المجلة الجزائرية للأبحاث والدراسات ISSN 2602 -5663
المجلد 03 - العدد 09 - شهر جانفي - السنة 2020

تأثير الجريمة الالكترونية على المعلومات الرقمية

أ/ مقدم شبيلة د/ مقناني صبرينة
جامعة عبد الحميد مهري قسنطينة 2، الجزائر
choubeila.mokedem@univ-constantine2.dz meguenani.sabrina@yahoo.fr

تاريخ الارسال: 2019/05/20 تاريخ القبول: 2019/10/14 تاريخ النشر 2020/01/15

ملخص:

لقد افرز التطور التكنولوجي والانفجار المعلوماتي العديد من المخاطر والتجاوزات التي تهدد المحتويات الرقمية، فظهرت الجريمة المعلوماتية كأهم هذه المخاطر مسببة إرهاقا للحقوقيين ومهندسي المعلومات من جهة، ولمستفيدي الانترنت من جهة أخرى، بسبب طبيعتها المتخفية، الأمر الذي يسبب معاناة الكثير جراء تبعاتها، فأصبحت مؤسسات أمن المعلومات في صراع زمني، وصراع مع التغير والتطور المتلاحق للجريمة الالكترونية. فبالرغم من عدم وضوح حدودها، إلا أنها امتداد للجرائم التقليدية، لكن بأساليب ووسائل يصعب تعقبها كما يصعب معاقبة فاعلها بسبب تخفي الأدلة. فلا يمكن نفي الايجابيات التي يوفرها الفضاء الافتراضي الذي يمكِن أي شخص من النشر من أي مكان وفي أي زمان، إلا انه يطرح العديد من المخاطر خاصة سرية وأمن المعلومات المنشورة وغير المنشورة، حيث سنت في هذا الإطار قوانين للردع والعقاب. كما يعمل مطورو التقنيات التكنولوجية على تحيين وابتكار طرق للحماية يوميا لحفظ سرية وممتلكات الأفراد، المجتمعات والحكومات. ومنه، تطرح التساؤلات الموالية:

ما هي الجرائم المعلوماتية؟ وما أسبابها؟ وكيف يمكن محاربتها؟ وما هي التحديات التي يواجهها العالم المعاصر لمواجهة هذه الجرائم؟

كلمات مفتاحية: الجريمة الالكترونية. المعلومة الرقمية. أمن المعلومات.

Abstract

Technological development and information explosion have created many risks and abuses that threaten digital content. Cybercrime has emerged as the most important problems that cause fatigue for jurists and information engineers on the one hand and for Internet users on the other hand; because of their hidden nature, but those affected are suffering from them. Companies and institutions providing information security programs have become in conflict with time and in conflict with change and continuous development of cybercrime. Although their borders are unclear, they are an extension of traditional crimes; but in ways and means hard to track .It is also difficult to punish the perpetrators because of the lack of evidence that often convicts them. The positive ability of anyone to use and publish anything from anywhere, cannot be denied but on the other hand, Many poses Special risks concerning confidentiality and security of published and unpublished information, where laws were enacted to keep pace with development technological deterrence and even punishment. Technology developers are also creating and inventing protection methods on a daily basis. With a view to preserving the confidentiality and property of individuals, communities and even governments. From there, the following questions arise: What are informational crimes? What is the reason? How can it be combated? And what challenges the modern world face?

Keywords: cybercrime; digital information; information security.

مقدمة

عرف العالم انفجارا معلوماتيا نتيجة التطور التكنولوجي، صاحبه تحول الحكومات إلى حكومات الكترونية، إذ صارت المعلومات أهم اهتماماتها، فتحول الاقتصاد إلى اقتصاد معلوماتي بحت، كل من يمتلك المعلومات فيه يتحكم في ميزان القوة لأنها السلعة والمنتج نظرا لقيمتها الاستراتيجية والمالية، كما ظهر إعصار البيانات الضخمة، واستعمالها كمصدر رئيسي لاتخاذ القرار. إلا أن هذه البيانات تتعرض لتهديدات مباشرة وغير مباشرة، سواء ما تعلق منها بالأفراد، أو الدول، أو المجتمعات. وأصبح كل من يتصل بالإنترنت مهددا، خاصة مع شروط الاستعمال التي تفرضها مختلف محركات البحث والبرمجيات، ليوافق فيها الفرد مجبرا على استخدام بياناته من أطراف غير معروفة لأسباب وغايات مجهولة، ولعل أهم أشكال هذه التهديدات القرصنة، السرقة، التجسس وغيرها.

لهذا، ظهرت تسمية الجريمة الالكترونية كإشارة للتخريب الذي يطال المعلومات الرقمية، يعتبرها الكثيرون انتشارا للفكر الإجرامي التقليدي. قد يقوم بها أولئك الذين لم يتجرؤوا على الجريمة في الواقع خوفا من العقاب، أو أولئك الذين يجهلون أن ما يقومون به في العالم الافتراضي عبارة عن عمل إجرامي. ففئة الشباب خاصة تلجأ للقرصنة كطريقة لملأ الفراغ دون معرفة تبعاتها، لكن من جهة أخرى، هناك من اتخذها عملا يذر الأموال دون عقاب. فالجريمة الالكترونية تتميز بلا حدوديتها ولا مكانيتها ومن الصعب معاقبة فاعلها.

وعليه، فإن جل القوانين الخاصة بالردع والعقاب عبر العالم لا تعالج كافة أنواع وأشكال وطرق القيام بالجرائم، وتعتبر شكلية فحسب، الأمر الذي أثقل كاهل الشركات التي تجبر على حماية المستفيدين من الهجمات الالكترونية، خاصة حساباتهم البنكية والشخصية، وكذا الشركات والمؤسسات التي توفر الخدمات الالكترونية حيث تجد نفسها مجبرة على مواجهة تحدي حماية مواقع خدماتها من العبث والتخريب، وبين هذا وذاك، تطرح مجموعة من الأسئلة تستدعي توضيح مفهوم الجرائم الالكترونية وتبعاتها ندرجها كما يلي:

- ما هي الجرائم المعلوماتية؟ وما طبيعتها؟
- ما أنواعها وأسبابها؟ وكيف يمكن محاربتها؟ وما هي آثارها على المعلومات الالكترونية؟
- ما هي التحديات التي يواجهها العالم المعاصر لمواجهة هذه الجرائم؟

أهمية الدراسة وأهدافها.

للدراسة أهمية وأهداف نظرية تكمن في التعرف على مفهوم الجريمة الالكترونية، كما تهدف إلى التعرف على أنواع الجرائم الظاهرة منها والخفية، ومساعدة المحيط العلمي على التعرف على الجرائم المعلوماتية خاصة وأن المحيط الاجتماعي يجهل الجريمة الالكترونية. كما تتمثل أهميتها في تحديد صور الاعتداء على المعلومات والبيانات، إذ تظهر بعض التحديات التي تواجهها الحكومات والمجتمعات في مواجهة هذا النوع من الجرائم بسن قوانين تساير تنامي الظاهرة. كما تبين بعض الطرق الوقائية لمواجهتها.

منهج الدراسة.

بغية استكشاف مختلف جوانب وخصائص الموضوع، خاصة وأنه في بيئة الكترونية بحتة، فقد تم الاعتماد على الدراسات السابقة باتباع المنهج الوصفي التحليلي لشرح الظاهرة محل الدراسة.

مصطلحات الدراسة:

قبل تناول الدراسة من مختلف الجوانب وجب توضيح معاني بعض المصطلحات الواردة منها:

المجرم المعلوماتي:

يمكن تعريفة على أنه فرد يرتكب الجرائم الالكترونية باستخدام الحاسوب كوسيلة، أو كهدف أو كليهما معا، وغالبا ما تتم هذه الجرائم عن طريق مجموعات متعاونة ومنظمة من المجرمين، فمنهم:

- المبرمجون: مهمتهم كتابة البرامج المستخدمة في عمليات الاختراق.
- الموزعون: يقومون بتوزيع وبيع البيانات والفوائد المسروقة من مجرمين آخرين.
- خبراء تكنولوجيا المعلومات: مهمتهم صيانة وإصلاح الهياكل القاعدية كالخوادم وتكنولوجيات التشفير وغيرها.
- القراصنة: يكمن دورهم في استغلال نقاط الضعف في أنظمة المعلومات.

