

الجريمة الالكترونية (خصائصها ومجالات استخدامها، وأهم سبل مكافحتها)

Cybercrime:

its characteristics, areas of use, and the most important ways to combat it.

الدكتورة: نعيمة دوادي

naimadouadi090@gmail.com

جامعة علي لونيسي- البليدة (الجزائر)

تاريخ النشر: 2020/08/20

تاريخ القبول: 2020/07/27

تاريخ الإرسال: 2020/07/24

ملخص:

يعرف العصر الحالي العديد من التطورات العلمية، ومن بينها التطور الحاصل الذي تشهده الثورة المعلوماتية والإلكترونية والانتشار الواسع للشبكة العنكبوتية، والتي ساهمت بشكل كبير في تطور العديد من مجالات الحياة، غير أنه في المقابل أنتجت هذه الثورة نمط جديد من أنواع الجريمة وهي الجريمة الالكترونية أو المعلوماتية، وهي جريمة تمس في صميمها قيما جوهرية تخص الأفراد والمؤسسات وحتى الدول فتسارعت العديد من الدول لإيجاد الحلول لها من خلال التشخيص العلمي الدقيق لمختلف العوامل الكامنة وراءها والتعرف على مختلف الاستراتيجيات والآليات التي تؤدي إلى الحد منها، ومن هنا تقترح الباحثة مداخله تتطرق فيها إلى استعراض جملة من المفاهيم المتعلقة بالمشكلة والمتمثلة في مفهوم الجريمة الالكترونية لدى مجموعة من العلماء، وتعريفها في التشريع الجزائري، وكذلك خصائص هذا النوع من الجرائم ومرتكبيها، بالإضافة إلى مجالات استخدامها، وأخير أهم الآليات والسبل التي يمكن استغلالها من أجل التصدي لها.

الكلمات المفتاحية: الجريمة الالكترونية، أنظمة المعالجة الآلية للمعطيات.

Abstract:

The current era is known for many scientific developments, one of which is development in the information and electronic revolution and high prevalence of the web that contributed greatly to the progress of many areas of life. On the other hand, this revolution produced a new type of crime, namely electronic or information crime. The latter, at its core, affects the fundamental values of individuals, institutions and even countries. Consequently, many countries have accelerated to find solutions through accurate scientific diagnosis of the various factors behind it, and identify the different strategies and mechanisms to reduce it. This research paper attempts to describe cybercrime and provide definitions and related concepts set by scholars, and its definition in the Algerian legislation. The paper also illustrates the characteristics of this crime, its perpetrators, areas of use, and the most important mechanisms and ways to confront it.

Key words: Cybercrime; Automatic data processing systems.

مقدمة:

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

وكنيجة لهذا الانتشار الحاصل في مجال العلوم والاكتشافات التقنية، ظهر بما يسمى الجرائم الإلكترونية التي أتت لتنبه المجتمعات على عظيم خطرها، فظهر محترفوها ينهون ويخربون ويهددون أمن دول عديدة، لهذا وجب علينا طرح الانشغال التالي: ما هي الآليات والسبل التي يمكن استغلالها من أجل التصدي للجريمة الإلكترونية؟

1. مفهوم الجريمة الإلكترونية:

نحن نعلم أن كل نشاط يقام بطريقة غير مشروعة وغير قانونية يعتبر جريمة، إذن فهو عمل مخالف للقوانين العرفية والوضعية المتعارف عليها والمعمول بها عبر مختلف دول العالم، فما هي الجريمة الإلكترونية؟

تعتبر الجريمة الإلكترونية ذلك السلوك الغير مشروع المتعلق بالمعالجة الآلية للبيانات ونقلها كون التقنية فيها تكون إما وسيلة تستخدم في ارتكاب الفعل أو البيئة والوسط الذي يحدث فيه الجرم، أين أن الوسيط يكون آلة تقنية كجهاز كمبيوتر من خلال الاتصال بالإنترنت ويكون هدفها اختراق الشبكات أو تخريبها أو التحريف أو التزويد أو السرقة أو الاختلاس، ويشمل السلوك الانحرافي في جريمة بأركانها المادية والمعنوية ولا عبء فيها بالباحث على ارتكابها (يونس خالد عرب مصطفى 1994، ص 36)، فهي متعلقة كذلك ببعض الأجهزة التقنية الأخرى كالجيل الثالث للهواتف النقالة واستخدام الإنترنت فيها الذي حول العالم إلى قرية صغيرة باعتباره وسيلة اتصال عالمية تعتمد على برامج معلوماتية حديثة في ضبط مختلف البيانات والمعطيات المعلوماتية الدقيقة.

