الجريمة الإكترونية والمجرم المعلوماتي: مقاربة مفاهمية

Electronic crime and Cybercriminal: Conceptual approach

ط.د. رضا عسال[1]
قسم علم الإجتماع
جامعة العربي التبسي- تبسة- الجزائر
rida.assel@univ-tebessa.dz

ط.د. عماد عبد الرزاق
قسم علم الإجتماع
جامعة العربي التبسي- تبسة- الجزائر
imed.abderrezak@univ-tebessa.dz

تاريخ الإرسال:2020/02/16 تاريخ القبول: 2020/03/15 تاريخ النشر: 2020/03/30

ملخص

قد شهد القرن الماضي ثورة من نوع غير مألوف أصطلح على تسميتها بثورة المعلومات أو التقنية الجديدة، والتي أضافت كثيرا من الإيجابيات في حياتنا اليومية إلا أنها أفرزت أنماطا جديدة من الجريمة والمجرمين ومن بين هذه الأنماط الحديثة التي أفرزتها هذه الثورة التكنولوجية، الجريمة الإكترونية والمجرم المعلوماتي اللذان إرتبطا مع بعضهما البعض في الآونة الأخيرة، حيث تمثل الجريمة الإكترونية الفعل الإجرامي الذي أخذ بعدا أكثر تعقيدا، وفاعل وهو المجرم المعلوماتي الذي يتميز عن باقي المجرمين التقليدين بعدة خصائص وسمات حيث مزال هذين المفهومين يعتليهما لبس في تعريفهما وتحديد خصائصهما، لهذا جاءت هذه الدراسة لتقديم مقاربة مفاهمية للجريمة الإكترونية والمجرم المعلوماتي من شأنها رفع اللبس على هذين المفهومين لأن للجريمة الإكترونية عدة مسميات وتصنيفات وأنواع وخصائص المميز لها وأيضا المجرم المعلوماتي الذي يتميز عن باقي المجرمين التقليديين بعدة خصائص وسمات وله أهدافه الخاصة .

الكلمات المفتاحية: الجريمة الإلكترونية، المجرم المعلوماتي.

Abstract

Which added many positives to our daily lives, but it has produced new patterns of crime and criminals. Among these modern patterns that this technological revolution has produced, electronic crime and Cybercriminal Which is connected with each other in the last utensils, where the electronic crime represents the criminal act that took on a more complex and effective dimension, and it is the Cyber-criminal that distinguishes from other traditional criminals with several characteristics and Features where these two concepts are still attributed to ambiguity in their definition and specification of their characteristics, That is why this study came to provide a conceptual approach to cybercrime and Cyber-criminal, which would raise confusion on these two concepts because cybercrime has several names, classifications, types, and characteristics that are unique to them, as well as the Cyber-criminal, which is distinguished from other traditional criminals with several characteristics and characteristics and has its own goals.

[1] المؤلف المراسل: رضا عسال، rida.assel@univ-tebessa.dz

Key words: *electronic crime, Cyber criminal*

مقدمة

مرت الجريمة عبر مختلف المراحل التي عرفها الإنسان، بتطورات في مختلف مجالات الحياة، وتغيرت حسب دوافعه وظروفه الإجتماعية، وذلك باختلاف الزمان والمكان، فالجرائم التي كانت ترتكب في وقت مضى لم يعد لها وجود في الوقت الحاضر والعكس صحيح، بالإضافة إلى ذلك أن الجرائم التي ترتكب في مكان ما لا ترتكب في مكان آخر، وذلك راجع للاختلاف الموجود بين أفراد المجتمع من حيث المستوى الثقافي والعلمي والمادي وفي بعض الأحيان الديني .

حيث تطورت الجريمة بتطور نمط حياة الإنسان، ولقد بلغ هذا التطور أوجه بالظهور المجتمعات بمفهومها المعاصر، حيث أن هذه المجتمعات أصبحت تعيش الكثير من التراكمات ما نتج عنها وقوع الكثير من الجرائم، وذلك جراء الضغوط النفسية وتميز حياة الأفراد بطبيعة براغماتية مادية، حيث أصبح الفرد داخل هذه المجتمعات يسعى بشتى الطرق للوصول إلى إشباع رغباته الشخصية، حتى ولو وصل به الأمر إلى لارتكاب العديد من الجرائم تكون نتائجها وخيمة على الأفراد بصفة خاصة وعلى المجتمع بصفة عامة.

