

الجريمة الالكترونية: بعد جديد لمفهوم الإجرام

عبر منصات مواقع التواصل الاجتماعي.

Cyber crime: a new dimension to the concept of crime

Across social media platforms.

لامية طالة¹ ، كهيبة سلام²¹ جامعة الجزائر 3 (الجزائر)، lamia.tll@gmail.com² جامعة الجزائر 3 (الجزائر)، sellamkahina1@gmail.com

تاريخ النشر: 2020/12/30

تاريخ القبول: 2020/12/24

تاريخ الاستلام: 2020/06/20

ملخص:

لقد شهد العالم تطورات كبيرة في جميع المجالات والميادين خاصة الميدان التكنولوجي، فمن الأبواب التي طرقها هذه التطورات نجد تكنولوجيا وسائل الإعلام والاتصال، فبالرغم من حداثة العهد بهذه التكنولوجيا في مجتمعنا، إلا أنها ودون منازع استطاعت أن تفرض وجودها في حياة كل فرد، فقد ساهم التطور المعاصر في تبادل الأفكار والمعلومات إلى إحداث سلوكيات مقبولة وغير مقبولة. في جميع المجالات التي تتعلق بالفرد والمجتمع، وقد يؤدي الاستخدام المفرط لهذه المواقع، إلى تدني المنظومة القيمية نتيجة للتأثر بالثقافات المفتوحة، من أخطرها انتشار الجرائم الالكترونية، أو كما تسمى أيضا جرائم الانترنت، أو جرائم الكمبيوتر، أو جرائم المعلوماتية والتي تطوّرت بالتزامن مع التطورات التي تطرأ على التقنيات والتكنولوجيا والتي لا يقتصر استخدامها على الإنسان الخبير بل كذلك الإنسان الشرير الذي قد يوصف كمجرم لسعيه وراء أطماعه واقتناصه الفرص لتحقيق أغراضه غير المشروعة، ولا يتوانى عن استغلال التقنية لتطوير قدراته الإجرامية باستخدام شبكة المعلوماتية كوسيلة سهلة لتنفيذ العمليات الإجرامية، مما يلحق ضررا بالآخرين، ومن أجل ذلك لا بد من فهم ماهية هذه الظاهرة الإجرامية المستحدثة في الفضاء الرقمي، وفهم أدواتها وطبيعتها مرتكبيها، وسنحاول في مقالنا هذا تعريف الجريمة الالكترونية والمجرم الالكتروني، أنواعها، خصائصها وأسبابها وأهدافها، وأهم تأثيراتها على نفسية الفرد وقيم المجتمع، وكذا أبرز أساليب مواجهة الجرائم الالكترونية.

كلمات مفتاحية: الجريمة الالكترونية؛ مواقع التواصل الاجتماعي؛ المجرم الالكتروني؛ الأمن المعلوماتي؛ الفضاء السيبراني.

Abstract:

The world has witnessed great developments in all fields and fields, especially the technological field. One of the doors that these developments have touched upon is the technology of the media and communication. The contemporary exchange of ideas and information leads to the creation of acceptable and unacceptable behaviors in all areas that relate to the individual and society, and the excessive use of these sites may lead to a decline in the value system as a result of influencing open cultures, the most dangerous of which is the spread of cybercrime, or also called cybercrime, or Computer crimes, or information crimes, which have developed in conjunction with developments in technologies and technology that are used not only for good people but also for the evil person who may be described as a criminal for his pursuit of his ambitions and seizing opportunities to achieve his illegal purposes, and he does not hesitate to use technology to develop his criminal capabilities using Information network as an easy way to carry out criminal operations, which harm others. For this, it is necessary to understand what this criminal phenomenon created in the digital space, and to understand its tools and the nature of its perpetrators, and in this article we will try to define electronic crime and cybercriminals, their types, characteristics, causes and goals, and the most important effects on the psyche of the individual and the values of society, as well as the most prominent methods of confronting crimes.

Keywords: Electronic crime; Social Media; Cyber criminal; Information security, cyberspace.

*المؤلف المرسل

1. مقدمة:

يعرف العصر الذي نعيش فيه اليوم بعصر المعلومات، وهو العصر الذي يعرف انفجارا في حجم المعلومات، وسرعة وسهولة انتشارها وتداولها بين الأشخاص، وقد ساهم في هذا الانتشار المذهل للتكنولوجيا الحديثة، وبشكل خاص الحواسيب والأجهزة الالكترونية الأخرى كاللوحات الالكترونية والهواتف الذكية، التي تساعد في نشر وتبادل المعلومات في أشكال مختلفة من صور وملفات وأشكال أخرى.

وقد غزت هذه الوسائل، بالإضافة إلى التطبيقات التي تتوفر على الانترنت والبرامج المعلوماتية المختلفة، كل ميادين الحياة، فأثرت وحولت أنماط الاتصال الشخصي والجماهيري، والمؤسساتي، وغيّرت من طرق المعاملات في مختلف المؤسسات، فطغى استخدام التعاملات عن طريق البطاقات الرقمية في مجالات عدة، خاصة المالية والمصرفية.

إن انتشار استخدام التكنولوجيا الحديثة للإعلام والاتصال، فرض واقعا جديدا أو فضاء رقميا يسمى بالفضاء السيبراني أو الافتراضي، أثر هذا الفضاء على حياة الأشخاص والمؤسسات، فترتبت عنه آثارا إيجابية عدة، لكن وبالمقابل أنتج العديد من الظواهر السلبية، لعل أهمها انتشار الجرائم الالكترونية، أو كما تسمى أيضا جرائم الانترنت، أو جرائم الكمبيوتر، أو جرائم المعلوماتية والتي تطوّرت بالتزامن مع التطورات التي تطرأ على التقنيات والتكنولوجيا والتي لا يقتصر استخدامها على الإنسان الخير بل كذلك الإنسان الشرير الذي قد يوصف كمجرم لسعيه وراء أطماعه واقتناصه الفرص لتحقيق أغراضه غير المشروعة، ولا يتوانى عن استغلال التقنية لتطوير قدراته الإجرامية باستخدام شبكة المعلوماتية كوسيلة سهلة لتنفيذ العمليات الإجرامية، مما يلحق ضررا بالآخرين.

وقد سجلت الجريمة الالكترونية معدلات هائلة في مختلف دول العالم، مما أدى إلى دق ناقوس الخطر، ومحاولة إيجاد سبل مكافحتها والحد منها، فمميزاتها وخصائصها تجعلها خطرا، بل وتستهدف الاعتداء على الحياة الشخصية للأفراد وممتلكاتهم وفكرهم وإبداعهم، حيث أخذت الجرائم الالكترونية تنتشر لتشكّل خطرا على الممتلكات المالية والمالية للأفراد والمؤسسات والدول، وكذلك على الممتلكات الفكرية، كما أنها أصبحت تهدد قيم المجتمعات وحياة أفرادها، وتشكّل أيضا تهديدا للأمن القومي، إذ يمكن لمجرمي الإنترنت العمل من أي مكان في العالم، واستهداف أعداد كبيرة من الناس أو الشركات عبر الحدود الدولية، وتزداد التهديدات التي تفرضها استنادا إلى نطاق وحجم الجرائم، والتعقيد التقني لتحديد هوية الجناة، ومن خلال ما سبق يمكن طرح السؤال التالي: ما هي الجريمة الالكترونية؟ وكيف هو شكل الإجرام عبر منصات مواقع التواصل الاجتماعي؟.