- المحتالون: يقومون بإنشاء المخططات ونشرها كالرسائل غير المرغوب فيها والاحتيال عبر الشبكة [1] وغيرهم الكثيرون.

المعلومة الرقمية:

المعلومات الرقمية ليست فقط أرقام وكلمات، بل يمكن رقمنة أي شيء يمكن سماعه أو رؤيته، فيمكن أن تحتوي قواعد البيانات والانترنت على موسيقى، صور وحتى أعمال فنية، وكذا المنتجات السمعية والبصرية. وبالتالي، فالمعلومات الرقمية هي أي معلومة يمكن أن تضم الصوت والصورة والنص[2] كل على حدى أو معا.

ويمكن القول ان مصادر المعلومات الرقمية تتضمن المعلومة التي تم رقمنتها من مصادر تقليدية، وتلك التي كان منشؤها رقمي بحت.[3]

1. الجرائم الالكترونية:

وردت الكثير من التعريفات للجريمة الالكترونية، بعضها يشير إلى أنها عبارة عن" كل سلوك غير قانوني، وغير مصرح به في نظام يقوم بمعالجة المعلومات أوتوماتيكيا، أو ينقل البيانات" [4] . كما يمكن تعريفها على أنها'' مصطلح عام يعود على الأنشطة الإجرامية التي تتم باستعمال الحواسيب، والانترنت، والفضاءات الرقمية، والشبكة العالمية العنكبوتية'' [5]. وبالرغم من عدم وجود تعريف دقيق للجرائم الالكترونية، إلا أنها تشمل كل تصرف إجرامي مرتبط بالحواسيب والشبكات.

2. تاريخ الجريمة الالكترونية:[6]

مرت الجريمة الالكترونية بمجموعة من المراحل منذ ظهور الحاسوب. فمن المعترف به أن أول ظهور للجرائم الالكترونية تم تسجيله سنة 1820 ، مع حقيقة وجود الحاسوب قبل 3500 سنة في الهند، اليابان والصين بالموازاة مع الحاسوب الحديث وفكرة المحرك التحليلي لشارلز باباغ سنة1837، وتم تحديد و تعقب أول فيروس في حاسوب شخصي سنة 1980. ولكن، العالم لم يعر هذا الفيروس اهتماما .

في أواخر مارس 1999، بدأ فيروس ميليسا يصيب ملايين الحواسيب، وهو فيروس أنشئ على شكل مستند **Word** وضع في موقع للأخبار. فعندما يقوم أي شخص بتحميل الملف وفتحه، يتفعل الفيروس، ويقوم بإرسال

المستند إلى أول خمسون شخصا في العناوين المخزنة**book Address**. يحتوي المستند على ملاحظة لطيفة واسم الشخص المرسل إليه. عندما يقوم المرسل إليه بفتح المستند، يتم إرساله إلى خمسين شخصا آخر. وبهذه الطريقة، أصبح فيروس **Melissa**أسرع فيروس في الانتشار.[7] لكن، لاحقا قامت شرطة نيو جرسي، ومكتب التحقيق الفيديرالي بإلقاء القبض على المتهم الذي أطلقه.

ما يمكن استنتاجه، أن الجرائم الالكترونية وكذا محاولات تعقبها ظهرت في زمن مبكر جدا، مع بدايات ظهور الحاسوب. وكانت الولايات المتحدة الامريكية السباقة في ابتكار عمليات تطوير وسائل التعقب للقبض على المخالفين، كما يمكن القول أن هذا الفيروس والاضرار التي خلفها كان سببا في مضاعفة مجهودات تطوير برامج حماية البيانات والمعلومات.

ففي السبعينيات من القرن الماضي، منذ بدايات استعمال نظم الأمن المعلوماتي في أعمال المعلوماتية كان التركيز منصبا على الحماية من الاحتيال، حيث كانت الحماية التقليدية للحواسيب تفتقر للخصوصية، والحماية من السرقات. ولأن نظم الحماية بدأت تتعامل مع أساليب متطورة من الجرائم، خاصة تسربات المعلومات، وسرقة هويات الأشخاص لاستعمالها في السرقات وانتحال الشخصية. لذلك، هددت آنذاك وفرة الانترنت والأجهزة الخدمات الوطنية والعالمية، ما أوجب الاهتمام بطبيعة تلك التهديدات ودراسة علاقتها مع الأصول، وبالتالي، يساعد على اتخاذ الإجراءات اللازمة لتفاديها خاصة مع التطور التكنولوجي المستمر.

3. طبيعة الجرائم الالكترونية:[8]

إن التحديات التي تطرحها الجرائم عبر البيئة الالكترونية، لا تبرز هويتها بقدر ما تبرز طبيعة البيئة التي تمت فيها، كون المجرمين المعلوماتيين يرتكبون اجرامهم من أي مكان في العالم، مستهدفين عددا كبيرا من الأشخاص والأعمال، متخطين الحدود الجغرافية، لتتسع رقعة هذه الجرائم، وما يصاحبها من صعوبات تقنية لتحديد الجناة، لتزداد مع ذلك الحاجة للعمل والتعاون الدولي، خاصة وان الأنترنت سهل على المجرمين المعلوماتيين أعمالهم، وشجعهم على الخوض في هذه البيئة كون القوانين الردعية والعقابية تتخبط لتنفيذها في ظل البيئة الرقمية.

تظهر الجريمة الالكترونية في أشكال متعددة بداية من إفساد وتدمير الخدمات الالكترونية، إلى عمليات السرقة، الرسائل الالكترونية، والابتزاز. طبيعة هذه الجرائم تجعلها معقلا للبرمجيات الخبيثة، وبرامج التجسس، إذ تسعى لتحقيق

الربح مهما كانت الطريقة. فغالبا ما تكون الهجمات واسعة النطاق، إلا أنها تعتبر إيجابية كونها تسهم في معرفة حجم الثغرات الأمنية في البرمجيات والأجهزة[9]. كمثال على اتساع رقعة الجرائم الالكترونية، يمكن ذكر السرقة باستغلال الأعطال في أجهزة آبل آيفون على سبيل المثال، وكل عامل في شركة ما لديه هاتف من ذلك النوع، فإن مساحة الهجمة بإمكانها الانتقال من العشرات إلى الآلاف باختلاف حجم الشركة. ويمكن حتى القول أن أي شخص يمتلك هذا الجهاز عبر العالم مهدد، ما يوسع من رقعة مساحة الهجمة التي قد تقدر بالآلاف أو الملايين.

كذلك الثغرة الأمنية التي عرفها موقع التواصل الاجتماعي فايسبوك سنة **2019**، تمكن فيها المقرصن من سرقة آلاف الحسابات الشخصية من خلال خاصية عرض الملف الشخصي، بحيث كان حجم الثغرة كبيرا طال مختلف القارات، ما كبد الشركة خسائر جمة، أجبرت على إزالة تلك الخاصية لغلق الثغرة الأمنية.