فالجريمة الإلكترونية إذن هي كل فعل ضار يأتية الفرد أو الجماعة عبر استعماله لأجهزة الكترونية، ويكون لهذا الفعل أثر ضار على غيره من الأفراد فهي إذن تستهدف القضاء على التكنولوجيا الحديثة عبر الوسائط الإلكترونية (أمير فرج يوسف، 2001، ص 97)، ومع غزو الإنترنت دول العالم أصبح من الصعوبة ضبط مكان وكشف هذه الجرائم، نظرا لكونها عابرة للحدود لا دين ولا وطن لها، وتتم بسرعة فائقة دون رقيب ومن أمثلتها السطو على برامج الحاسوب بغرض سرقة البيانات وقاعدة المعطيات المعلوماتية واستخدامها في التجسس أو تلك المتعلقة بالقرصنة والسطو على الأموال إلى جانب ظهور ما اصطلح عليه بالإرهاب الإلكتروني وتهديد الأمن القومي للدول، وكذا جرائم الآداب العامة والمساس بالأخلاق من خلال الإباحية الإلكترونية التي تجسدها المواقع الجنسية الإباحية.

تعريف التشريع الجزائري:

المشرع الجزائري على غرار الكثير من التشريعات لم يعرف نظام المعالجة الآلية للمعطيات، وأوكل بذلك المهمة لكل من الفقه والقضاء، ولمزيد من التفصيل نتطرق إلى تعريف ذلك من خلال القانونين 15-04 و04-09 على التوالي:

أ- تعريف الجريمة الإلكترونية في التشريع الجزائري في القانون 15-04:

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

- الدخول والبقاء بالغش في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات أو محاولة ذلك.
- حذف أو تغيير لمعطيات المنظومة إذا ترتب عن الدخول أو البقاء غير المشروع بغرض تخريب نظام اشتغال المنظومة.

أما المادة 394 مكررا فقد أشارت على مايلي:

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

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

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلية عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو إفشاء أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم. (القانون رقم 15-04 المؤرخ في 10 نوفمبر، يعدل ويتمم الأمر 156-66 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71 لسنة 2004)

ب- تعريف الجريمة الإلكترونية في التشريع الجزائري في القانون 04-09:

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

-الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

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

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

- معطيات معلوماتية:

أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها. (القانون 04-09 المؤرخ في 05 أغسطس 2009)

2. خصائص الجريمة الإلكترونية:

تتميز الجرائم الإلكترونية بجملة من الخصائص لا تتوافر في الجرائم العادية، نبيها في الآتي:

1- صعوبة اكتشاف الجريمة الإلكترونية:

توصف الجرائم الإلكترونية بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة، كإرسال فيروسات، وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم. (محمد عبيد الكعبي، 2009، ص31)

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

2- الجريمة الإلكترونية عابرة للحدود (الزمان والمكان):

المقصود بذلك أن هذا النوع من الجرائم لا يعتد بالحدود الجغرافية للدول ولا بين القارات، فمع انتشار شبكة الاتصالات بين دول العالم وأقاليمه أمكن ربط أعداد لا حصر لها من أجهزة الكمبيوتر عبر مختلف دول العالم بهذه الشبكة، حيث يمكن أن يكون الجاني في بلد والمجني عليه في بلد آخر، وهكذا فالجرائم الإلكترونية تقع أغلبها عبر حدود دولية كثيرة. (عبد الفتاح مراد، ص42)

ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمال الإجرامية التي يعتمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، وهو ما يعني أن مسرح الجريمة المعلوماتية لم يعد محلياً بل أصبح عالمياً، إذ أن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي لحصول الجريمة الإلكترونية في مكان الجريمة، ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء، فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الكمبيوتر الموجود في بلد آخر، وهو بذلك السلوك قد يضر شخصاً آخر موجود في بلد ثالث. (نائلة عادل، 2005، ص25)