أهمية الدراسة: حيث تبرز هذه الأهمية في أن يرجع سبب اختيار الموضوع التعريف بظاهرة جديدة هي الجريمة الالكترونية التي بدأت في الظهور والانتشار وارتبطت بتكنولوجيا الحاسبات الآلية مما أسفر عن تمييزها بمجموعة من الخصائص تختلف عن غيرها من الجرائم مما يستتبع ضرورة التعامل معها بما يتلاءم من هذه الخصوصية، ولما كانت هذه الجرائم ترتبط بتقدم المجتمعات فكلما ازداد اعتماد المجتمع على الحاسبات الآلية كلما كان ذلك إيذانا بزيادة معدل جرائم المعلوماتية كان لزاما أن يواكب هذا التقدم فهما كاملا للجريمة المعلوماتية وكيفية مواجهتها سواء من الناحية التقنية وهو عمل المتخصصين في مجال تكنولوجيا المعلومات أو من الناحية القانونية وهي مهمة المشتغلين بالقانون.

1. مفهوم الجريمة الإلكترونية:

لقد أدى الانتشار الكبير للتكنولوجيا الحديثة، والتطور المذهل للجريمة الإلكترونية الناتجة عنها إلى زيادة اهتمام الباحثين والمختصين من ميادين عدة كالقانون، الإعلام والاتصال، السياسة، الاقتصاد، علم النفس وغيرها بموضوعها، مما أدى إلى تنوع تعريفاتها ومسمياتها، ومن ثم صعوبة إيجاد تعريفا جامعا مانعا لها، فمنهم من عرفها من الجانب التقني الفني والبعض الآخر من الجانب القانوني، وكما يقول فان دير هيلست وونيف " هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية (مرعي، 2016).

يتكون مصطلح الجريمة الإلكترونية cyber crime من جزأين هما: الجريمة والإلكترونية، وهو يجمع بين المفهوم العام للجريمة وطابعها الإلكتروني.

والجريمة هي خرق لمعايير وضوابط المجتمع، وهي ضرر يصيب الفرد والمجتمع، ويقرر له القانون الذي يحمي ويمثل الهيئة الاجتماعية عقابا أو جزاء جنائيا (غفور، 2015، ص 16).

ويعتبر علماء الاجتماع الجريمة ظاهرة اجتماعية، وأنّ التّجريم ليس حكرا على المشرع- رجال القانون- بقدر ما هو مستمد من الواقع الاجتماعي بما يحويه من قيم ومعايير اجتماعية (غفور، 2015، ص 41)، أي أن الجريمة عبارة عن خروج عن معايير المجتمع أو عن قواعد الإجماع، أي القواعد التي يحددها المجتمع وتحكم سلوك أفرادها، أو هي تلك الأفعال التي تمّل خطرا على المجتمع وتجعل من المستحيل تحقيق التعايش والتعاون بين الأفراد الذين يؤلفون المجتمع، أو هي كلّ مخالفة لمشاعر الولاء الاجتماعي، وهذا ما ذهب

إليه دوركايم وميرتون عندما اعتبرا الجريمة سلوكا لا معياريا أي منحرفا عن المستوى المعياري في المجتمع (غفور، 2015، ص 42).

أما قانونا، فيجمع الفقهاء على اعتبار الجريمة أو السلوك الإجرامي: "كل فعل أو امتناع عن سلوك أو فعل يجرمه المشرع وينص له قانون، يمثل قاعدة جزائية تطبق على الخارجين عنها". ومن التعاريف القانونية المشهورة للجريمة تعريف العالم سذرلاند الذي يقول فيه: "أن الجريمة هي السلوك الذي تجرمه الدولة لما يترتب عليه من ضرر على المجتمع، والذي تتدخل لمنعه بعقاب مرتكبيه"، ويرتبط تعريف الجريمة من هذه الناحية بقانون العقوبات من جهة، وبالمجتمع من جهة أخرى، فهي فعل ما يعاقب عليه المجتمع ممثلا في مشرعه، لما ينطوي عليه هذا الفعل من المساس بشرط يعده المجتمع من الشروط الأساسية لكيانه أو من الظروف المكتملة لهذه الشروط (غفور، 2015، ص 45).

أما بالنسبة للالكتروني فهي طابع هذه الجريمة التي يستخدم فيها المجرم الأجهزة و البرامج و التطبيقات الالكترونية، لذا تعرف الجرائم الإلكترونية باختصار على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الهاتف الجوال.

وتعرف الجريمة المعلوماتية بأنها: "أية جريمة ضد المال مرتبطة باستخدام المعالجة الإلية للمعلومات، كما تعرف بأنها: الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح"، أو أنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن إن تكون جديرة بالعقاب، كما تعرف بأنها مجموعة الجرائم المتصلة بعلم المعالجة المنطقية للمعلومات" (سالم و هجيج، 2007، ص 87).

ويرى عبد الفتاح مراد جرائم الانترنت على أنها: "مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة الكترونية أو شبكة الانترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها" (مراد، 2007، ص 38).

اقترح بعض المؤلفين تعريفاتهم من خلال استهداف الكمبيوتر كوسيلة لارتكاب الجريمة. بحسب Tidemann تغطي الجرائم الالكترونية "أي عمل غير قانوني يرتكبه جهاز الكمبيوتر"، بالنسبة لـ COMER فإن "سوء النية المالي الذي يستخدم بيئة تكنولوجيا المعلومات هو احتيال معلوماتي"، أما Parker، فقد اعتبر أن جرائم الكمبيوتر هي: "أي عمل غير قانوني تتطلب معرفة متخصصة بأجهزة الكمبيوتر، والتي تستجوب تحقيق الشرطة أو الملاحقة الجنائية" (Chawki, 2006, P 26).

وتعرف الجريمة الالكترونية قانونا بأنها:

◀ مجموعة الأفعال والأنشطة المعاقب عليها قانونا والتي تربط بين الفعل الإجرامي والثورة التكنولوجية.

◀ نشاط جنائي يمثل اعتداء على برامج الحاسب الآلي.

◀ الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني.

◀ الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح (ريان، 2002، ص03).

وقد أشار المشرع الجزائري للجريمة الإلكترونية لكنه لم يعرفها، وإنما تبنى للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة (الجريدة الرسمية، 2004)، ويمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لا بد من تحققه حتى يمكن توافر أركان الجريمة استنادا إلى قانون العقوبات الجزائري المعدل والمتمم لم يعرف جرائم الانترنت، بل اكتفى بالعقاب على بعض الأفعال، تحت عنوان الجرائم الماسة بنظام المعالجة الآلية للمعطيات (الجريدة الرسمية، 2004)، كما صدر قانون يتضمن القواعد

الخاصة للوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، نصّ على أحكام إجرائية تتعلق بكيفيات التحقيق في هذه جرائم، وأدرج عقوبات تسلّط على كل من يعرقل حسن سير التحقيقات القضائية في هذا المجال (الجريدة الرسمية، 2009).

2. أركان الجريمة الإلكترونية:

بما أن الجريمة الالكترونية فعل إجرامي يعاقب عنه القانون فهي تقوم على نفس أركان الجريمة العادية والمتمثلة في الركن الشرعي والمادي والمعنوي (عاقلي، 2017، ص 119):

◀ الركن الشرعي: معناه اعتراف المشرع والنص على تجريم الفعل المرتكب، " لا

جريمة ولا عقوبة إلا بنص"، بالنسبة للتشريع الجزائري فقد احدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث خاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات (عاقلي، 2017، ص 121).