4. أنواع الجرائم الالكترونية:

يمكن تقسيم الجريمة الالكترونية إلى قسمين رئيسيين يكون فيهما الحاسوب إما هدفا، أو وسيلة،[10] كما يمكن تقسيمها إلى ما يلي:

- الحواسيب والشبكات العنكبوتية كوسيلة للنشاط الإجرامي: من أهم تجليات هذا النوع، البريد الالكتروني غير المرغوب فيه، وهو ما يسمى بـ **spamming**، وسرقات بروتوكولات الانترنت **IP**، وكذا حقوق الملكية الفكرية، والجرائم التي تتم في شبكات الند للند.
- الحواسيب والشبكات العنكبوتية كهدف للمجرمين المعلوماتيين: مثل الوصول غير المصرح به، والحرمان من الخدمات والهجمات الالكترونية باستخدام الأرقام التسلسلية وعمليات التشفير الضار.
- الحواسيب والشبكات كمكان لنشاط المجرمين: كعمليات الاحتيال وسرقة الأموال.
- الحواسيب والشبكات كامتداد للجرائم التقليدية: نذكر على سبيل المثال لا الحصر: المقامرة عبر الانترنت، العنف، التجسس، والإرهاب.

وهناك من قسم الجرائم الالكترونية كالآتي:

1- الجرائم التقليدية باستخدام الحواسيب: كمخططات الاحتيال عبر الانترنت، والقمار عبر الانترنت، ونشر التحرش بالأطفال، والتجسس والمطاردة عبر الانترنت.

2- جرائم سوء استعمال الحاسوب: كالقرصنة، ونشر الفيروسات، والديدان، وهجمات إفساد الخدمات الالكترونية.[11]

ما يمكن استنتاجه مما سبق أن الحاسوب هو الوسيلة الأساسية للجرائم الالكترونية، سواء كان الحاسوب هدف للجريمة أو وسيلة للقيام بها، فيما يمكن ملاحظة ضعف استخدام التكنولوجيات الأخرى في عمليات التعدي كالهواتف الذكية واللوحات الرقمية، يعود ذلك إلى القدرات الكبيرة التي توفرها الحواسيب، من مساحة تخزين وسرعة أداء، كما يساعد ويدعم عمليات التشفير المختلفة، وكذا الوسيلة التي توفر الراحة خلال الاستخدام.

كما يمكن تقسيمها على النحو التالي:

3- الجرائم الالكترونية ضد الأفراد وملكيتهم [12].: مثل الابتزاز عبر البريد الالكتروني، نشر المحتويات الفاحشة، التشهير، القرصنة، الغش والاحتيال، الخداع عبر البريد الالكتروني، تخريب الحواسيب، ونشر الاكواد الضارة كالطروجان والفيروسات والديدان، وجرائم الملكية الفكرية، كقرصنة البرامج والنسخ غير القانوني للتطبيقات والبرامج، ونشرها أو المتاجرة بها، وانتهاك حقوق الملكية الفكرية كسرقة العلامات التجارية، وكذا تقليدها.

4- الجرائم الالكترونية ضد المؤسسات والمنظمات: مثل إفساد، تدمير الخدمات وتعديل الواقع بغير حق، سرقة واحتكار المعلومات بشكل غير قانوني، ونشر التطبيقات والبرامج المقرصنة، والإرهاب الالكتروني ضد المؤسسات الحكومية وغير الحكومية.

5- الجرائم الالكترونية ضد المجتمع ككل: مثل الجرائم الجنسية، وإتاحة الفيديوهات المخلة بالحياء التي تلوث الطفولة والشباب والاتجار بها، والجرائم المالية، وبيع المقالات غير القانونية، والمقامرة عبر الانترنت، بالاضافة إلى التزوير والاحتيال عبر الانترنت.

ما يمكن اضافته أن هذا النوع من الجرائم يمس بالمجتمع ككل، فيؤثر على الحياة الشخصية للأفراد، ويمس قيم المجتمع، وثقافته، وعاداته، ودينه. كما أنها تؤثر على كافة مناحي الحياة، وتهدد جميع المجالات الاقتصادية، الثقافية، والاجتماعية، لهذا فأي نشاط يومي يعتمد على التكنولوجيا الرقمية يعرض صاحبه للهجمات والجرائم المعلوماتية.

5. تصنيف الجرائم الالكترونية:

صنفت الجرائم الالكترونية إلى مجموعات منفصلة منها:

1 – الجرائم الالكترونية ضد الملكية الفكرية: عبارة عن أي فعل إلكتروني ينتهك أمن براءات الاختراع، والأسرار التجارية، والعلامات التجارية، وحقوق التأليف، والنشر، وتتمدد اللائحة إلى المصنفات والمعلومات المرتبطة بالشبكات، وسرية الحواسيب كالبرمجيات، قواعد البيانات، المحتويات الرقمية، الخوارزميات، وغيرها..[13] ويمكن تفصيلها على النحو التالي:

- السرقة العلمية للكتب والبحوث العلمية الأكاديمية خاصة ذات الطبيعة التجريبية والتطبيقية، وكذا سرقة الاختراعات لاستخدامها أو بيعها.
- قرصنة البرمجيات من خلال النسخ غير القانوني لها، واستخدامها وبيعها.
- قرصنة البيانات والمعلومات: وتشمل سرقة البيانات وحفظها بقصد الاستفادة منها، خاصة كلمات المرور، وأرقام البطاقات البنكية وغيرها.[14]

2– التجسس الالكتروني: Cyberespionnage : يعد هذا النوع من الجرائم من الأنواع التي تتم بين الحكومات وليس الأفراد، إذ تستعين الحكومات بمجرمين معلوماتيين لاستيقاء معلومات عن الدول المنافسة لها في مختلف المجالات الاقتصادية، والعسكرية، والاجتماعية لتحقق السبق والأرباح، خاصة بين الدول المتقدمة التي عرفت تطورا تكنولوجيا منقطع النظير كالولايات المتحدة الأمريكية والصين.

يستنتج أن الجسس الالكتروني، وبالرغم من تصنيفه ضمن الجرائم المعلوماتية إلا ان الحكومات تتنافس لابتكار افضل برامج التجسس الرقمي، وتتعاون مع المجرمين المعلوماتيين من ذوي القدرات التقنية الكبيرة لتصميمها، ولاكتشاف الثغرات الأمنية في نظمها، وهو ما يعني الاعتماد على مبدأ الغاية تبرر الوسيلة في هذا المجال، خاصة في ظل المجتمعات المعلوماتية التي تسعى لتحقيق السبق العسكري والعلمي والسيطرة على الثروات.

3– الاحتيال عبر الانترنت: cyber fraud : هو أي تحريف غير صادق للحقيقة يهدف إلى السماح لشخص، أو منعه عن فعل شيء ما ويسبب خسائر، ويهدف إلى تحقيق فوائد مادية [15]. عادة ما يكون الاحتيال عبر بطاقات

البنوك، والدفع المالي، و استعمالها بشكل غير قانوني للقيام ببعض المعاملات المالية، وهو يتشابه مع الاحتيال التقليدي عن طريق ايهام الافراد والشركات بتحقيق أرباح طائلة، ثم النصب عليهم وسرقتهم.

4- غسيل وتبييض الأموال إلكترونيا: Cyberlaundering: تتمثل في استعمال الحاسوب للقيام بمعاملات أو علاقات تجارية تعود بالربح سواء كانت ملموسة أو غير ملموسة، والتي تم التحصل عليها عن طريق نشاط اجرامي[16] . تجدر الإشارة هنا إلى أن تبييض الأموال يشمل تلك الأموال القذرة الناتجة عن جميع الجرائم والأعمال غير المشروعة، وليست فقط الاعمال الناتجة عن معاملات تجارة المخدرات.[17] إن أهم ما يميز هذه العملية طريقة تهريب الأموال، واخفائها في البنوك، وتحويلها عبر مجالات جغرافية متنوعة لتحويل الجانب غير القانوني منها إلى قانوني.

5 – الابتزاز والترصد الالكتروني أو السيبرياني: Cyberstalking and Cyber extortion :حيث يعرف قاموس أكسفورد الترصد على أنه متابعة أو ملاحقة بخلسة، ويتضمن متابعة تحركات شخص عبر الانترنت[18] ويعتمد هؤلاء المطاردين على نشر رسائل تهديدية في المواقع التي يزورها الضحية، وفي لوحات الاعلانات، وعبر مواقع الدردشة والبريد الالكتروني. أما الابتزاز، فيتشابه مع ذلك التقليدي الذي يشمل التهديد للأفراد باستخدام معلوماتهم الشخصية بهدف الحصول على الأموال.