ما دامت الجريمة ظاهرة إجتماعية، تتأثر طبيعتها وحجمها بالتحولات الإقتصادية والإجتماعية والثقافية دوليا ووطنيا، فقد ظهر للوجود نمط جديد من الإجرام، تجسد في انتشار الجرائم المعلوماتية أو الإلكترونية، والتي تعتبر من أكبر السلبيات التي خلفتها الثورة المعلوماتية، لكون هذه الجرائم تشمل في اعتداءاتها قيما جوهرية تخص الأفراد والمؤسسات وحتى الدول في كافة نواحي الحياة، كما أن هذه الجرائم تركت في النفوس شعورا بعدم الثقة بخصوص التعامل والإستفادة من ثمار هذه الثورة الجديدة ومنفذي هذه الجرائم .

وما يشهده العصر من تطور الوسائل المعلوماتية الحديثة، ساعد هؤلاء المجرمين في زيادة سرعة نشر جرائمهم حتى أصبحت تهدد النظام المعلوماتي، بل أصبح في إمكانهم التسبُّب في خلق شلل كامل للأنظمة المدنيّة الأرضيّة والفضائيّة، وتعطيل المعدات الإلكترونيّة، واختراق النُّظم المصرفيّة، وإرباك حركة الطيران وشل محطات الطاقة وغيرها بواسطة قنابل معلوماتية ترسلها لوحة مفاتيح الكمبيوتر من على مسافات تتعدّى عشرات الآلاف من الأميال، وذلك دون أن يترك المجرم المعلوماتي أو الإلكتروني أثرًا ملموسًا لملاحقته ومعرفة مَصدرها، والمجرم يستطيع بواسطة هذه التقنيات العالية أن يصل إلى أي مكان يرغب فيه، عبر الإبحار في الشبكة المعلوماتية ويتصل ويتفاعل مع من شاء في أي مكان، فلا مكان ولا زمان يستطيع وضع حدود لهذه الشبكة وبالتالي فالجريمة الإكترونية والمجرم المعلوماتي هما الركزتين الأساسيتين في هذه العملية، هذا مايدفعنا أن نطرح التساؤل التالي :

ماهي الجريمة الإكترونية وماالمفاهيم المرتبطة بها وما سمات وخصائص وأهداف المجرم المعلوماتي؟

أولا : ماهية الجريمة المعلوماتية

نستعرض فيما يلي مفهوم الجريمة الإلكترونية وخصائصها وأنواعها.

1- مسميات الجريمة الإلكترونية

تعدَّدت ألفاظ ومفردات وصِيَغ ومصطلحات التعريف بالجريمة الإلكترونية تعدُّدًا يحمل صورة التنوُّع والثراء لا التنازع والتضاد، " فأُطْلِقَ على الجريمة الإلكترونية عدة تسميات وهي كتالي :

- جرائم الكمبيوتر والإنترنت، وجرائم الحاسب الآلي (Computer Crimes).
- جرائم التقنية العالية (High-Tick).
- الجرائم المعلوماتيّة (Information Crimes).

- الجرائم الرقمية (Digital Crimes).
- السيبر كرايم (Cyber Crime).
- جريمة أصحاب الياقات البيضاء (White Collar).
- الجرائم الناعمة (Soft Crimes).
- الجرائم النظيفة (Clean Crimes)".[1]

2- تعريف الجريمة الإلكترونية

"عرفت الجريمة بصفة عامة على أنها كل فعل غير مشروع صادر عن إرادة آثمة يقرر له القانون عقوبة أو تدابير إحترازية، وتعتمد الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت على المعلومة بشكل رئيسي، وهذا الذي أدى إلى إطلاق مصطلح الجريمة الإلكترونية على هذا النوع من الجرائم" [2]