◀ الركن المادي: يتكون الركن المادي للجريمة الالكترونية من السلوك الإجرامي

والنتيجة والعلاقة السببية، علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها، مثلا: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل، ويتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل ايجابي مرتكب، مثلا: جريمة الغش المعلوماتي: الركن المادي فيها هو تغيير الحقيقة في التسجيلات الالكترونية أو المحررات الإلكترونية (حسني، 1992، ص 04).

◀ الركن المعنوي: يتكون الركن المعنوي للجريمة الإلكترونية من عنصريها أي

العلم، أي إدراك الفاعل للأمور والإرادة، بمعنى اتجاه السلوك الإجرامي لتحقيق النتيجة.

3. مراحل تطور الجريمة الإلكترونية:

مرتطور الجرائم الإلكترونية بثلاثة مراحل تبعا لتطور التقنية واستخدامات الحاسوب.

◀ **المرحلة الأولى:** بظهور استخدام الكمبيوتر و ربطه بالشبكة في الستينات إلى السبعينيات، حيث ظهرت أول معالجة لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي، وشكلت موضوع التساؤل إذا ما كانت هذه الجرائم مجرد حالة عابرة أم ظاهرة إجرامية مستجدة ؟و هل هي جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في مجال المعلوماتية؟ ، فبقيت محصورة في إطار السلوك اللا أخلاقي دون النطاق القانوني و مع توسع الدراسات تدريجيا و خلال السبعينات بدا الحديث عنها كظاهرة إجرامية جديدة.

◀ **المرحلة الثانية:** في بداية الثمانينات، تؤكد مفهوم جديد لجرائم الكمبيوتر والانترنت حيث ارتبطت هذه الأخيرة بعمليات اقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدمير كلي للملفات أو البرامج،و شاع اصطلاح "الهكرز " المعبر عن مقتحمي النظم وكذا المجرم المعلوماتي المتفوق.

◀ **المرحلة الثالثة:** حيث شهدت فترة التسعينات تناميا هائلا في حقل الجرائم الإلكترونية وتغييرا في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيلات لعمليات دخول الأنظمة واقتحام شبكة المعلومات ظهرت أنماط جديدة وخطيرة في ذات الوقت، بحيث نمت الإنترنت بشكل مذهل خلال هذه الفترة، بعد ما كانت مجرد شبكة أكاديمية صغيرة وتحولت إلى بيئة متكاملة للاستثمار والعمل والإنتاج والإعلام والحصول على المعلومات ، وفي البداية لم

يكن ثمة اهتمام بمسائل الأمن بقدر ما كان الاهتمام ببناء الشبكة وتوسيع نشاطها، دون مراعاة تحديات أمن المعلومات، فالاهتمام الأساسي تركز على الربط والدخول ولم يكن الأمن من بين الموضوعات الهامة في بناء الشبكة. وهذه الثغرة التي شجعت تنامي الجريمة الإلكترونية وتسببت في أضرار بالغة، وهو ما أدى إلى لفت النظر إلى حاجة شبكة الإنترنت إلى توفير معايير من الأمن، وبدأ التفكير ملياً في الثغرات ونقاط الضعف، وعليه قد يكون الكمبيوتر هدفاً للجريمة، وغايته المعلومات المخزنة والسيطرة على النظام دون التصريح والسرقه والاعتداء على الملكية الفكرية وغيرها.

كما قد يكون الكمبيوتر محل للجريمة، كحالة استغلال الكمبيوتر للاستيلاء على أموال الغير بإجراء تحويلات غير شرعية، كما أن الكمبيوتر قد يعد أداة للجريمة، كحالة تخزين البرامج المنسوخة أو في حالة استخدامه لنشر المواد غير قانونية (الأشقر جبور، 2008، ص 70-71).

4. جرائم الإنترنت... ثالث أكبر تهديد:

يقول "Colin ROSE" تشكل جرائم الإنترنت ثالث أكبر تهديد للقوى العظمى، بعد الأسلحة الكيماوية والبكتريولوجية والنووية"، ووفقاً لمنطق ROSE المتخصص في الجرائم الإلكترونية للشركة الاسكتلندية الدولية Buchanan تصنف الجريمة الإلكترونية في المرتبة الثالثة بالنسبة لتهديدات القوى العظمى بعد الأسلحة الكيماوية والبكتريولوجية والنووية.

مثال على تطور هذه التهديدات الإلكترونية نجد عملة البيتكوين bitcoin وهي عملة افتراضية يمكن استخدامها بشكل مجهول، تحظى بشعبية لدى مجرمي الإنترنت في غسيل الأموال وتمويل الإرهاب... ففي الوقت الذي توغلت فيه الإنترنت في كل مكان، ومع

تزايد قوة شبكة الويب المظلمة Dark Web ، تبرز الجريمة الإلكترونية على أنها " تهديد القرن الحادي والعشرين ."

أصبحت الجرائم الإلكترونية مشكلة مجتمعية ، سواء بالنسبة للحكومات أو الشركات أو المواطنين، وهذه فقط البداية، فكل الدراسات نتوقع زيادة كبيرة في عدد الجرائم المتعلقة بالإنترنت على مر السنين ولعقود قادمة... وهذا تحدي حقيقي للدول وقوات الشرطة في جميع أنحاء العالم (Azzouzi, 2010, P 86).

5. أطراف الجريمة الالكترونية:

تشابه الجريمة الالكترونية مع الجريمة التقليدية في أطراف الجريمة من مجرم ذي دافع لارتكاب الجريمة وضحية والذي قد يكون شخص طبيعي أو شخص معنوي، وأداة ومكان الجريمة، ويكمن الاختلاف الحقيقي بين نوعي الجريمة في الأداة ذات تقنية عالية التي تمارس بها الجريمة الالكترونية مكان الجريمة الذي لا يتطلب انتقال الجاني إليه جسدياً، فالكثير من تلك الجرائم تتم عن بعد باستخدام الأجهزة الالكترونية و خطوط وشبكات الاتصال بين الجاني ومكان الجريمة.

إن الجرائم المعلوماتية كغيرها من الجرائم تحتاج إلى طرفين جاني ومجني عليه، إلا إن أطراف الجريمة المعلوماتية يختلفون نوعاً ما عن أطراف باقي الجرائم، ومما لاشك فيه أن الشخص الطبيعي هو الذي يربى فرصة استغلال الوسيلة المعلوماتية لإجراء الجريمة، وقد يكون عبارة عن مجموعة أشخاص تمثل شخصاً معنوياً، والشخص الطبيعي والمؤسسات العامة والبنوك وغيرها التي تحمل صفة الشخص المعنوي معرضون لاعتداءات عن طريق هذه الشبكة من المعلومات.

ويمكن تحديد أطراف الجريمة المعلوماتية بالآتي:

1. المجرم المعلوماتي: في الجريمة المعلوماتية لا نكون بصدد مجرم عادي بل أمام

مجرم ذي مهارات تقنية وذو علم بالتكنيك المستخدم في نظام الحاسبات الآلية، فشخصية المجرم المعلوماتي سواء أكان طبيعياً أو معنوياً، وآلية ارتكاب الجريمة

تجعل منه شخصاً يتسم بسمات خاصة تضاف إلى الصفات الأخرى التي يجب أن تتوافر في المجرم العادي، ولعل أهم ما يتميز به الشخص المذكور أنه يتوافر لديه خبره بالمسائل المعلوماتية ومعرفة كافية بالية عمل الحاسب الآلي وتشغيله باعتبار إن الإجرام المعلوماتي ينشأ من تقنيات التدمير الهائلة التي تتمثل بالتلاعب بالمعلومات والكيانات المنطقية أو البيانات، بيد أنه ذلك لا يعني إمكانية تصور العنف الموجه ضد النظام المعلوماتي، فقد يكون محل الجريمة إتلاف الحاسب الآلي ذاته أو وحدة المعالجة المركزية، أي إن ما يمكن الاعتداء عليه قد يكون بهيكلية الحاسبات لا بمعلوماتها المتنقلة عبر شبكة المعلومات (سالم و هجيج، 2007، ص 88).