6-الإرهاب الالكتروني:Cyber terrorism : يشمل جميع أصناف الجرائم الالكترونية[19]، ما زاد من فرص الإرهاب تطور أسلحته، وسهل عل المجموعات الإرهابية عملية الترصد والايقاع بضحاياها، وبالتالي أصبحت اهداف الهجمات الارهابية سهلة سواء على الخط أو في الواقع، كما أصبح التأثير على الشباب للالتحاق بمجموعاتها سهلا يقتصر على نقرة زر.

7-السطو والسرقة عبر الانترنت:Cyber theft : من الجرائم التي تعتمد كثيرا على سرقة الأقراص الصلبة والمرنة للحصول على المعلومات المخزنة بها،[20] ثم بيعها والمتاجرة بها فيما بعد، خاصة عمليات السطو على بطاقات الائتمان، وهو ما قد يسبب زوال وإفلاس بعض الشركات الائتمانية والبنكية.

8-القرصنة: Hacking :هي"جماعات تؤمن بالحرية المطلقة في الرأي والتعبير والاستخدام"،[21] تستعمل طرق خاصة لاختراق أجهزة الحاسوب، الأرقام السرية للأشخاص وبريدهم الالكتروني، وبالتالي معرفة أسرار الناس

وخصوصياتهم. يذكر على سبيل المثال ما قام به موقع ويكيليكس من خلال نشر حوالي ربع مليون وثيقة رسمية، مما سبب توتر كبير في العلاقات الدولية.

9- انتحال الشخصية:Identity theft : حيث يمكن القيام بهذه العملية عن طريق الحصول على المعلومات الأساسية حول شخص ما بهدف انتحال صفته والقيام بجرائم متعددة باستخدام اسمه، إلى جانب المعلومات الأساسية مثل الاسم، رقم الهاتف والعنوان الشخصي. فالمنتحلون يستطيعون من خلالها الحصول على أرقام الضمان الاجتماعي، وأرقام رخصة القيادة، وحتى أرقام البطاقات الائتمانية، وأرقام جوازات السفر، مما يسمح للمجرمين بالقيام بمختلف أنواع السرقة والاحتيال. لذلك، فهي" من أخطر الجرائم التي يتعرض لها الأفراد"[22]، والتي يجب التوعية حولها خاصة في الدول المتقدمة التي تعتمد اعتمادا كليا على الحكومات الالكترونية.

10- التصيد:Phishing : هو محاولة الحصول على المعلومات الخاصة بمستخدمي الانترنت سواء أكانت معلومات شخصية، أو مالية، عن طريق الرسائل الإلكترونية، أو مواقع الانترنت التي تبدو وكأنها مبعوثة من شركات موثوقة، أو مؤسسات مالية وحكومية، كالبنوك الإلكترونية. وتستخدم هذه الكلمة لأن المجرمين يستخدمون رسائل إلكترونية مغرية لاصطياد كلمات السر والبيانات المالية من مستخدميها".[23]

وغيرها من الجرائم الالكترونية المتعددة التي تؤثر على المعلومات الرقمية والإلكترونية، والتي تؤدي إلى تدميرها وخرابها مع إلحاق خسائر مادية معتبرة على المتضررين منها.

6. أسباب الجرائم المعلوماتية:[24]

تنتشر الجريمة الالكترونية والمعلوماتية عند توفر مجموعة من العوامل والأسباب. ولعل كون النزاهة والسرية التي تتميز بها بعض المعلومات المهمة والمفيدة من أهم الأسباب، والإعتماد الكلي على الأنترنت والحوسبة السحابية [25]،وخلقها لتحديات تحفز المجرمين المعلوماتيين سواء أفراد أو مجموعات، أو حتى حكومات. ومن بين أهم الأسباب :

- سهولة الوصول- Ease of acces: من المعروف أن أي شخص عبر العالم يمكن أن يتصل بالانترنت، يكفي ان يمتلك حاسوب واشتراك دوري، هذا ما خلق مشكلة حماية نظم الحاسوب ضد الوصول غير المصرح به، حيث توفر الإمكانيات لانتهاك التكنولوجيا من خلال سرقة اكواد وشيفرات الوصول، والتسجيلات،

وتصوير شبكيات العيون، وغيرها، إذ يمكن استخدامها في أنظمة بيومترية وتجاوز جدران الحماية للتحايل على أنظمة الحماية.

- الإهمال-Negligence: عبارة عن عدم الانتباه لحماية النظم المعلوماتية، ويعتبر إهمالا يسمح للمجرمين بالتحكم أو تدمير الحواسيب. يمكن القول أن الإهمال هو أهم أسباب الجرائم الالكترونية سواء من طرف الافراد او الشركات، فعدم تحيين برامج حماية الحاسوب ونظم التشغيل، يؤدي إلى التعرض للهجمات الالكترونية. كذلك الشركات والمؤسسات التي تتقاعس عن اقتناء برامج الحماية، تخاطر بسرية وخصوصية معلومات زبائنها.
- الانتقام أوالتحفيز- Revenge or Motivation: المجرم المعلوماتي يسعى دائما لتحدي نفسه، ليتكون لديه نوع من الطمع الدائم في اتقان الأنظمة المعقدة لإلحاق الضرر والخسائر بالضحايا، خاصة منهم الشباب الذين تحركهم رغباتهم للحصول على عائدات مالية بسرعة، تكون وجهتهم العبث بالبيانات خاصة في اعمال التجارة الالكترونية، والدفع الالكتروني.
- ضعف تنفيذ القوانين وفرضها- Poor law enforcing bodies:
- جرائم الانترنت بهدف الدعاية أو اكتساب الشهرة- Cyber crimes committed for publicity or recognition: أغلبها تتم من طرف الشباب وهدفهم منها ملاحظتهم لكن دون الحاق الأذى بالآخرين.

كما يمكن الإشارة إلى الأسباب النفسية، كالإحباط والفراغ الذي يعاني منه بعض مستخدمي الانترنت، ما يؤدي بهم إلى استكشاف طرق القرصنة وتعلمها لملأ الفراغ وتحقيق الربح المادي. بالإضافة إلى عدم وعي المسخدمين، خاصة مع اهمالهم لسبل الحماية اللازمة، كتحيين نظم التشغيل وتثبيت برامج الامن والحماية، كما يميلون لاستخدام المواقع غير الموثوقة التي تحتوي عديد الثغرات المساعدة على عمليات القرصنة والتي تنشر الفيروسات.

7. تأثيرات الجرائم المعلوماتية على المعلومات الرقمية:[26]

مع ارتفاع أعداد مستخدمي الحاسوب والانترنت، ارتفع عدد الجرائم وتفاقمت نتائج هذه الجرائم. ما أدى إلى فشل الحكومات، والمؤسسات القانونية، والمنظمات، والشركات، وحتى الافراد خاصة منهم الذين يعتمدون في أعمالهم على الحاسوب والانترنت في مواجهة هذا الاشكال بسبب الخسائر والآثار السلبية الناجمة عنها . ولقد تم تصنيف

الجرائم الالكترونية على مستويات دولية، وتم خلق مجموعات، ومراكز جهوية للتحري حول المجرمين المعلوماتيين. لكن، هذه تحريات وملفات الجرائم الالكترونية تغلق مع مرور الزمن بالنظر الى الضغوطات والطلب الكبير على عمليات التحقيق. فمن آثار الجرائم المعلوماتية:

- **الأثر الاقتصادي:**

من المعلوم أن الشركات والمؤسسات الاقتصادية تسعى لإثبات وجودها إلكترونيا، وذلك لتحقيق الانتشار الواسع، وربح الوقت، وتطوير الخدمات. لكن، ما يجب الانتباه له هو وضع أمان وسرية خدماتها، ومعلوماتها في أعلى هرم اهتماماتها لأنها معرضة وبشكل كبير لمخاطر الجريمة الالكترونية [27] . إن اهم ما تؤثر عليه الجرائم الالكترونية القطاع الاقتصادي مسببة خسائر مادية مباشرة وغير مباشرة كسرقة حسابات المستخدمين، هو أثر مباشر وإستعادة هذه الحسابات أثر غير مباشر، كون الشركة تتكبد خسائر عند تعرضها للسرقة، وخسائر اكبر عند محاولة استعادة الحسابات .

