثة أو الدردشة[2].

الفرع الثاني: جريمة إلكترونية تطال الأموال

من المعلوم أنه باتت الكثير من المعاملات المالية في وقتنا الحاضر تتم بواسطة الشبكات الإلكترونية، مما زاد من تطور وسائل الدفع الإلكتروني، الأمر الذي أدى إلى تطور الجريمة الإلكترونية بغاية الحصول على الأموال بأقل تكلفة ممكنة. ذلك ما نشرحه في الآتي:

أولا: جرائم إلكترونية تطال بطاقات الائتمان والتحويلات المالية الإلكترونية

تتم الجريمة الإلكترونية في هذه الحالة من خلال الحصول على كلمة السر المدرجة في أنظمة الكمبيوتر الخاصة بالمجني عليه، مما يسهل على المجرم الإلكتروني الولوج إلى النظام المعلوماتي، ويكون ذلك سواء بالتواجد على الشبكة أثناء إتمام عملية ما، أو بإدخال بيانات إلى ذاكرة الجهاز[3]، ويكون ذلك باستخدام الاحتيال، وكذلك الاحتيال بواسطة بطاقات الدفع الالكتروني

---

[1] – عبد الكريم خالد الشامي، جرائم الكومبيوتر والانترنت في التشريع الفلسطيني، راجع الموقع الإلكتروني: www.pal-ip.org أطلع عليه بتاريخ: 2017/03/11 الساعة 23:11

[2] – محمد الكعبي، مشار إليه، ص 114.

3 – صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل درجة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013، ص 44.

1- الاحتيال:

يتم الاحتيال على الضحية من خلال تضليله بوجود مشروع يحصل من وراءه على أموال مما يدفعه إلى الانسياق وراء تغرير المجرم الإلكتروني، هذا الأخير يحصل بواسطة استعماله أفعال تضليلية على أموال ملك للغير دون مسوغ قانوني، ويكون ذلك سواء باتصال عبر الشبكة بين الجاني الإلكتروني والمجني عليه، أو من خلال استخدم المجرم الإلكتروني البيانات الكاذبة التي تساعده على ايهام الكمبيوتر والاحتيال عليه بغاية الحصول على الأموال[1].

2- الاحتيال بواسطة بطاقات الدفع الإلكتروني

يتم الدفع الإلكتروني بواسطة بطاقة الدفع الإلكتروني بتحويل مالي من المصدر وهو بنك العميل إلى رصيد متعامل آخر قد يكون تاجر أو دائن أو...، كل ذلك يتم بواسطة شبكة التسوية الإلكترونية الدولية (مثلاً ماستر كارد)، حيث يقوم المجرم بكسر كلمة السر للبطاقة الإلكترونية أو خداع الصراف الآلي، وبالتالي يتمكن من الحصول على السلع والخدمات من خلال ملء نموذج إلكتروني ببيانات بطاقة الائتمان الخاصة بالمشتري[2].

ثانياً: سرقة أموال البنوك

وتتحقق بواسطة استخدام المجرم الإلكتروني الكمبيوتر بغرض الدخول إلى الشبكة والوصول غير المشروع إلى البنوك وغيرها من المؤسسات المالية، وتحويل الأموال من الحسابات الخاصة بالعملاء إلى حسابات أخرى، وقد يتم ذلك بكميات بسيطة بصفة متكررة بحيث لا يلفت الانتباه، وقد يتم دفعة واحدة[3].

---

[1] – يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الإلكترونية، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، مسقط، عُمان، من 02 إلى 04 ابريل 2006، ص 16.

2 – صغير يوسف، الجريمة الإلكترونية عبر الانترنت، مشار إليه، ص 45.

[3] – محمود حجازي، مشار إليه، ص 18.

ثالثاً: غسيل الأموال

يعد غسيل الأموال من أبرز الأنشطة التي تقوم بها شبكات منظمة تحترف الإجرام الإلكتروني، وتأخذ درجة عالية من التنسيق والتخطيط والانتشار في كافة أنحاء العالم، وتشير إحصائيات الأمم المتحدة وصندوق النقد الدولي إلى أن 30 مليار دولار أمريكي من الأموال القدرة تغسل سنويا عبر الشبكات الإلكترونية مخترقة حدود ما يقارب أو يزيد عن 76 دولة في العالم[1].

الفرع الثالث: جريمة إلكترونية تطال أمن الدولة

وتتمثل في جرائم الإرهاب والتجسس والجريمة المنظمة، هذا ما نعالجه في النقاط التالية:

أولاً: الإرهاب والجريمة الإلكترونية

مما لا شك فيه أن ظاهرة الإرهاب أضحت عالمية، حيث ظهرت الكثير من التنظيمات التي تتبنى هذا الفكر في مختلف دول العالم وبمختلف التسميات، وتظهر العلاقة بين الإرهاب والجريمة الإلكترونية من خلال تجنيد وتجييش أعضاء جدد في التنظيم أو حشد الهمم بواسطة استخدام مختلف وسائل التواصل الإلكتروني.

كما يتم تبني العمليات الإرهابية والدعاية لهذه التنظيمات وأعمالها من خلال مختلف الوسائط والمواقع الإلكترونية بما يحقق أهدافها[2].

ثانياً: التجسس والجريمة الإلكترونية

غير خاف أن التطور في المجال الإلكتروني المعلوماتي سهل من مهمة التجسس، فالمجرم الإلكتروني سواء كان شخص واحد أو تنظيم يمكنه التجسس

[1] – نفس المرجع، ص 21.