ويمكن تقسيم الجناة في جرائم الانترنت أو كما يطلق عليهم "القراصنة إلى:

◀ الهاكرز: ويُطلق هذا الاسم على القراصنة الذين يتخذون من الجرائم الإلكترونية، والقراصنة هواية أو فضولي ليس أكثر ويكون غرضها تخريبياً ليس هادفاً لغايات، وتكون غالباً من الفئة الشبابية المصابة بهوس التعمق بالمعلومات الإلكترونية والحاسوب.

◀ الكرakers: وهم القراصنة المحترفون، ويعد هذا النوع من أكثر أنواع مرتكبي الجرائم الإلكترونية خطورة، ويكون القراصنة من هذه الطائفة ذوي مكانة اجتماعية عادية أو متخصصين في العلوم الإلكترونية.

◀ الطائفة الحاقدة: وتستهدف غالباً هذه الطائفة المنظمات والمنشآت وأرباب العمل، ويكون الهدف من ارتكابها للجريمة بحق هذه الأطراف عادة بغية الانتقام والحصول على المنفعة المادية أو السياسية، وقد يكون متطرف أو جاسوس أو مخترق الأنظمة (مراد، 2007، ص 65).

حتى يتمكن القراصنة من تنفيذ جريمتهم الإلكترونية يستلزم توفر أدوات عدة أبرزها: الاتصال بشبكة الإنترنت، توفر برمجيات خاصة لنسخ المعلومات المخزنة عند المستخدم على جهاز الحاسوب، وسائل التجسس، ومنها ربط الكاميرات بخطوط الاتصال الهاتفي، البار كود، وهي عبارة عن أدوات تستخدم لمسح الترميز الرقمي وفك شفرة الرموز، طابعات، هواتف رقمية ونقالة (مراد، 2007، ص 68).

2. المجني عليه في الجريمة المعلوماتية: فكما يمكن أن يرتكب جرائم المعلوماتية

شخص طبيعي أو معنوي فإن المجني عليه في تلك الجرائم قد يكون كذلك أيضا، مع انه الغالبية العظمى من هذه الجرائم تقع على شخص معنوي يتمثل بمؤسسات وقطاعات مالية وشركات ضخمة، إلا أن المعلومات المجردة تعد في الوقت الحاضر من أهم المصالح المستهدفة بعد الأموال وخصوصا إذا كانت هذه المعلومات ذات أهمية بالغة، وكان هدف المجرم المعلوماتي هو الحصول على مقابل وعوض عن طريق المقايضة غير المشروعة لهذه المعلومات أو بيعها لغير أصحابها الشرعيين، وسواء كانت المعلومات مخزنة بذاكرة الحاسوب أم مدخلة في بنوك المعلومات إذ يتم تشويشها وإظهارها على غير حقيقتها ويدخل في هذا النوع ما يتعلق بأسرار الدولة والمشاريع الصناعية (سالم وهجيج، 2007، ص 88-89).

6. خصائص الجريمة الإلكترونية:

تتميز الجريمة الإلكترونية بجملة من الخصائص التي تجعل عملية محاربتها صعبة نوعا ما، وتجعل الدول والمنظمات تجتهد لإيجاد الآليات المناسبة لمكافحتها، وترتبط هذه الخصائص بمميزات الأجهزة الإلكترونية التي تستخدمها والبرامج وشبكة الانترنت ومختلف التطبيقات التي توظفها، ومن أهم هذه الخصائص نذكر:

◀ العالمية: بمعنى أنها تتعدى الحدود الجغرافية للدول، إنها جرائم عابرة للقارات، لأنه مع انتشار شبكة الاتصالات العالمية والانترنت أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة حيث يمكن إن يكون الجاني في بلد والمجني عليه في بلد آخر (مراد، 2007، ص 42).

◀ صعوبة الإثبات: صعوبة متابعتها واكتشافها بحيث لا تترك أثرا فهي مجرد أرقام تتغير في السجلات، فمعظم الجرائم الالكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، ويلاحظ أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها، على أساس أنها تفتقر إلى الدليل المادي التقليدي كال بصمات، كما يصعب الاحتفاظ الفني بأثارها إن وجدت، تحتاج لخبرة فنية خاصة يتعذر على المحقق التقليدي منالها أو التعامل معها، لأنها تعتمد غالبا على قمة الذكاء المصحوب بالخداع والتضليل بدس برامج أو وضع كلمات سرية ورموز تعوق الوصول إلى الدليل وقد يلجا مرتكبها لتشفير التعليمات لمنع إيجاد أي دليل يدينه (رستم، 1994، ص 24).

◀ النعومة: إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل، السرقة، وغيرها، فالجرائم الالكترونية لا تتطلب أدنى مجهود عضلي ممكن، بل تعتمد على المجهود الذهني المحكم، والتفكير العلمي المدروس القائم عن معرفة تقنية ممتازة بالحاسب الآلي، والتعامل السليم بالشبكة، على أساس أن الجاني في الجرائم الالكترونية هو إنسان متوافق مع المجتمع ولكنه يقترب هذا النوع من الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يشتغل بها، وأكد لتحقيق مصلحة ما (مراد، 2007، ص 46).

◀ **عدم التبليغ:** عند وقوع الجريمة بواسطة الانترنت نجد إن بعض المجني عليهم يمتنعون عن إبلاغ السلطات المختصة خشية على السمعة والمكانة، وعدم اهتزاز الثقة في كفاءته خاصة إذا كان كيان أو هيئة معينة.

هذا بالإضافة إلى اتسامها بمجموعة من الخصائص الأخرى، أهمها:

◀ أنها جريمة غير مقيّدة بزمان ومكان إذ تمتاز بالتباعد الجغرافي وعدم تقيدها بالتوقيت الزمني.

◀ سهولة إخفاء آثار الجريمة والأدلة التي تدلّ على الجاني نظراً للترميز والتشفير الذي يحدث على الرموز المخزنة على وسائط التخزين الممغنطة.

7. أسباب الجريمة الالكترونية:

هناك عدد من الأسباب التي يمكن حصرها كأسباب للجريمة الإلكترونية، منها ما يقع على مستوى كوني، ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى فردي أو شخصي، كما أن أسباب الجريمة الإلكترونية تتفاوت وفق نوعها ونوع المستهدف ونوع الجاني ومستوى تنفيذه (فردية، مجتمعية، كونية)، فجرائم الشباب والهواة والصغار تختلف عن أسباب جرائم المحترفين، وتختلف وفق هدفها سرقة أو معلومات أو تجارة بالمعلومات أو شخصية..

1.7 أسباب الجريمة على المستوى الفردي: يرجع المختصون أسباب ارتكاب الجرائم الالكترونية على مستوى الفرد إلى (البداينة، 2014، ص 13):

◀ البحث عن التقدير: هناك بعض الجرائم الإلكترونية التي يرتكبها شباب طائش وصغار سن، وذلك من باب التحدي، وحب الظهور في الإعلام، وغالباً ما تتوقف هذه الفئة عن مثل هذه السلوكيات في عمر لاحق بعد سن العشرينيات.