ورد في تقريرالمجلس العالمي حول الجريمة المنظمة أن الجريمة الالكترونية أثرت على الاقتصاد مسببة خسائر تقدر بعدة بلايين الدولارات. فبالرجوع إلى سنة 2011 ،تكبد العالم خسائر مالية تراوحت بين 300 بليون وواحد ترليون دولار، والولايات المتحدة الامريكية وحدها قدرت الخسائر بها بحوالي 120 بليون دولار.

- **أثرها على الملكية الفكرية[28]:**

ذكر في التقرير الحكومي البريطاني أن الحكومة قد عرفت الأثر السلبي الذي تحدثه التكنولوجيا على الملكية الفكرية خاصة عند نسخ الحقوق بشكل غير قانوني، ونشرها على مدى واسع، وتبادل المعلومات غير المشروعة باستعمال شبكات الند للند عبر الانترنت مؤثرة بذلك سلبيا على قطاع الصناعات الإبداعية، بالاضافة إلى قرصنة الأنظمة المعلوماتية من أفراد داخل وخارج المؤسسات الموفرة للنظم وقواعد البيانات، ما قد يؤدي بمالكي الحقوق إلى فقدان حقوقهم المادية.

إن حماية حقوق الملكية الفكرية مهمة لقطاع الصناعات التكنولوجية، إنها مطالبة بتوفير الحماية للتصاميم والبرمجيات والمعلومات المتاحة عبر الانترنت من السرقة وإعادة الاستعمال التي تستهدف بشكل أساسي المعلومات القيمة التي تعود بالربح المادي.

- **أثر الجرائم الالكترونية على المعلومات الرقمية:**

هناك العديد من التهديدات التي تتعرض لها الشركات والأفراد على حد سواء. فمع تطور التكنولوجيا ومرور الزمن، أصبح الأمر أكثر تعقيدا، إذ أصبحت أعدادا كبيرة من المجرمين وبوتيرة مرتفعة تعنى بالجريمة الالكترونية، فقد تطورت بيئة العمل وأصبحت الأنظمة ديناميكية متنقلة تعتمد اعتمادا كليا على البيانات والمعلومات. وأصبح العمال يستخدمون الهواتف الذكية المتنقلة التي تحتوى على اسرار شركاتهم، ما يفتح أبواب الجرائم الالكترونية والقرصنة للملفات الرقمية والبريد الالكتروني.

كثيرا ما تلجأ المؤسسات وحتى الافراد إلى الحوسبة السحابية، أو الحفظ السحابي للمعلومات لحفظ المساحة [29] من جهة، ولتسهيل عملية تسييرها من جهة أخرى. لكن، بالرغم من ايجابيتها، إلا انها تعتبر فرصة جديدة للمقرصنين للحصول عليها كون المعلومات استراتيجية تحقق الميزة التنافسية، ولا شك أن البرمجيات الخبيثة واحدة من طرق الهجوم الاجرامي المعروفة عبر الانترنت، لكن، هناك توجه لمجموعة جديدة من التهديدات كالهجوم على الملفات، وشن الهجمات على بروتوكولات التحكم في صفحات الانترنت، وحتى التسلل المشفر للحواسيب والحسابات الشخصية والبنكية والاحتيال من خلالها، واختراق المعلومات السرية، أو اختراق تقنيات حماية البيانات، وكمثال على ذلك إطلاق عملية Aurora سنة 2010، وهي عبارة عن عملية صينية المنشأ[30] تم فيها شن مجموعة من الهجمات على مجموعة كبيرة من شركات البرمجيات، وقد سجلت أضرارا كبيرة لدى مؤسسات محركات البحث. قام المجرمون بخلق ثغرة في يوم الصفر (يوم الصفر معناه السرعة إذ أن القراصنة لا ينتظرون يوما أو ساعة للقيام بهجومهم، لكن يتسارعون مع المطورين الذين يعملون في نفس الوقت على سد الثغرات الأمنية)، وبالتالي يقوم القراصنة بوضع نفق في الشبكات الداخلية للموظفين عبر محطات عملهم المخترقة، مما ينتج عنه اكتشافهم لحسابات البريد الالكتروني، وعن المعلومات الخاصة بالشركة، وحتى المستودعات الخاصة بها التي تعاني من الثغرات الأمنية.[31]

كذلك **Gozi virus** والذي بمجرد البحث عنه في أحد محركات البحث، تبدأ إشعارات الأمان والسرية في الظهور. من المعروف أنه من الفيروسات التي أصابت ملايين الحواسيب، يمنع فيها الأفراد من الزيارة والإطلاع على حساباتهم البنكية[32] وتم به سرقة حوالي خمسون مليون دولار في الفترة الممتدة بين 2005 و2011 ، وتم نشره أساسا في أوروبا وأمريكا الشمالية. كما يمكن سرد اثر الجرائم الالكترونية في ما يلي:

- –نهاية مهام الحلول التقليدية بسبب زيادة المخاطر مع تغير بيئة الاقتصاد.
- تمدد مقياس ونطاق الاخطار من خلال الاعمال والمعلومات والأنشطة العلمية.
- تنشر الحواسيب، والاتصال بالانترنت بسرعة الفيروسات، وتسهل ارسال أو التحكم في ارسال البريد غير المرغوب.

مما قيل، نجد أن قراصنة المعلومات لن يتوقفوا عن وضع واختراع تقنيات جديدة وحتى اكتشاف نقاط ضعف جديدة لاختراق نظم المعلومات الرقمية. لذلك، فالرقمنة تخلق مشاكل فريدة من نوعها تهدد المعلومة الرقمية والمعاملات الالكترونية، فالتكنولوجيا لن تتوقف عن التطور وكذلك الطرق الجديدة لقرصنتها، وبالتالي فالعمل المستمر لتوفير الحماية لهذه النظم يعد من أكبر التحديات التي يواجهها المعلوماتيون لضمان السرية للمستخدمين.

8. تحديات مواجهة الجريمة الالكترونية:

1–تحديات عامة:

- الاعتماد الكلي على تكنولوجيا المعلومات والاتصالات: من المعروف أن الاتصال اليومي يتم عبر تكنولوجيا المعلومات القائمة على خدمات الانترنت كالبريد الالكتروني والإدارة، وخدمات السيارات والطائرات، وقطاع الطاقة وغيرها. فهي كلها تعتمد على التكنولوجيا. لقد سيطرت على الحياة اليومية سيطرة مرشحة للتزايد والاستمرار، مما يجعل الأنظمة المعلوماتية معرضة للهجمات خاصة مع البنى التحتية الضعيفة، حيث يسبب انقطاع قصير في الانترنت خسائر كبيرة، خاصة في البلدان المتطورة التي تعتمد اعتمادا كليا عليها. فهي تواجه اكبر التحديات في التصدي للهجمات ضد هياكلها ومستخدميها، لهذا، وجب توفير سبل وطرق لقياس مدى أمان نظمها وهو ما يتطلب استثمارات كبيرة، وكذا إيجاد استراتيجيات جديدة وتقنيات للوقاية من الهجمات بمساعدة القوانين الخاصة بالجرائم العقابية والردعية لمجرمي الانترنت، مما يمكن من الحد من هذه الظاهرة.
- تزايد عدد مستخدمي الانترنت:**Number of users** إن عدد مستخدمي الانترنت في تطور مستمر. حيث قدر عدد المستخدمين في جوان 2018 بحوالي 4.1 بليون مستخدم حوالي 3.3 بليون منهم مستخدمون لوسائل التواصل الاجتماعي . كان عدد المستخدمين سنة 2010 حوالي 2 بليون مستخدم، وسنة 2005 حوالي 3.38 بليون. ليتطور سنة 2017 ويصبح 3.58 بليون.[33]وهذا إن دل على شيء،

فإنما يدل على الانتشار الواسع للانترنت بين المستخدمين، وبالتالي، ارتفاع عدد المستهدفين من الجرائم الالكترونية. فمن الصعب تحديد اعداد المستخدمين الذين يستغلونه لأغراض إجرامية، وغير أخلاقية. وبالرغم من إن حدة استخدام الانترنت في الدول النامية أقل من المتطورة، إلا أن الجرائم يمكن القيام بها من أي مكان عبر العالم، الأمر الذي يطرح التحدي القانوني الذي يعرف الكثير من العثرات خاصة مع غياب وسائل التحقيق الرقمية التي تكشف المجرمين الحقيقيين.