"و يصعب الإتفاق على تعريف موحد للجريمة الإلكترونية، حيث إختلفت الإجتهادات في ذلك إختلافاً كبيرا، يرجع إلى سرعة وتيرة تطور التقنية المعلوماتية من جهة، و تباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى، حيث أدت الحداثة التي تتميز بها الجرائم الإلكترونية، وإختلفت النظم القانونية والثقافية بين الدول إلى عدم الإتفاق على مصطلح موحد للدلالة عليها، وعدم الإتفاق، هذا إنجر عليه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية وذلك خشيت حصرها في مجال ضيق " [3]

"وكان كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي؛ وتجدر الإشارة أيضاً إلى أن أهم عوامل صعوبة الإتفاق على تعريف هو أن التقنية المعلوماتية أصبحت تحل محل العديد من التقنيات السابقة كالهاتف والفاكس والتلفزيون، فالمسألة لم تقتصر على معالجة البيانات فحسب بل تعدتها إلى وظائف عديدة مثل وظيفة النشر والنسخ، وهو ما يحتم ضرورة التفرقة بين جرائم الإنترنت وشبكات المعلومات بالمعنى الفني عن بقية الجرائم الأخرى التي يستخدم فيها الإنترنت أو الحاسب الآلي كأداة لارتكابها فيقصد بجرائم الأنترنت وشبكات المعلومات، الدخول غير المشروع إلى الشبكات الخاصة كالشركات والبنوك وغيرها وكذلك الأفراد، والعبث بالبيانات الرقمية التي تحتويها شبكة المعلومات مثل تزييف البيانات أو إتلافها ومحوها، وامتلاك أدوات أو كلمات سرية لتسهيل إرتكاب مثل هذه الجرائم التي تلحق ضرراً بالبيانات والمعلومات ذاتها وكذلك بالنسبة للبرامج والأجهزة التي تحتويها وهي الجرائم التي تلعب فيها التقنية المعلوماتية دوراً رئيسياً في مادياتها أو السلوك الإجرامي فيها، أما الجرائم التقليدية الأخرى مثل غسيل الأموال، تجارة المخدرات، الإرهاب، الدعارة، الإستخدام غير المشروع للكروت الإلكترونية، ودعارة الأطفال Pornography وجرائم التجارة الإلكترونية، وكذلك جرائم السب و القذف، هي جرائم تستخدم التقنية المعلوماتية كأداة في ارتكابها دون أن تكون جرائم معلوماتية بالمعنى الفني وإن كان يطلق عليها الجرائم الإلكترونية". [4]

3- خصائص الجريمة الإلكترونية

أدى إرتباط الجريمة الإلكترونية بجهاز الحاسوب وشبكة الإنترنت إلى إضفاء مجموعة من الخصائص والسمات المميزة لهذه الجريمة عن الجرائم التقليدية، ويمكن إجمالها فيمايلي:

1.3. الجريمة المعلوماتية متعددة الحدود (جريمة عابرة للحدود)

"المجتمع المعلوماتي لا يعترف بالحدود الجغرافية ولا يعيرها اهتماما فهو مجتمع منفتح عبر شبكات تخترق المكان والزمان دون أن تخضع للحواجز الحدودية، فبعد ظهور شبكة المعلوماتية لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدارة التي تتمتع بها الحواسيب وشبكاتها من نقل

كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينهما آلأف الأميال قد أدت الى نتيجة تتمثل في أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد".[5]

فالسهولة في حركة المعلومات عبر أنظمة وبرامج التقنية الحديثة جعل بالإمكان إرتكاب جريمة عن طريق الكمبيوتر موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة اخرى.