◀ الفرصة: لقد وفرت التقنيات الحديثة والانترنت فرصاً غير مسبقة لانتشار الجريمة الالكترونية، فقد ولدت بيئة قد تشكل المعلومات فيها

هدفاً سهل المنال ويحقق المنفعة السريعة، وبالتالي يمكن سرقتها أو سرقة محتوياتها فهي فرصة مربحة وقليلة المخاطر واحتمالية الكشف للفاعل فيها ضئيلة.

◀ ضبط الذات المنخفض: يتعرض الأفراد على الإنترنت لنماذج التعلم الإجرامي والأقران قد يكونون أكثر ميلاً للانخراط في الجريمة الإلكترونية ونظرية التعلم الاجتماعي نظرية قد يكون لها تطبيق خاص عندما يتعلق الأمر بالجرائم الإلكترونية، فالمجرمين غالباً ما يحتاجون إلى تعلم تقنيات فالنظرية العامة للجريمة ونظرية التعلم الاجتماعي تريان إن الأفراد يتصرفون في البيئة الافتراضية كما يتصرفون في العالم الحقيقي، ويكون الأفراد ذوي التصرف الطائش والذين يمتازون بضبط الذات المنخفض على استعداد لارتكاب الجرائم الالكترونية، خاصة إذا كانوا ممن يحسن استعمال التكنولوجيا الجديدة.

◀ النشاط الروتيني: يمكن تفسير زيادة ضحايا الجريمة الإلكترونية من خلال التغييرات في أنشطة الناس الروتينية في الحياة اليومية، فمع ظهور شبكة الإنترنت فقد تغيرت طريقة الناس التي يتواصلون فيها أو يتفاعلون مع الآخرين في العلاقات الشخصية والترفيه والتجارة، ذلك أن التغييرات في أنشطة الناس الروتينية مثل استخدام الانترنت وشبكات التفاعل الاجتماعي مثل الفيسبوك والايمل والمواقع وغيرها قد خلقت فرصاً للجنة المتحفزين مع وجود أهداف قيمة وسهلة في الحيز الفضائي مع غياب الحراسة، يرى كوهين وفيلسون أنه من المرجح أن تحدث الجريمة عندما تتلاقى ثلاثة عوامل هي الجاني المتحفز والهدف المناسب وغياب الحراسة أنه لا بد من توافر هذه العوامل الثلاثة من أجل أن تحدث الجريمة وعدم وجود واحد من هذه العوامل هو كافي لمنع حدوث الجريمة.

2.7 أسباب الجريمة على المستوى المجتمعي (البداينة، 2014، ص 14):

- ◀ التحضر: يعد التحضر أحد أسباب الجريمة الإلكترونية عامة حيث الهجرة الكبيرة من الريف إلى المدينة ولي المناطق الحضرية والمدن الكبيرة وعادة ما يهاجر الشباب غير المتمكنين من مواجهة متطلبات الحياة الحضرية باهظة التكاليف، والتي تتطلب مهارات عالية أحيانا مما يجعل شرائح كبيرة من المهاجرين غير قادرين على تلبية متطلبات الحياة الحضرية مما يجعلهم يعيشون في مدن الصفيح والأحياء الطرفية والهامشية وكنتيجة يجد الناس أنفسهم في تنافس غير قادرين على مجاراته مما يجعلهم يلتفتون إلى الاستثمار في الجريمة الإلكترونية.
- ◀ البطالة: ترتبط الجريمة الإلكترونية شأنها شأن الجريمة التقليدية بالبطالة والظروف الاقتصادية الصعبة وتتركز البطالة بين قطاعات كبيرة من الشباب، لذا سيستثمر الذين يملكون المعرفة ذلك في النشاط الإجرامي الإلكتروني.
- ◀ الضغوط العامة: تعد الضغوط العامة التي يتعرض لها المجتمع من فقر وبطالة وأمية وظروف اقتصادية صعبة وعوامل ضاغطة على المجتمع عامة وخاصة على قطاع الشباب مما يولد مشاعر سلبية عند شرائح كبيرة من الناس ضد الظروف وضد المجتمع مما يدفعهم إلى أساليب تأقلم سلبية مع هذه الظروف منها الاتجار الإلكتروني بالبشر والجنس والجريمة الإلكترونية وغيرها.
- ◀ البحث عن الثراء: يسعى الإنسان إلى المتعة ويتجنب الألم هكذا تقول النظرية العامة في الجريمة لجتفردسون وهيرشي Gottfredson and Hirschi، ويسعى الناس إلى الوسائل غير المقبولة اجتماعيا لتحقيق أهداف مقبولة اجتماعيا كما ترى نظرية الأنومي لميرتون فالرغبة في الثراء يواجهها صعوبات بالغة في تحقيقه بالطرق المقبولة اجتماعيا والقانونية ولذا يلجأ بعض الناس إلى الجرائم

الإلكترونية حيث المستهدف مجتمع أكبر وسهولة التنفيذ وسرعة المردود وقلة الخطورة.

◀ ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية: هناك الكثير من الدول التي لم تطور تشريعاتها وأجهزة العدالة فيها لكي تتمكن من مجاراة التقدم في الجرائم الإلكترونية وأساليبها وهذا لا يتوقف عند التشريعات وإنما يشمل الشرطة والتحقيق والقضاء وكيفية التعامل مع الأدلة الرقمية على المستوى الوطني كما هو الحال على المستوى الدولي فمما يشعل الجريمة الإلكترونية غياب التشريعات الجزائية والجنائية وضعف الممارسات العدلية والشرطية والقضائية في محاكمة والتحقيق في الجرائم الإلكترونية.

3.7 أسباب الجريمة على المستوى العالمي (البداينة، 2014، ص 15):

◀ التحول للمجتمع الرقمي: والذي يمتاز بتغيرات كمية في مقدار المعلومات المتدفقة ونوعيتها، فبفعل تكنولوجيا الاتصالات والمواصلات فأن الصور والمعلومات تغطي كافة المعمورة بسرعة ودقة، ووجود الشبكات حيث يتم تداول المعلومات بين جميع الأطراف مثل البريد الإلكتروني، الهاتف الجوال، وغيرها.

◀ العولمة: إن ظهور الفضاء الإلكتروني فضاء خصب لانتشار الجرائم الالكترونية، فالأشخاص الرقميين قد يرتكبون جرائم في الفضاء الإلكتروني لا يرتكبونها في الواقع المادي بسبب مكانتهم وموقعهم بالإضافة إلى ذلك، فمرونة الهوية وعدم ظهور الهوية وضعف عوامل الردع تحفز السلوك الإجرامي في العالم الافتراضي.