- توافر الأجهزة وحرية الوصول **Availability of devices and access** : يتطلب القيام بالجريمة الكترونية توفر جهاز يشمل المعدات والبرمجيات مع اشتراك بالانترنت إذ يمكنه القيام بأكبر الجرائم الالكترونية. كما توجد برمجيات تجعل القيام بهذه الجرائم سهلا، حيث يتمكن المجرم من تحميل البرمجية كالتي تقرصن الحسابات، وحتى كلمات السر.

أما الاشتراك بالانترنت بالرغم أنه بمقابل، إلا انه يبقى رمزي خاصة في الدول النامية التي يعتمد فيها أغلب المستخدمون على الدخول غير المشروع والأجهزة المنسوخة، وغير الأصلية. تم اقتراح الحد من المجتمع الذي يتمكن من الاتصال بالانترنت كون أي شخص، وفي أي مكان يمكنه القيام بالجرائم، لكن، اعتبر فيما بعد تعدي على حقوق الانسان، لذلك، يبقى من أعقد المشاكل.

- توافر المعلومات: Availability of information : كل من يتصل بالانترنت يستطيع نشر معلومات، بمعنى أن المشاركة متاحة للجميع. ولعل يعود أكبر نجاح للانترنت لمحركات البحث التي توفر للمستخدم ملايين نتائج بحث في ثواني، ومما لا يعرفه الكثيرون أن هذه المحركات تستعمل في الأعمال الجنائية، كما تستعمل في الأعمال غير المشروعة، نذكر على سبيل المثال **googlehacking** و**googledorks** التي تستعمل لأوامر البحث المعقدة لتنقية وفلترة نتائج البحث من المعلومات حول أمن وسرية الحواسيب. فالقراصنة يبحثون عن الحواسيب ذات كلمات السر الضعيفة وغير المضمونة، كما يمكن استخدامها في تتبع وتحليل المعلومات حول الضحية المحتملة، وغير ذلك من المعلومات التي يوفرها الويب الخفي الذي يعتبر الأهم، ملاذ للقراصنة والمجرمين المعلوماتيين.

- غياب آليات للتحكم: Missing mechanisms of control : حسب قاموس الأعمال، آليات التحكم هي تلك المناهج التي تسير المتغيرات المختلفة بطريقة مرغوبة. فكل مؤسسة يجب أن يتم فيها تطبيق مجموعة من آليات التحكم لمتابعة العمال والأجهزة من جهة، ومدخلات الإنتاج من جهة أخرى للزيادة من فاعلية وجودة الإنتاج[34]، هذا بالمعنى الاقتصادي. أما في الانترنت، فنحن في البدايات المبكرة للقلق حول التحكم في الانترنت. فمستعملو الويب الخفي مثل القراصنة يرون انه من الصعب اخضاع الانترنت لقواعد إلا أن المستخدمين العاديين للانترنت يخضعون لأدوات تحكم لا يعرفون عنها، فمثلا نتائج بحثهم يتم التحكم فيها بدون دراية منهم وغير ذلك الكثير[35]
- البعد العالمي: International dimensions : كما يقول أحد الباحثين في أحد مستخلصات مقالاته أنه " في العمل الشبكي لم تعد الجزيرة جزيرة" [36]بمعنى أن العمل بالانترنت قد جعل العالم قرية واحدة. فالمجرمون المعلوماتيون لا يحتاجون للتنقل إلى مكان بعينه للقيام بالجريمة الالكترونية، فكل ما يحتاجونه هو حاسوب، واتصال بالانترنت. لذلك، يعتبر البعد العالمي للانترنت من أشد التحديات التي تواجه معاقبة الجرائم الالكترونية.
- استقلالية المواقع وعدم الحضور في موقع الجريمة: **Independence of location and presence at the crime site** : لا يحتاج المجرم المعلوماتي إلى التواجد في مكان، أو موقع الضحية للقيام بعمله، غالبا ما يختلف موقع المجرم عن المكان الذي تدل عليه بياناته بفضل تطبيقات تغيير الموقع والعنوان الالكتروني للمستخدم. فالجرائم العالمية والتي تتم خارج الحدود الجغرافية للمجرم تأخذ الوقت والجهد لإثبات فاعلها، كما يختار المجرمون البلدان التي تعاني من الضعف القانوني في محاربة الجريمة الالكترونية كهدف لهم.
- الرقمنة: **Digitization** : تعتبر الرقمنة من أهم إيجابيات التكنولوجيا. لذلك، يتجه العالم إلى رقمنة كل ما هو ورقي وإتاحته، وهو ما يساعد المجرمين بسبب تضاعف الملفات والمواقع غير المحمية التي تسهل عليهم عمليات اختراقها، وهو الأمر ذاته بالنسبة للهجمات التي يشنونها، حيث أصبحت تتطور بفعل الرقمنة كالفيروسات والديدان. فبالرغم من الإيجابيات التي توفرها هذه العملية، إلا أنها تشكل تهديدا كبيرا على أمن معلومات الأفراد والشركات.

- سرعة عمليات تبادل البيانات وسرعة التطور والنمو: في البداية، كان المقرصن إذا توصل إلى ثغرة ما وأحدث ضررا، أو سرق مصدرا ما، من الصعب عليه نشره بين الناس. لكن، مع تطور الإنترنت، أصبح من السهل تبادل المعلومات إذ يمكن لشخص ما أن يقوم بنشر معلومات عن غيره، أو معلومات قام بقرصنتها عبر العالم في ثواني معدودة، كل ذلك بفضل الألياف الضوئية.
- الاتصال بالانترنت بشكل متخفي أو الاتصال المشفر: من أهم التحديثات في الشبكة العنكبوتية، الانترنت الخفي، ولأن المستخدمين أصبحوا واعين بدراسة معلومات اتصالهم من قبل المزودين بالوسائل التكنولوجية المختلفة، وبالتالي، تم التوجه نحو التخفي الالكتروني كأحد الحلول، وأصبحت الشركات التكنولوجية تتسابق لإنتاج أفضل التطبيقات التي تسهم في التخفي. ويسمى الويب الخفي بمعقل المجرمين المعلوماتيين لأنه يوفر المعلومات الخفية والعسكرية، والأمنية الدقيقة التي لا يمكن الوصول إليها عن طريق نتائج البحث العادية، وهذا ما ساعد بشكل كبير على تفشي الجريمة الالكترونية واختفاء آثارها وعدم التمكن من حل ملابسات قضاياها.