2.3. صعوبة إكتشاف الجريمة المعلوماتية

"تتميز الجريمة المعلوماتية بصعوبة اكتشافها، وإذا ما اكتشفت فان ذلك يكون بمحض الصدفة عادة، حيث يبدو من الواضح أن عدد الحالات التي تم فيها إكتشاف هذه الجريمة قليلة إذا قورنت بما يتم إكتشافه مع الجرائم التقليدية".[6]

" ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة الإلكترونية الى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، فلا يوجد جثث لقتلى ولا آثار للدماء، كما أن المجرم يمكنه إرتكاب هذه الجريمة في دول وقارات مختلفة إذ أن الجريمة الإلكترونية كما سبق وأشرنا جريمة عابرة للحدود وكذلك فإن قدرة المجرم تدمير دليل الإدانة في أقل من ثانية الواحدة يشكل عاملا إضافيا في صعوبة إكتشاف هذا النوع من الجرائم".[7]

3.3. أسلوب أرتكاب الجريمة المعلوماتية

"من خصائص الجريمة المعلوماتية أنها تبرز ذاتيتها بصورة أكثر وضوحا في أسلوب إرتكابها وطريقتها، فإذا كانت الجرائم التقليدية تتطلب نوعا من الجهد العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء، كما هو الحال في جريمة القتل أو الإختطاف أو صورة الكسر وتقليد المفاتيح، كما هو الحال أيضا في جريمة السرقة،فإن الجريمة المعلوماتية هي جرائم هادئة بطبيعتها لا تحتاج إلى العنف بل كل ماتحتاجه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير مشروعة".[8]

4. أنواع الجرائم الإكترونية

هناك عدة تصنيفات للجرائم الإكترونية وهذا حسب معيار الغاية من ارتكابها أو حسب الوسيلة المعتمدة، ويمكن تلخيص أنواع الجرائم الإكترونية في مايلي :

1.4. **الجرائم ضد الافراد:**

وتسمى بجرائم الأنترنت الشخصية مثل : سرقة الهوية ومنها البريد الإلكتروني أو سرقة الإشتراكات في مواقع شبكة الأنترنت.

2.4. **الجرائم ضد الملكية :**

إنتقال برمجيات ضارة المضمنة في بعض البرامج التطبيقية والخدمة أو غيرها لتدمير الأجهزة أو البرامج المملوكة للشركات أو الأجهزة الحكومية أو البنوك أو حتى ممتلاكات الشخصية.

3.4. **الجرائم ضد الحكومات :**

مهاجمة المواقع الرسمية أو أنظمة الشبكة الحكومية والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي كالهجمات الإرهابية على شبكة الأنترنت وهي تتركز على تدمير الخدمات والبنى التحتية ومهاجمة شبكة الكمبيوتر وغالبا مايكون هدفها سياسي بحت".[9]

ثانيا : المجرم المعلوماتي وسماته

1 ـ تعريف المجرم المعلوماتي

"هو كل شخص سواءً طفل أو رجل أو أنثى يأتي أفعالا إرادية تشكل سلوكا إيجابيا أو سلبيا باستخدام تقنية المعلوماتية لإحداث نموذج إجرامي بالاعتداء على حق أو مصلحة، وسمات المجرم المعلوماتي تشبه في كثير من الأحيان سمات المجرمين ذوي الياقات البيضاء، حيث أن كل من هؤلاء المجرمين قد يكونوا من ذوي المناصب الرفيعة والمستوى العالي، ومن ذوي التخصصات والكفاءات العالية ويتمتعون بالذكاء والقدرة على التكيف الإجتماعي في المحيط الذي يعيشون فيه بل وإن بعضهم يتمتع بالإحترام والثقة العالية من الأشخاص المحيطين بهم في مجال العمل أو في المحيط الاجتماعي".[10]

2ـ سمات المجرم المعلوماتي

يتميز المجرم المعلوماتي عن باقي المجرمين التقليدين بعدة خصائص أهمها:

1.2. المجرم المعلوماتي يتمتع بالمهارة والمعرفة والذكاء

" رسم بعض العلماء صورة عامة للمجرم المعلوماتي متسمة بصفة الذكاء، وذلك على سند من القول أن بعض أنماط الجريمة المعلوماتية مثل إتلاف الحاسوب أو سرقة المعلومات المخزنة داخله أو الدخول إلى بيانات الشركات لا تحتاج في مرتكبها إلى قوة عضلية بل تحتاج إلى معرفة ومهارة وذكاء وقدرة كبيرة في التحكم في جميع تقنيات الإعلام الآلي لهذا يتميز المجرم المعلوماتي غالبا بالذكاء، حيث أن الجريمة المعلوماتية تتطلب مقدرة عقلية وذهنية عميقة، خاصة في جرائم المالية التي تؤدي الى خسارة مادية كبيرة تلحق بالمجني عليه، وبالتالي فالمجرم المعلوماتي لا يلجاء إلى العنف أو إتلاف المادي بل يحاول أن يحقق أهدافه بهدوء.[11]

2.2. المجرم المعلوماتي شخص إجتماعي

باستطاعتنا القول بأن المجرم المعلوماتي بصفته إنسان ذكي فهو إجتماعي، فلا يضع نفسه في حالة عداءٍ مع المجتمع الذي يحيط به، بل أنه إنسان يستطيع التوافق والتصالح مع مجتمعه، فهو شخص مرتفع الذكاء مما يساعده على عملية التكيف مع المجتمع، فالذكاء في نظر الكثيرين ليس سوى القدرة على التكيف ولا يقصد بذلك التقليل من شأن المجرم المعلوماتي، بل أن خطورته الإجرامية قد تزداد إذا زاد تكيفه الإجتماعي مع توافر الشخصية الإجرامية لديه، فالحساس المجرم أنه محل ثقة من مجموعته، وشعوره أنه خارج إطار الشبهات قد يدفعه إلى التمادي في إرتكاب جرائمه التي قد لا تكتشف، وإذا اكتشفت فإنها تواجه صعوبة في إثباته". [12]

3.2. المجرم المعلوماتي يتمتع بالسلطة تجاه النظام المعلوماتي

"تعني بالسلطة تلك المزايا والحقوق التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، فمعظم مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، وقد تتمثل هذه السلطة في الرقم السري الخاص للولوج إلى النظام الذي يحتوي على المعلومات، والتي تمد الفاعل بمزايا متعددة كفتح الملفات وقراءتها وكتابتها ومحو المعلومات أو إجراء تعديلات وقد تتمثل هذه السلطات في الحق في استعمال الأنظمة المعلوماتية أو إجراء بعض التعاملات أو مجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة".[13]

3ـ دوافع مجرمي المعلومات

تختلف الجريمة المرتكبة عبر الإنترنت عن الجريمة التقليدية من حيث الدوافع، حيث أن مجرمي الأنترنت يسعون من خلال إرتكابهم للجريمة بالإضافة إلى تحقيق المكسب المادي إلى تحقيق أغراض معنوية مثل التعلم أو اللعب والمزاح، أو لمجرد الإنتقام، ويمكن حصر هذه الدوافع في :

1.3. الدوافع الرئيسية لارتكاب المجرمين للجريمة عبر الإنترنت

1.1.3. <u>تحقيق الكسب المادي:</u>

"يقوم مرتكبوا الجريمة عبر الإنترنت ذوي الكفاءة الفنية العالية، بما لديهم من خبرة ومهارة في المجال التكنولوجي بتوجيه هذه الإمكانات نحو المؤسسات المالية لمحاولة تحقيق المكاسب المادية إما بسرقة تلك الأموال أو بتحويلها لحسابه الشخصي داخل البنك، يستطيع المجرمون بمجرد دخولهم إلى أنظمة البنوك معرفة أرقام الحاسب وسرقتها أو تحويلها، ويكون المكسب المادي أيضا هدفا لمن هم أقل في المعرفة التقنية وقد يكونون غير مؤهلين على الإطلاق في المجال المعلوماتي لذلك يكون أسلوب إرتكابهم للجريمة مختلفا، لأن الجريمة تكون متعلقة بالحاسب الآلي أو المعلومات ولكن دون الدخول إلى أنظمة تلك الحواسب ويكون أسلوب ارتكابهم للجرائم أسلوبا محدودا في مجال معين لا يحتاج إلى خبرة ومهارة".[14]

تجدر الإشارة إلى أنه في حال نجاح المجرم في ارتكاب جريمته عبر الإنترنت، فإن ذلك قد يدر عليه أرباحة هائلة في زمن قياسي.