[2] – يوسف صغير، مشار إليه، ص 96.

سواء على الأشخاص أو المنظمات وحتى الدول أو أجهزتها، ويأخذ التجسس عدة صور، فقد يكون تجسس اقتصادي أو سياسي أو عسكري.

ثالثاً: الجريمة المنظمة والجريمة الإلكترونية

غني عن البيان أن أعضاء الجريمة المنظمة يستفيدون من التطور التكنولوجي في مجال المعلومات الإلكترونية، وذلك من خلال استغلال الإمكانات المتاحة إلكترونياً في التخطيط والتوجيه وتنفيذ المخططات الإجرامية بسهولة مخترقة حدود الدول بأقل تكلفة ممكنة ودون مخاطرة.

خاتمة:

من خلال ما تقدم ذكره يتجلى لنا أن الجريمة الإلكترونية أصبحت من الخطورة بمكان، فضررها أصاب الأفراد والجماعات، وكذا المجتمع، ولم تسلم منها حتى الدول، كما أضحت عائقا يواجه مختلف مظاهر الحياة الأمنية منها والمالية والاقتصادية والاجتماعية، مما ينذر بخطر محدق يهدد أمن واستقرار المجتمع الدولي برمته.

لذلك؛ وبغرض مواجهة هذه التحديات، فإنه بات من الضروري والملح مواكبة التشريعات الرائدة في مواجهة الجريمة الإلكترونية، خصوصاً أن الدولة الجزائرية تسعى حثيثا نحو عصرنة ورقمنة كافة أجهزت الدولة ومرافقها، وعلى ذلك فإن الواجب يقتضي تعريف الجريمة الإلكترونية تعريفا جامعا مانعا يحددها بدقة يحين كلما اقتضت الضرورة، كما يتوجب أن تسن قوانين تتناسب وحجم ظاهرة الجريمة الإلكترونية، والاستفادة من التشريعات المقارنة التي لها فضل السبق في هذا المجال، وكذا التنسيق الدولي في هذا المجال سواء من حيث تكوين إطارات الأجهزة المعنية بمتابعة هذه الجرائم أو من خلال التنسيق بين هذه الأجهزة بحد ذاتها، حتى يمكن مواكبة التطور المتواتر في مجال الجريمة الإلكترونية، وتسهيل الوصول إليها وكشف خبايا مرتكبيها، ولا شك أن

هذا الأمر الذي في نهايته يضفي حماية قانونية على المستخدم الإلكتروني في مختلف مناح حياته، وبمختلف فئاته العمرية، وكذلك يحقق الاستقرار السياسي والاقتصادي والأمني داخل الدولة ويحمي أجهزتها ومرافقها من كل اختراق قد يطالها بما يدعى بالجريمة الإلكترونية.

قائمة المصادر والمراجع:

أولاً: المصادر

- القانون رقم 04-15 المؤرخ في 10 نوفمبر، يعدل ويتمم الأمر 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71 لسنة 2004.
- القانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما الجريدة الرسمية، العدد 47 لسنة 2009.

ثانياً: المراجع:

1- باللغة العربية:

- محمد حجازي، جرائم الحاسبات والانترنت (الجرائم المعلوماتية)، المركز المصري للملكية الفكرية، القاهرة، مصر، 2005.
- هدى حامد قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، مصر، ط الأولى، 1992.
- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة ، أسيوط ، مصر.
- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، مصر.
- نائلة عادل محمد فريد قورة، جرائم الحاسب الالي الاقتصادية. منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الأولى، 2005 .
- عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية، القاهرة، مصر.
- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، مصر، 2009.
- عبد الصبور عبد القوي علي، الجريمة الالكترونية الطبعة الأولي دار العلوم للطباعة والنشر، القاهرة، مصر،2007.

– عمرو موسى، الجرائم المعلوماتية (جرائم الحاسب الآلي في مصر وفي الدول العربية)، المكتب الجامعي، الإسكندرية، مصر، 2006.

– عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003.

– علي عبد القادر القهوجي , الحماية الجنائية لبرامج الحاسب الآلي , منشأة المعارف , الإسكندرية , مصر، 1999.

– طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي (النظام القانوني لحماية المعلوماتي)، دار الجامعة الجديدة، القاهرة، مصر، ط .2009

2– باللغة الأجنبية

1- Tom forester, Essential problems to High-Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989.

2- Computer Hackers : Tomorrows Torrortsts , Dgnamics , News For And Aboutmembers Of the American Society For Industrial Security, Varyl Febrauary , 1990.

ثالثاً: المذكرات

– صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل درجة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013

رابعاً: المجلات

– أحمد محمد اللوزي و محمد عبد المجيد الذنيبات، الجريمة الإباحية الإلكترونية كما نظمها قانون جرائم أنظمة المعلومات الأردني، مجلة دراسات، كلية علوم الشريعة والقانون، الجامعة الأردنية، مجلد 42، العدد03، 2015.

– رستم هشام، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون، دبي، الإمارات العربية المتحدة، العدد(2)، 1999.

– محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة، عمان، الأردن.

– يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الإلكترونية، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، مسقط، عُمان، من 02 إلى 04 ابريل 2006.

خامساً: المواقع الإلكترونية

1-www.iasj.net/iasj?func=fulltext&aId=28397
2- www .iefpedia.com/arab/wp-content/uploads/2010/04/.doc
3- www.pal-ip.org