8. أنواع الجرائم الإلكترونية:

إن الجرائم الإلكترونية جرائم متعددة ومتنوعة، ويصعب حصرها بسهولة، فهي تشمل أي أمر غير مشروع بدءا من عدم تسليم الخدمات أو البضائع مروراً باقتحام الكمبيوتر، التسلل إلى ملفاته، وصولاً إلى انتهاك حقوق الملكية الفكرية، والتجسس الاقتصادي كسرقة الأسرار التجارية، والابتزاز عبر الانترنت، وتبييض الأموال الدولية وسرقة الهوية والقائمة مفتوحة لتشمل كل ما يمكن تصوره بما يمكن أن يرتكب عبر الانترنت من انحرافات، توجد عدة تصنيفات لجرائم الحاسب الآلي والانترنت فهناك من يصنفها بحسب الفئات مثل جرائم ترتكب على نظم الحاسب الآلي، أو بحسب الأسلوب المتبع في الجريمة أو الباعث الدافع لارتكاب، وتتمثل أهم أنواعها فيما يلي:

- ◀ **جريمة الدخول غير المشروع:** بمعنى دخول الشخص إلى شبكة الانترنت بدون ترخيصا من الجهة المخولة منح هذه الصلاحية، هذا الفعل يؤكد ارتكاب الجريمة عمدا عن طريق خرق التدابير الأمنية بقصد الحصول على بيانات الكمبيوتر.
- ◀ **تخريب أو إتلاف أجهزة المعلومات أو احدي مكوناتها:** إن حماية شبكة المعلوماتية يستلزم التدخل لتجريم الأفعال التي تهدف إلى تخريب أو تعطيل أو إتلاف الأجهزة المادية والمتمثلة في الحاسوب أو البيانات والمعلومات الموجودة بداخله لأن علة التجريم هي حماية المعلومات والأجهزة المادية من أفعال التخريب.
- ◀ **صناعة الفيروسات أو نشرها:** وهي وسيلة تستخدم لتدمير المعلومات والبيانات والبرامج وتعطيل شبكة المعلومات (عاقلي، 2017، ص 124).
- ◀ **الغش أو التغير في مواصفات وخصائص تقنية المعلومات:** تتحقق الجريمة بتغير الخصائص أو المواصفات بسلوك إيجابي يأتيه الفاعل بطرق تدليسية احتيالية بحيث تعرض تقنية المعلومات أو مكوناتها وما في حكمها إلى الغش الذي يعد انتهاكا لحقوق الملكية الفكرية.

◀ سرقة الأجهزة أو المكونات أو المعلومات وما في حكمها: تعتبر جريمة سرقة وإخلال بحقوق الملكية الفكرية أو براءة الاختراع أو العلامات المسجلة على أساس أن محل السرقة الحاسوب ككيان مادي.

◀ جرائم النظام العام والآداب العامة الاتجار في الجنس البشري: كالإخلال بالنظام العام والآداب، إنشاء أو نشر مواقع بقصد ترويج أفكار وبرامج مخالفة للنظام العام الآداب، انتهاك المعتقدات الدينية أو حرمة الحياة الخاصة، الإساءة إلى السمعة، والدعارة والمخدرات وغسيل الأموال.

◀ الجرائم المتعلقة بأمن الدولة وسلامتها الداخلية والخارجية: إن التمعن في قراءة النصوص المنظمة لجرائم الانترنت في التشريعات العربية تكشف عن حقيقة متواترة في جل هذه التشريعات، ألا وهي اهتمامها الكبير عند تنظيم الانترنت وضبطه، بجعل حماية الدولة وأمنها كهدف أسمى من طرف المشرع قبل حماية أمن المواطن، وهذه مسألة واضحة على مستوى النصوص.

◀ جرائم الإرهاب الاعتداء على الملكية الفكرية: إن المتضرر الأول من إساءة استخدام شبكة المعلوماتية حقوق الملكية الفكرية سواء ما يتعلق منها بحقوق المؤلف أو الحقوق المجاورة والمتعلقة بالبرامج والإصدارات الخاصة بنظم المعلومات أو بالمصنفات الفكرية أو الأدبية أو الأبحاث العلمية التي باتت متاحة على شبكة المعلوماتية ويتم نسخها وتداولها دون أن تنسب إلى صاحبها الأصلي وهو ما يلحق ضررا بليغا بهذه الطائفة من الحقوق التي تعرف بالذهنية أو الفكرية (عاقلي، 2017، ص 125).

9. أهم الجرائم الإلكترونية:

- يمكن اعتبار العمل الإجرامي المحدد قانوناً جريمة معلوماتية عندما يستهدف الهجوم:
- ◀ أمن المعلومات: أي مصداقيتها، وتوافرها، وصحتها، وتندرج في هذا الإطار، عمليات اختراق الأنظمة، عبر سرقة كلمة السر، أو التصيد، أو التضليل والاحتيال، كذا عمليات تدمير البيانات وسرقتها.
 - ◀ سلامة الأشخاص: كما هو حال التربص والترصد للأطفال، بغية الاعتداء عليهم، واستدراجهم، بهدف استغلالهم جنسياً، كما تندرج هنا عمليات استدراج الأشخاص، في إطار عمليات الاتجار بالرقيق، أو تجارة الأعضاء البشرية، أو إنتاج المواد الإباحية، أو تقديمها.
 - ◀ الأموال: من خلال عمليات الغش، والاحتيال، والتزوير، الابتزاز، تبييض الأموال، وغيرها.
 - ◀ المحتوى: كتوزيع مواد إباحية عن الأطفال، بث الكراهية، التمييز العنصري، عرض خدمات المرتزقة، الترويج للإرهاب.
 - ◀ أمن الدولة وسيادتها: مثل التجسس، التصنت، إفشاء معلومات سرية، والترويج لما يعرف بالإرهاب الإلكتروني.
 - ◀ الملكية الفكرية: والتي يدخل فيها سرقة البرامج والقرصنة، والاستعمال غير الشرعي لإنتاج محمي بالملكية الفكرية (الأشقر جبور، 2017، ص 50).

10. تصنيفات الجريمة الإلكترونية:

- ◀ جريمة إلكترونية تستهدف الأفراد ويُطلق عليها أيضاً مسمى جرائم الإنترنت الشخصية والتي تقتضي على الحصول بطريقة غير شرعية على هوية الأفراد الإلكترونية كالبريد الإلكتروني وكلمة السر الخاصة بهم وكما تمتد لتصل إلى انتحال الشخصية الإلكترونية وسحب الصور والملفات المهمة من جهاز الضحية

لتهديده بها وإخضاعه للأوامر، كما تُعتبر سرقة الاشتراك أيضاً من الجرائم ضد الأفراد.

◀ جريمة إلكترونية تستهدف الملكية يستهدف هذا النوع من الجريمة الجهات الحكومية والخاصة والشخصية ويركّز على تدمير الملفات الهامة أو البرامج ذات الملكية الخاصة ويكون ذلك عبر برامج ضارة يتم نقلها إلى جهاز المستخدم بعدة طرق من أبرزها الرسائل الإلكترونية.

◀ جريمة إلكترونية تستهدف الحكومات وهي هجمات يشنّها القراصنة على المواقع الرسمية الحكومية وأنظمة شبكاتها والتي تركز جل اهتمامها على القضاء على البنية التحتية للموقع أو النظام الشبكي وتدميره بالكامل ومثل هذه الهجمات في الغالب يكون الهدف منها سياسياً.

◀ النصب والاحتيال الإلكتروني.

◀ الجرائم السياسية الإلكترونية والتي تركز على استهداف المواقع العسكرية لبعض الدول لسرقة المعلومات التي تتعلق بأمن الدولة.

◀ سرقة المعلومات الموثقة إلكترونياً ونشرها بطرق غير شرعية.

◀ جرائم الشتم والسب والقذف.

◀ جرائم التشهير ويكون هدفها الإساءة لسمعة الأفراد.

◀ جرائم الاعتداء على الأموال أو الابتزاز الإلكتروني.

◀ الوصول إلى مواقع محجوبة.

◀ الإرهاب الإلكتروني.

◀ الجرائم الجنسية الإلكترونية.

◀ جرائم الاعتداء على الأموال (مؤسسات مصرفية ومالية وبنوك) (مرعي، 2016).