2.1.3. الرغبة في التعلم

"هناك من يرتكب جرائم الأنترنت بغية الحصول على الجديد من المعلومات وسبر أغوار هذه التقنية المتسارعة النمو والتطور، وهؤلاء الأشخاص يقومون بالبحث واكتشاف الأنظمة والعمل من خلال الجماعة وتعليم بعضهم، ويفضل هؤلاء القراصنة البقاء مجهولين أكبر وقت ممكن حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة ويكرس البعض منهم كل وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة الحاسوب".[15]

3.1.3. دوافع ذهنية أو نمطية

"غالبا ما يكون الدافع لدى مرتكب الجرائم عبر الأنترنت هو الرغبة في إثبات الذات وتحقيق إنتصار على تقنية الأنظمة المعلوماتية دون أن يكون لهم نوايا آثمة، ويرجع ذلك إلى وجود عجز في التقنية التي تترك الفرصة لمشيدي برامج النظام المعلوماتي لارتكاب تلك الجرائم".[16]

2.3. الدوافع الشخصية والمؤثرات الخارجية

1.2.3. إرتكاب الجرائم من أجل التسلية

" يعتبر دافع المزاح والتسلية من الدوافع التي تجعل الشخص يقوم بتصرفات وإن كان لا يقصد من ورائها إحداث جرائم وإنما بغرض المزاح فقط ولكن هذه التصرفات قد تنتج عنها نتائج ترقى إلى درجة الجريمة". [17]

2.2.3. دوافع سياسية

"إنتشرت الكثير من المواقع غير المرغوب فيها على شبكة الإنترنت ومن هذه المواقع ما يكون موجها ضد سياسة دولة محددة أو ضد عقيدة أو مذهب معين، وهي تهدف في المقام الأول إلى تشويه صورة الدولة أو المعتقد المستهدف؛ حيث تعد الدوافع السياسية من أبرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم، كما أن الأفراد قد يتمكنون من اختراق الأجهزة الأمنية الحكومية، كذلك أصبحت شبكة الإنترنت مجالا خصبا لنشر أفكار العديد من الأفراد والمجموعات، ووسيلة للترويج لأخبار وأمور أخرى قد تحمل في طياتها مساسا بأمن الدولة أو بنظام الحكم أو قدحا في رموز دولية أو سياسية والإساءة لها بالذم والتشهي".[18]

3.3. دافع الانتقام

"يكون دافع الإنتقام مؤثرا في ارتكاب هذه الجرائم، حيث يعد من أخطر الدوافع التي يمكن أن تدفع شخصا يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها لأنه غالبا ما يكون أحد موظفيها، ويقوم بهذا الدافع نتيجة إما لفصله من العمل أو تخطيه في الحوافز أو الترقية فهذه الأمور تجعله يقدم على ارتكاب جريمته" [19] و "تشير التقديرات إلى أن نسبة كبيرة من الجرائم المرتكبة عبر الإنترنت ترتكب من قبل موظفي الجهة نفسها، ومن الوقائع

التي حدثت في الولايات المتحدة الأمريكية أنه حكم على أحد الموظفين في إحدى شركات التأمين بالسجن لمدة سبع سنوات وغرامة مقدارها 150 ألف دولار لأنه أدخل فيروسا في أجهزة الشركة التي كان يعمل فيها مما أدى إلى ضياع 160 سجلا من سجلات العملاء، وذلك انتقاما من الشركة لأنها قامت بفصله من العمل". [20]

4ـ أهداف المجرم المعلوماتي

للمجرم المعلوماتي أهداف كثيرة نستطيع أن نلخصها فيمايلي :

1ـ التمكن من الوصول الى المعلومات بشكل غير شرعي، كسرقة المعلومات أو الإطلاع عليها أو حذفها أو تغييرها بما يحقق هدف المجرم.

2 ـ التمكن من الوصول عن طريق الشبكة العنكبوتية إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها أوالتلاعب بمعطياتها.