2. تحديات قانونية:

- تحديات في وضع مراسيم وقوانين لمعاقبة المجرمين: يرى الكثير من الباحثين أنه وبدون تعاون دولي لن تفيد القوانين التي تعاقب وتردع الجريمة الالكترونية، خاصة مع تساهل القوانين في بعض بلدان العالم. فكل بلد يشرع قوانين تخصه فقط مما يسهم في تكرار ومضيعة للوقت، إذا كانت تقتصر على موقع جغرافي معين. لهذا، يجب أن تتجه الدول نحو سن نفس القوانين العقابية والوقائية الردعية لمحاربة الجريمة الالكترونية، أو على الأقل التنسيق من خلال الاتفاقيات الدولية كما هو الأمر في اتفاقيات حماية الملكية الفكرية، كما وجب في نفس الوقت ابتكار وتطوير عمليات جديدة لتحقيق السرية الرقمية ليتأكد مستخدمو الانترنت من امان معلوماتهم، كما تضمن المؤسسات المختلفة خصوصية وحماية منتجاتها.[37]

9. طرق تجنب الجرائم الالكترونية:

ان أمن المعلومات هو أهم هدف في بناء طرق ووسائل الحماية كآليات إثبات الهوية، وضمان السرية والأمان للمعلومات والبيانات المنقولة والمرسلة والمنشورة مثلها مثل أنظمة الأمان والحماية من الجرائم الالكترونية المعتمدة في

البنوك العالمية والوطنية، كالتشفير عن طريق كلمات السر، أو لوحات المفاتيح والرسومات الافتراضية.[38] التي تعتبر مهددة وغير آمنة بشكل نهائي، فقد يعرض أي خلل في هذه الأنظمة المستخدمين لخسائر فادحة.

1.9 بالنسبة للافراد:[39]

- التوعية: إن أعدادا كبيرة من مستخدمي الانترنت غير واعين بأهمية الأمان والسرية عبر الويب، ويستخدمون برمجيات مقرصنة خاصة في الدول المتخلفة، وعادة ما يسهل تخريب حساباتهم بسبب ضعف كلمات السر وافشاء الأرقام السرية لحساباتهم، وهم أكثر عرضة للقرصنة والسرقة خاصة عند النقر اللاارادي والسريع على العناوين غير المعروفة، لذلك، فالتوعية حول استخدام الانترنت ضرورية للحفاظ على السرية والممتلكات.
- الحذر من الاستخدام غير المشروع لبروتوكولات الانترنت لكل حاسوب: تستعمل الكثير من المؤسسات وحتى الجامعات وخاصة في الدول النامية نطاقات حرة ومفتوحة، وبالتالي، لا تحتوي على شروط الأمان والسرية، ولهذا تعطي الفرصة لمستخدمين آخرين باستعمال بروتوكول الانترنت الخاص بهم في أغراض مجهولة.
- الالتزام بالمبادئ من طرف مقاهي الانترنت: لا يحق لهم بأي طريقة كانت متابعة المعلومات التي يبحث عنها المستفيدون أو نشرها، قد يعرضهم ذلك للعقوبة وهو ما ذكر في قانون تكنولوجيا المعلومات لسنة 2000.

2.9 بالنسبة للحكومات:

- العمل على جعل عناوين بروتوكولات الانترنت سرية لصعوبة متابعة المجرمين: [40] إذا كان بروتوكول الانترنت الذي يستخدمه شخص معين مرتبط بمودم واحد طوال الوقت حين ذلك يسهل أو تسهل عملية تعقب المستخدم له أو المجرم على سبيل المثال. لكن العكس عند استعمال مودم واحد في مكان عام. فكلما زاد عدد المستخدمين له زاد الاستعمال لبروتوكول الانترنت الواحد، وبالتالي، يصعب تحديد الشخص الذي قام بنشاط اجرامي. لكن، توجد محركات بحث تغير من بروتوكولات الانترنت لدى المستخدمين، لكن تحفظها في مكان ما. لذا، وجب التعاون مع محركات بحث الويب الخفي من طرف الحكومات للتمكن من اثبات تواجد شخص معين في موقع الجريمة الالكترونية ومعاقبته.

- العمل على استمرارية وانتظام عملية حجب المواقع الضارة: فعلى الحكومات العمل مع المجتمعات الدولية لحجب المواقع التي تهدد مواطنيها وتشكل خطرا على معتقداتهم وثقافاتهم خاصة منها تلك التي تستعمل في الاباحة، وكذلك الإرهاب الالكتروني والتي تشجع على العنصرية.
- العمل للتوصل إلى اتفاقيات عالمية فيما يخص الجريمة الالكترونية: [41] لا تسن معظم البلدان وخاصة النامية منها قوانين تفصيلية فيما يخص الجريمة الالكترونية، إذ أن اكتشاف موقع مجرم ما في أحد البلدان التي لا يقيم بها لا يعرضه لأي عقوبة إذا كان بلده غير منخرط في اتفاقيات أو قوانين عالمية تنص على معاقبته، ما يحفز المجرمين لعدم وجود قوانين عقابية كافية.

وهناك الكثير من الإجراءات التي يجب على الحكومات اتخاذها للعمل على ردع الجريمة الالكترونية، منها تطوير وكالات ومؤسسات تعمل خصيصا في تطوير نظم وبرامج الحماية خاصة في الدول النامية مصصمة حسب حاجتها بدل استيرادها من دول أخرى، وكذا إعطاء الفرصة للهواة والطلبة، وتوفير الحوافز لرفع مستويات الابتكار لديهم.

وللوقاية من بعض الجرائم المعلوماتية عبر البريد الالكتروني وجب:

- التنبه للاتصالات الهاتفية أو البريد الالكتروني الذي يطلب معلومات مالية بحجة تحديث الملفات الشخصية والمالية العائدة للفرد أو للشركة.
- الامتناع عن الرد على أية مراسلة واردة بالبريد الالكتروني عبر الضغط على الرد المباشر وإنما عبر رسائل جديدة لأن المقرصن قد ينشئ حساب مشابه للأصلي.
- عند إرسال رسائل الكترونية لعدة أشخاص يجب وضع عناوين البريد الالكتروني في خانة Bcc لكي لا يطلع عليها الغير ويحاولوا اختراقها.
- عدم استخدام كلمة مرور واحدة لأكثر من بريد أو موقع الكتروني، كما يجب استخدام كلمة مرور قوية وتغييرها بشكل دائم.
- التنبه للرسائل الواردة والمتضمنة مرفقات مع وصف ك **scr. Dll. Cox. Com. Exe. Bat. Vbs.dif. shs.pif** لإمكانية احتوائها على برامج خبيثة.

- تحديث المتصفح باسمرار وتحديث نظام التشغيل، استعمال برنامج أصلي لمكافحة الفيروسات وتحديثه باستمرار.
- التنبه من تصفح البريد الالكتروني من خلال الشبكات العمومية public wifi . [42]
- تبقى هذه الحلول من وجهة نظرنا وقائية ونظرية وعلى المستوى الفردي، لكن، في الأصل يجب على الشركات المنتجة للتكنولوجيا الرقمية أن تتوصل إلى ابتكارات تحمي مستخدميها، ولما لا فتح أبواب التعاون مع مخربي الانترنت والمعلومات، والاستفادة منهم في جعل نظم المعلومات اكثر أمانا.