11. الجريمة في مواقع التواصل الاجتماعي:

يمتاز به هذا الفضاء الافتراضي من ايجابيات وتسهيل للتواصل بين الأفراد في جميع أنحاء العالم، إلا انه لا يخضع للمراقبة التي يمكن أن توفر حماية كافية لجميع مستخدميها، لا من ناحية نشر الأفكار ولا من ناحية مشاركة الصور، فتجعل المشترك مكشوفاً للعالم وتقلل من خصوصية حياته وبالتالي يمكن أن تستغل هذه المعلومات ضد صاحبها، أو أن يتعرض للتشويش الفكري بسبب أفكار متطرفة ينشرها البعض، خاصة إذا كان المشترك صغيراً في السن وليست له خلفية حول الموضوع المعرض له.

ورغم أن لهذه المواقع إجراءات تحمي الخصوصية إلا أنها غير كافية لأنها مواقع للتواصل الاجتماعي أولاً فالحماية المفرطة يمكن أن تعزل الفرد عن التواصل، ورغم محاولات التشريع الجزائي حماية الأفراد من الجرائم المتعلقة بالكمبيوتر إلا أن ما جاءت به مواقع التواصل الاجتماعي يختلف تماماً عن الجرائم الإلكترونية، وبالتالي أي شخص يمكن أن يكون عرضة لأن يصبح ضحية جريمة ما بسبب تواجده على مستوى هذه المواقع، حيث أصبحت تعتبر مواقع التواصل الاجتماعي فضاء محتمل للإيذاء خاصة لصغار السن فيما يتعلق بالاعتداءات الجنسية و التواصل غير المرغوب فيه، و العنف اللفظي (حطاب، 2017، ص 412).

هنالك نوعين من الأفعال التي ترتكب للإيذاء على مواقع التواصل الاجتماعي:

- ◀ أفعال جديدة غير مجرمة قانوناً رغم أنها ضارة.
- ◀ أفعال مجرمة بقانون العقوبات و لكنها ارتكبت في فضاء مواقع التواصل الاجتماعي بدلاً من أماكن أخرى.

وهذا الفعل الأخير المجرم بالقانون هو في العادة ما يرتكب على مواقع التواصل الاجتماعي، فالجريمة في مواقع التواصل الاجتماعي مشابهة جداً للجريمة في الواقع من

ناحية الأفعال المادية، فكلاهما يمكن أن تستهدف عرض الشخص أو ماله أو بدنه، كجرائم الابتزاز والنصب والتشهير والجرائم الجنسية، كما يمكن أن يعتمد المجرم على ما تقدمه هذه مواقع من خدمات من أجل تنفيذ جريمته على أرض الواقع.

الضحية في مواقع التواصل الاجتماعي:

من الصعب تحديد انتشار النشاط الإجرامي على مواقع التواصل الاجتماعي لأنه لا توجد حاليا إحصاءات شاملة عنها، وهذا يمكن أن يكون راجعا إلى العديد من العوامل، منها الطابع الواسع والمنفتح لمواقع التواصل الاجتماعي، جهل هوية المجرم، قلة وعي المستخدمين، الأمر الذي يمكن أن يخلق بيئة ناضجة للإيذاء.

و من أجل مواجهة هذه الجريمة سيتعين علينا الانتقال من سياسة الوقاية من الجريمة القائمة على أكتاف المنظمات الحكومية، إلى سياسة الوقاية من أن يصبح الفرد ضحية محتملة و التي هي معتمدة على المستويات الفردية و المجموعات الصغيرة، وأن يكون الأفراد أكثر وعيا و حذرا خاصة أولئك الأفراد الذين تزداد فرص تعرضهم لان يكونوا ضحية . و بالتالي فانه لا يمكن الاعتماد كليا على السياسة التشريعية الجزائية و لا على المؤسسات الأمنية و لا على منظومة العدالة الجزائية بصفة عامة، بل تعتمد الدولة أكثر في سياستها الجزائية في الوقاية من هذا النوع من الجرائم على توعية المجتمع و الارتقاء بفكره لاستيعاب مخاطر الجريمة و كيفية تجنبها (حطاب، 2017، ص 417).

إجراءات الوقاية ومنع الجريمة:

في حين أنه من المستحيل الحفاظ على نفسك تماما من أن تكون ضحية محتملة على مواقع التواصل الاجتماعي، إلا انه هنالك نصائح يمكن أن يتبعها أي مستخدم لهذه المواقع يمكن أن يمنحه حماية معقولة من التعرض لان يكون ضحية على موقع التواصل الاجتماعي وهي:

- ◀ توخ الحذر عند النقر فوق الروابط التي تتلقاها في رسائل من أصدقائك على مواقع التواصل الاجتماعي.
- ◀ لا تثق في أن الرسالة هي حقاً من الذي يقول أنها منه، يمكن للقراصنة اقتحام الحسابات وإرسال الرسائل التي تبدو وكأنها من أصدقائك ولكنها ليست كذلك، استخدم طريقة بديلة للاتصال بصديقك لمعرفة ذلك.
- ◀ اكتب عنوان موقع التواصل الاجتماعي الخاص بك مباشرة في المتصفح، إذا نقرت على رابط في موقع ويب آخر وأدخلت اسم حسابك وكلمة المرور فإنه يمكن أن يكون موقع وهمي حيث المعلومات الشخصية الخاصة بك يمكن سرقتها.
- ◀ أن تكون انتقائياً فيما يتعلق بقبول طلبات الصداقة لأنه قد يكون المرسل لص هوية وأنشأ ملامح وهمية من أجل الحصول على معلومات منك.
- ◀ اضبط ميزة تحديد الموقع الجغرافي، هذا هو الحل الأكثر مباشرة ويمكنك معرفة كيفية القيام بذلك بالنسبة لمعظم الهواتف.
- ◀ لا تنشر معلومات خاصة عنك التي يمكن أن تستغل ضدك.
- ◀ حافظ على خصوصيتك وخصوصية أصدقائك حماية لك ولهم.
- ◀ على الأولياء مراقبة نشاط أطفالهم على مواقع التواصل الاجتماعي ومراقبة أصدقائهم عليها وعلى المواد التي يتفاعلون معها والتي ينشرونها.

12. مكافحة الجرائم الإلكترونية:

يمكن أن نلخص أساليب مكافحة الجرائم الإلكترونية في الآتي:

- ◀ رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الإنترنت إذ يستلزم التدخل الحكومي والدولي نظراً للخطورة الجسيمة للأمر.
- ◀ الاعتماد على أساليب وتقنيات متطورة للتمكن من الكشف عن هوية مرتكب الجريمة والاستدلال عليه بأقل وقت ممكن.
- ◀ توعية الأفراد ونصحهم لماهية الجرائم الإلكترونية وكل ما يترتب عليها من مخاطر.

- ◀ الحرص على الحفاظ على سرية المعلومات الخاصة بالعناوين الإلكترونية كالحسابات البنكية، والبطاقات الائتمانية وغيرها.
- ◀ عدم الكشف عن كلمة السر نهائياً وتغييرها بشكل مستمر واختيار كلمات سر صعبة.
- ◀ تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب.
- ◀ تجنب تحميل أي برنامج مجهول المصدر.
- ◀ استمرارية تحديث برامج الحماية الخاصة بأجهزة الحاسوب.
- ◀ تأسيس منظمة خاصة لمكافحة الجرائم الإلكترونية والحد منها.
- ◀ المسارعة في الإبلاغ للجهات الأمنية فور التعرض لجريمة إلكترونية.
- ◀ مواكبة التطورات المرتبطة بالجريمة الإلكترونية والحرص على تطوير وسائل مكافحتها.
- ◀ استخدام برمجيات أمنة ونظم تشغيل خالية من الثغرات.
- ◀ الحرص على استخدام كلمات سرية للوصول إلى البرامج الموجودة على جهاز الحاسوب.
- ◀ عدم ترك جهاز الحاسوب مفتوحاً.
- ◀ فصل اتصال جهاز الحاسوب بشبكة الإنترنت في حال عدم الاستخدام.
- ◀ أخذ الحيطة والحذر وعدم تصديق كل ما يصل من إعلانات والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة.
- ◀ وضع الرقم السري بشكل مطابق للمواصفات الجيدة التي تصعب من عملية القرصنة عليه من هذه المواصفات بأن يحتوي على أكثر من ثمانية أحرف أن يكون متنوع الحروف والرموز واللغات وغيرها.