3ـ الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات والبنوك والجهات الحكومية والأفراد وابتزازهم من خلالها بدافع مادي أو سياسي.

4ـ الكسب المادي أو المعنوي أو السياسي غير المشروع عن طريق تقنية المعلومات مثل عمليات إختراق وهدم المواقع على الشبكة العنكبوتية وتزوير بطاقات الإنتماء وسرقة الحسابات المصرفية ....إلخ.

كل هذه وأخرى هي أهداف يسعى إليها المجرم المعلوماتي للوصول إلى فائدة له على المستوى الفردي أو الجماعي".[21]

خاتمة

تطرقنا في هذه الدراسة إلى تعريف الجريمة الإلكترونية وتحديد مسمياتها وتصنيفاتها وخصائصها وكذلك مايخص المجرم المعلوماتي والذي يعتبر مفهوم جديد في وقتنا الراهن، إلا أن مايجب توضيحه في الأخير أن ظاهرة الإجرام المعلوماتي جديدة ومتجددة، لأن قطاع تكنولوجيات الإعلام والإتصال في تطور مستمر ودون توقف وخاصة مع استخدام الكثير لمواقع التواصل الإجتماعي كالفايسبوك والأنستغرام مما يؤدي إلى تواصل أكثر بين مستخدمي هذه المواقع في جميع أنحاء العالم، فهذا يعني أنه يمكن أن تظهر مستقبلا أنواع أخرى من الجرائم المعلوماتية، لا يمكننا ضبطها ولا حتى التحكم فيها، لهذا ندعو جميع الهيئات العلمية منها أو الهيئات التشريعية وخاصة الجهات المستهدفة من طرف هذا النوع من الجرائم لتسليط الضوء أكثر على هذه المواضيع الجديرة بالذكر.

قائمة المراجع

1- أحمد خليفة المالط. الجرائم المعلوماتية. الإسكندرية، مصر: دار الفكر الجامعي، 2006.

2- البيومي، عبد الفتاح.مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنات. الاسكندرية، مصر: دار الفكر الجامعي، 2000.

3- العريان محمد علي. الجرائم المعلوماتية. الاسكندرية، مصر: دار الجامعة الجديدة، 2004.

4- أيمن عبد الحفيظ. الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية. الاسكندرية، مصر: [د.ن]، 2005.

5- سيبار أونيش. جرائم الكمبيوتر وجرائم أخرى في مجال المعلومات. ترجمة سامي الشوي. القاهرة، مصر: دار النهضة العربية، 1993.

6- صالح بن محمد المسند، وعبد الرحمان بن راشد المهيني. جرائم الحاسب الآلي خطر حقيقي في عصر المعلومات. "المجلة العربية للدراسات والتدريب. 2007: 181.

7- عبد الباقي جميل. القانون الجنائي والتكنولوجية الحديثة. القاهرة، مصر: دار النهضة العربية، 1992.

8- عبد الرحمان المويشر تركي. "بناء نماذج أمنية لمكافحة الجرائم المعلوماتية وقياس فعاليته". أطروحة دكتوراه: الرياض، المملكة العربية السعودية، كلية الدراسات العليا بجامعة نايف للعلوم الأمنية، 2009، 39.

9- عبد الرحمان حاتم ومنصور شحات. الاجرام المعلوماتي. القاهرة، مصر: دار النهضة العربية، 2003.

10- عبيد الكعبي محمد. الجرائم الناشئة عن الاستخدام الغير المشروع لشبكة الانترنات. القاهرة، مصر: دار النهضة العربية، 2004.

11- عمر أبو الفتوح الحمامي. الحماية الجنائية للمعلومات المسجل إلكترونيا –دراسة مقارنة- القاهرة، مصر: دار النهضة العربية، 2010.

12- فهد بن عبد الله الحديدان. الانترنات، شبكة المعلومات العالمية. الرياض، المملكة العربية السعودية: دار النشر غير معروف، 1992.