خاتمة

لعل أهم ما تم استخلاصه أن المعلومة الرقمية من أهم مصادر المعلومات التي يتم الاعتماد عليها في الأعمال الحديثة، ولعل الجرائم الالكترونية تسبب تلوثا معلوماتيا في البيئة الكترونية من خلال المعارف المغلوطة والبيانات المخربة التي تهدد الأفراد والحكومات والمجتمعات. فعن طريق تداول فيديوهات الأطفال الإباحية قد تقضي على القيم الاجتماعية والاخلاقية في بعض البلدان خاصة العربية والمسلمة. كما يتسبب تبييض الأموال في غزو الأسواق بأموال ذات مصادر مشبوهة، مما ينتج عنه أزمات تجارية، والاحتيال والسرقة، فتتسبب في انهيار المؤسسات الاقتصادية، أو حتى الإفلاس لدى الشركات ذات رؤوس الأموال الضعيفة، وتكبد الكبرى منها خسائر هامة مما قد يفسد سمعتها التجارية. ويمكن أن يتسبب التجسس إلى نشوب حروب بين الدول كما هو الأمر عند اكتشاف الأسلحة النووية في العراق واحتلالها. لهذا، وجب التفكير في مدى مصداقية وشفافية المعلومات المتاحة عبر الانترنت، والتفكير في أسس واستراتيجيات القضاء على الجرائم الالكترونية، سيما أنها من الجرائم التي تلحق الضرر المعنوي والنفسي بالأفراد زيادة على الضرر المادي، ومنه وجب التوعية بمخاطرها لصالح الجميع، كما وجب مواكبة سلبياتها وإيجاد الحلول لها عن طريق القوانين والتشريعات لضمان الحقوق من جهة، وعن طريق تطوير واقتناء برامج الأمان والسرية المستحدثة والمحينة عبر الأنترنت من جهة أخرى.

الهوامش:

[1] TechnoPedia. (n.d.). *Cybercriminal*. Retrieved September 25, 2018, from TechnoPedia: https://www.techopedia.com/definition/27435/cybercriminal

[2] IT Law Wiki. (n.d.). *Digital information*. Retrieved September 21, 2018, from FANDOM: http://itlaw.wikia.com/wiki/Digital_information?

[3] Howell, A. (2013). Perfect one day- digital the next: Challenges in preserving digital information. *Australian academic and reaserch libraries , vol.4* (31), 121-141.

[4] Idem. Solak, D., & Topaloglu, M. (2015).

[5] Nfuka, E. N., Sanga, C., & Mshangi, M. The rapid growth of cybercrimes affecting information systems in the global: Is this a myth or reality in Tanzania. *International journal of information security science , vol.3* (2), 182-199.

[6] ibid. p.183

[7] مستودع جامهة بابل للابحاث والأوراق الالكترونية. (03 افريل, 2011). *فيروس الحاسوب* . تاريخ الاسترداد 17 أوت, 2018، من مستودع جامعة بابل للابحاث والأوراق الالكترونية: http://repository.uobabylon.edu.iq/2010_2011/4_14913_742.pdf

[8] Crown. (2010). *Cybercrime Strategy* . Richmond: The stationery office limited.

[9] ACS. (2016, Dec 05). *Cybersecurity: Threats challeges opperunities*. Retrieved aug 18, 2018, from ACS: https://www.acs.org.au/insightsandpublications/news/2016/120297.html

[10] Op.cit. Solak, D., & Topaloglu, M. (2015).p. 590-595

[11] Subramanian, R., & Sedita, S. (2006). Are cybercrime laws keeping up with the triple convergence of information, innovation and technology? *Communications of the IIMA , vol.6* (issue1), 39-50.

[12] Op. cit. Nfuka, E. N., Sanga, C., & Mshangi, M.p.184

[13] Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International journal of computer networks and communications security , vol.4* (n°6), 165-176.

[14] ذياب موسى البداينة. (2014). الجرائم الالكترونية: المفهوم والأسباب. الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، (الصفحات أ-28). عمان.

[15] Embeywa, H. (n.d.). *Iformation and cyber security: emerging trends in social media communication*. Machakos, Machakos university, Kenya.

[16] Leselie, A. (2014). Legal principles for combatting cyberlaundering. In A. Leselie, *law,governance and technology series* (pp. 55-64). Switzerland: Springer International Publishing.

[17] شعبان، س. (2010). جريمة تبييض الأموال، مفهومها ومخاطرها، والآليات المصرفية لمكافحته. المدية: جامعة المدية. ص 1-22.

[18] Goyal, A., & Singh, P. (2018). Cyber Extortion. *International journal of research in engineering, science and management , vol.1* (7), 53-57.

[19] مرجع سابق. البداينة، ذ، م. (2014)

[20] بونعارة، ي. (بلا تاريخ). الجريمة الالكترونية. قسنطينة، جامعة الأمير عبد القادر للعلوم الاسلامية، الجزائر

[21] المرجع نفسه. بونعارة، ي. ص.19

[22] Information and privacy commissioner. (2014, July). Identity theft: A Crime of opportunity. Ontario, Canada.

[23] مسعود، م، أ. (23 افريل, 2013). آليات مكافحة جرائم تكنولوجيات الاعلام والاتصال في ضوء القانون رقم 04/09. 118. ورقلة، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح

[24] Maghu, S., Sehra, S., & Bhardawaj, A. (2014). Inside of cyber crimes and information security: Threats and solutions. *International journal of information & computation technology , vol.4* (.8), 835-840.

[25] Chouhan, R. (2015). Cyber crime escalation vs solutions: a Literature snapshot. *Jaipur international journal of converging technologies and management (IJCTM) , vol.1* (2), 1-12.

[26] Mohammed, S. (2015). An introduction to digital crimes. *International journal in foundations of computer science & technology(IJFCST) , vol.5* (no.3), 13-24.

[27] Dalla, H. S. (2013). Cyber Crime – A threat to persons, property,government and societies. *International journal of advanced research in computer science and software engineering , vol.3* (5), 997-1002.

[28] Op.cit. Crown. (2010).p.16

[29] Jones, A. (2016, november 18). Cybercrime effects on stock prices. Kentucky, the Honors College at Murray, Usa.

[30] Schwartz, M. J. (2013, May 21). *Google aurora hack was chinese counterespionage operation*. Retrieved sebtember 12, 2018, from Dark Reading: https://www.darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060

[31] Malby, S., Mace, R., & Holterhof, A. (2013). *Comprehensive study on cybercrime.* New York: United nations office on drugs and crime.p.17

[32] Threat Encyclopedia - Trend Micro USA. (n.d.). *GOZI - Threat Encyclopedia - Trend Micro USA*. Retrieved sebtember 14, 2018, from Threat Encyclopedia - Trend Micro USA: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/gozi

[33] Statistica. (2018, July). *The Statistics Portal*. Retrieved sebtember 13, 2018, from Global digital population: https://www.statista.com/statistics/617136/digital-population-worldwide/

[34] Control mechanisms. BusinessDictionary.com. Retrieved September 21,2018 ,from BusinessDictionary.com website: http://www.businessdictionary.com/definition/control-mechanisms.html

[35] Zittrain, J., & Palfrey, J. (2011, December). *Internet filtering: The politics and mechanisms of control.* Retrieved September 21, 2018, from http://access.opennet.net: http://access.opennet.net/wp-content/uploads/2011/12/accessdenied-chapter-2.pdf

[36] Goodman, M. (2011, January). *International dimensions of cybercrime*. Retrieved September 20, 2018, from ResearchGate:https://www.researchgate.net/publication/251100620_International_Dimensions_of_Cybercrime/references

[37] International Telecommunication Union. (2014, September). *Understanding cybercrime:Phenomena challenges and legal response*. Retrieved Sebtember 20, 2018, from International Telecommunication Union: https://www.itu.int/pub/D-STR-CYB_CRIME-2015/en

[38] Op.cit. Chouhan, R. (2015).

[39] Singh, I. (2013, July). Prevention of Cybercrime: Issues and Challenges. Kanpur, IIT Kanpur Indian Institute of Technology Kanpur, India: RAKSHAk Foundation.

[40] Hofmann, M. (2011, Augest 24). *Why IP addresses alone don't identify criminals*. Retrieved October 01, 2018, from Electronic Frontier Foundation: https://www.eff.org/fr/deeplinks/2011/08/why-ip-addresses-alone-dont-identify-criminals

[41] Op. Cit. Singh, I. (2013, July).

[42] جمعية المصارف في لبنان. (2016). *جمعية مصارف لبنان*. تاريخ الاسترداد 01 اكتوبر, 2018، من مكافحة الجريمة الالكترونية المالية في لبنان: http://www.abl.org.lb/ar/index.aspx?pageid=206