◀ يفضل تغيير كلمة المرور الخاصة بك بصفة دورية.

◀ لا تضع معلومات علي الانترنت لا تحب أن يراها الجميع من تعرفهم ولا تعرفهم وتذكر أنه بمجرد أن تضع معلومات علي الانترنت لن تتمكن أبدا من إرجاعها مرة أخرى حتى لو قمت بحذفها.

◀ معلوماتك الخاصة (اجعلها خاصة): إن معلوماتك الخاصة مثل اسمك بالكامل ورقم هاتفك ورقم الهوية ورقم بطاقتك الائتمان وأيضا عنوانك بالتفصيل هي معلومات خاصة لا يجب أن تتاح للجميع علي الانترنت لا شخص لا تعرفه فلا تفصح له عنها أو تضعها علي أي موقع لا تثق به. (مرعي، 2016).

خاتمة:

لقد أدى تطور انتشار تكنولوجيا الإعلام والاتصال إلى استحداث الكثير من المفاهيم المتعلقة بالبيئة الرقمية، من بين هذه المفاهيم نذكر المواطنة الرقمية، المواطن الرقمي، الإعلام الإلكتروني أو البديل، شبكات التواصل الاجتماعي، والجريمة الإلكترونية. تتشابه الجريمة الإلكترونية مع الجريمة التقليدية في أطراف الجريمة من مجرم ذي دافع لارتكاب الجريمة وضحية والذي قد يكون شخص طبيعي أو شخص اعتباري وأداة ومكان الجريمة، وهنا يكمن الاختلاف الحقيقي بين نوعي الجريمة ففي الجريمة الإلكترونية الأداة ذات تقنية عالية وأيضا مكان الجريمة الذي لا يتطلب انتقال الجاني إليه انتقالا فيزيقيا ولكن في الكثير من تلك الجرائم فإن الجريمة تتم عن بعد باستخدام خطوط وشبكات الاتصال بين الجاني ومكان الجريمة.

وقد أخذت الجرائم الإلكترونية تنتشر لتشكل خطرا على الممتلكات المالية للأفراد والمؤسسات والدول، وكذلك على الممتلكات الفكرية، كما أنها أصبحت تهدد قيم المجتمعات وحياة أفرادها، وتشكل أيضا تهديدا للأمن القومي، لذا تسعى الحكومات إلى سن قوانين لمكافحةها، ومن أجل ذلك لا بد من فهم ماهية هذه الظاهرة الإجرامية المستحدثة في الفضاء الرقمي، وفهم أدواتها وطبيعتها مرتكبيها، ولأجل ذلك لا بد من تضافر

جهود كل الأطراف من أكاديميين، مختصين نفسانيين وقانونيين وسياسيين للحد من تفشي هذه الجرائم التي تنتشر بسرعة فائقة وتستخدم تقنيات فائقة تصعب من إمكانية مكافحتها.

وهنا تجب الإشارة إلى أن المكافحة و الوقاية من الجريمة ليست دورا حكرًا على الدولة فقط، بل يستوجب أن يكون للمواطن أيضا مشاركة و مساهمة في هذه العملية، وهذا عن طريق تنمية ثقافته و وعيه الكافي بما يحيط به وتحسيسه بمخاطر الجريمة و كيفية تجنبها وكيفية الحماية منها، ونشر الأفكار المستنكرة والمحترقة لأي نوع من أفعال الإيذاء من شأنه أن يخلق مجتمع امن أكثر، و يوعي ويحمي الأجيال المستقبلية أيضا منها، وينشئ جيل صاعد واعي يتأقلم مع التطور بكل صوره دون الحاجة إلى خوف من استغلال هذا التطور لخدمة الجريمة.

إذن تشكل الجرائم الالكترونية تحديا كبيرا، للبيئة التي ترتكب فيها، إذ لا يمكن لمجرمي الإنترنت العمل من أي مكان في العالم، واستهداف أعداد كبيرة من الناس أو الشركات عبر الحدود الدولية، وتزداد التهديدات التي تفرضها استنادا إلى نطاق وحجم الجرائم، والتعقيد التقني لتحديد هوية الجناة وكذلك ضرورة العمل على الصعيد الدولي لتقديمهم إلى العدالة، فالإنترنت تمنح فرصا جديدة لمجرميها، على أساس الاعتقاد بأن إنفاذ القانون لا يعمل في عالم الإنترنت.

قائمة المراجع:

1. الأشقر جبور منى، (2017)، السيرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت.
2. الأشقر جبور منى، (2008)، القانون والانترنت: تحدي التكيف والضبط، مكتبة صادر ناشرون، بيروت.
3. البداينة موسى ذياب، (2014)، الجرائم الالكترونية: المفهوم والأسباب، الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان.
4. حسني محمود نجيب، (1992)، شرح قانون العقوبات: القسم الخاص، دار النهضة العربية، القاهرة.
5. خطاب حجة خيرة، (2017)، مواقع التواصل الاجتماعي.....فضاء جديد للجريمة، مجلة دراسات وأبحاث، العدد 28، السنة التاسعة.
6. رستم هشام محمد، (1994)، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني: الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، مصر.
7. ريان محمد عادل، (2002)، جرائم الحاسب الآلي وأمن البيانات، بيروت.
8. سالم محمد علي، هجيج حسون عبيد، (2007)، الجريمة الالكترونية، مجلة جامعة بابل للعلوم الإنسانية، المجلد 14، العدد 2.
9. عاقل فاضلة، (2017)، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية. طرابلس.
10. غفور عبد الباقي، (2015)، مظاهر الإجرام في المجتمع الجزائري في الفترة الممتدة من 2005 حتى 2008، دراسة أنثروبولوجية من خلال أسبوعية الخبر حوادث، جامعة أبي بكر بلقايد، كلية العلوم الإنسانية والعلوم الاجتماعية، تلمسان.

11. القانون رقم 15-04 مؤرخ في 01 نوفمبر 2004، يعدل ويتمم الأمر رقم 156-66، المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، لجريدة الرسمية عدد 71 مؤرخة في 10 نوفمبر 2004.
12. القانون رقم: 04-09 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، مؤرخة في 16-08-2009.
13. مراد عبد الفتاح، (2007)، شرح جرائم الكمبيوتر والانترنت، دار الكتب والوثائق المصرية، الإسكندرية.
14. مرعي جبريل رشاد إسراء: الجرائم الإلكترونية: الأهداف، الأسباب، طرق الجريمة ومعالجتها، مقال منشور على الانترنت، المركز الديمقراطي العربي، شوهده بتاريخ 14-06-2020، على الساعة 21:00 ليلا، <https://democraticac.de/?p=3542>.
15. Azzouzi ali, (2010), La Cybercriminalité Au Maroc, édition ali el azzouzi, maroc.
16. Chawki mohamed, (2006), Essai Sur La Notion De Cybercriminalité, IEHEI.