13- البيومي حجازي عبد الفتاح. جرائم الكومبيوتر والنترنات في القانون العربي. القاهرة، مصر: دار الكتاب القانونية، 2007.

14- محمد أمين أحمد الشوايكة. جرائم الحاسوب والانترنات.عمان: مكتبة دار الثقافة للنشر والتوزيع، 2004.

15- ناول عبد الهادي. "تقييم فعالية المواجهة التشريعية لجرائم الانترنات". عدل 31 رجب، 2006: 21.

16- نهلا عبد القادر المومني. الجرائم المعلوماتية. عمان: دار الثقافة، 2008.

الهوامش

[1] ناول عبدالهادي. "تقييم فعالية المواجهة التشريعية لجرائم الانترنات." عدل 31 رجب, 2006: ص31.

[2] عبيد الكعبي محمد. الجرائم الناشئة عن الاستخدام الغير المشروع لشبكة الانترنات. القاهرة، مصر: دار النهضة العربية، 2004. ص32.

[3] العربان محمد علي. الجرائم المعلوماتية. الاسكندرية، مصر: دار الجامعة الجديدة، 2004. ص43.

[4] عبد الفتاح البيومي. مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنات. الاسكندرية، مصر: دار الفكر الجامعي، 2000.ص45.

[5] سيبار أونيش. جرائم الكمبيوتر وجرائم أخرى في مجال المعلومات. ترجمة سامي الشوي. القاهرة، مصر: دار النهضة العربية، 1993، ص58.

[6] عبد الباقي جميل. القانون الجنائي والتكنولوجية الحديثة. القاهرة، مصر: دار النهضة العربية، 1992.ص 17.

[7] نهلا عبد القادر المومني. الجرائم المعلوماتية. عمان: دار الثقافة، 2008. ص55.

[8] نهلا عبد القادر المومني. المرجع نفسه. ص55.

[9] فهد بن عبد الله الحديدان. الانترنات، شبكة المعلومات العالمية. الرياض، المملكة العربية السعودية: دار النشر غير معروف، 1992.ص 58.

[10] عبد الرحمان حاتم ومنصور شحات. الإجرام المعلوماتي. القاهرة، مصر: دار النهضة العربية، 2003.ص 88.

[11] عمر أبو الفتوح الحمامي. الحماية الجنائية للمعلومات المسجل إلكترونيا –دراسة مقارنة- القاهرة، مصر: دار النهضة العربية، 2010. ص 80-81.

[12] عمر أبو الفتوح الحمامي. المرجع نفسه، ص 80-81.

[13] البيومي حجازي عبد الفتاح. جرائم الكومبيوتر والنترنات في القانون العربي. القاهرة، مصر: دار الكتاب القانونية، 2007.ص 45.

[14] أيمن عبد الحفيظ. الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية. الاسكندرية، مصر: [د.ن]، 2005.ص20.

[15] عبد الرحمان المويشر تركي. "بناء نماذج أمنية لمكافحة الجرائم المعلوماتية وقياس فعاليته". أطروحة دكتوراه: الرياض، المملكة العربية السعودية، كلية الدراسات العليا بجامعة نايف للعلوم الأمنية، 2009، 39ص.

[16] خليفة المالط، أحمد خليفة المالط. الجرائم المعلوماتية. الإسكندرية، مصر: دار الفكر الجامعي، 2006.ص 90.

[17] أيمن عبد الحفيظ. الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية. مرجع سابق.ص20.

[18] عبد الرحمان المويشر تركي. "بناء نماذج أمنية لمكافحة الجرائم المعلوماتية وقياس فعاليته". مرجع سابق.ص39.

[19] أيمن عبد الحفيظ. الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية. مرجع سابق.ص20.

[20] صالح بن محمد المسند، وعبد الرحمان بن راشد المهيني. جرائم الحاسب الآلي خطر حقيقي في عصر المعلومات. "المجلة العربية للدراسات والتدريب. 2007: ص182.

[21] محمد أمين أحمد الشوايكة. جرائم الحاسوب والانترنات.عمان: مكتبة دار الثقافة للنشر والتوزيع، 2004.ص75