3- جرائم هادئة:

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل والسرقة وغيرها من الجرائم، فالجرائم الإلكترونية لا تحتاج أدنى مجهود عضلي بل تعتمد على الدراسة الذهنية، والتفكير العلمي المدروس القائم عن معرفة تقنية الكمبيوتر. (عبد الفتاح مراد، 2010، ص46)

وذلك يعود لكون هذا النوع من الجرائم عبارة عن معطيات وبيانات تتغير أو تعدل أو تمحى من السجلات المخزنة في ذاكرة الحاسبات، إلا أن البعض يشبهها بجرائم العنف مثل ما ذهب إليه مكتب

التحقيقات الفيدرالي بالولايات المتحدة الأمريكية (FBI) نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف. (مفتاح بوبكر المطردي 2012، ص 31)

4- جرائم صعبة الإثبات:

يعد إثبات الجريمة الالكترونية من الصعوبة بمكان حيث يصعب تتبعها واكتشافها فهي لا تترك أثرا يقتفى، حيث تعتبر مجرد أرقام فمعظم الجرائم الالكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أنها تفتقر إلى الدليل المادي التقليدي كال بصمات مثلا. (رستم هشام، 1999، ص 11) ومن جهة أخرى فإن تعقبها يتطلب خبرة فنية يصعب تواجدها لدى المحقق العادي للتعامل معها، زيادة على ذلك يعتمد مرتكب الجريمة الالكترونية إلى ممارسة التمويه عند ارتكابها والتضليل والتحايل بغاية عدم التعرف على مرتكبها.

3. مجالات استخدام الجريمة الالكترونية:

يتسع نطاق الجريمة الالكترونية ليشمل جميع مناحي حياة المجتمع وأفراده، بداية من التدخل في حياته الخاصة وصولا إلى أمنه، فنطاق الجريمة الالكترونية تطل حياة الأشخاص الخاصة، كما تطل أيضا أموال الأفراد والمؤسسات ، وأخرى تمس أمن الدولة وسلامتها، ذلك ما يعالج في النقاط التالية:

الفرع الأول: جريمة الكترونية تطل حياة الأشخاص الخاصة:

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

أولا: التهديد والمضايقة:

يقصد بالتهديد زرع الخوف في نفس الإنسان من ضرر قد يلحق به شخصا أو بمن تحت رعايته أو بمن لهم صلة به أو بماله..(عبد الصبور عبد القوي 2007، ص 21) حيث يقوم المجرم الالكتروني بإرسال رسالة الكترونية للمجني عليه تنطوي على ما يزعجه كيفما كان شكله أو مضمونه، وذلك رغبة منه في التحكم في الضحية أو ابتزازه أو لأي سبب آخر.

ثانيا: انتحال شخصية الغير والاستدراج:

يتم ذلك من خلال استخدام المجرم الالكتروني لشخصية الضحية أو المجني عليه بغرض الاستفادة من سمعته أو سلطته أو ماله أو غيره من الأسباب، فقد تتم بواسطة انتحال شخصية المجني عليه أو انتحال شخصية ما، ويكثر استخدام هذا النمط في الوسط التجاري.

أما الاستدراج فغالبا ضحاياه هم صغار السن، حيث يهيمون من قبل المجرم الالكتروني برغبته في تكوين صداقة عبر الشبكة تتحول إلى لقاء واقعي بينهما ، وقد تتم الجريمة في إقليم الدولة الواحدة، وقد تكون مختربة حدود الدولة أي أن المجرم الالكتروني في دولة والضحية موجود في دولة أخرى.(عمرو موسى 2006، ص 102)

ثالثاً: نشر الإباحة:

يقصد بنشر الإباحة كل إرسال أو نشر عمل إباحي أو بإعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية أو اتصل بالدعارة. (أحمد محمد اللوزي 2015، ص 853)

ويتم ذلك من خلال المواقع الالكترونية الموجودة على الشبكة، والتي تستخدم بغرض الإثارة الجنسية من خلال قيام المجرم الالكتروني بنشر صور جنسية فاضحة وأفلام جنسية، وكثيراً ما تستهدف الأطفال والشباب لأن هذه الفئة أقل تحصيناً.

رابعاً: جريمة الالكترونية ماسة بشخص الإنسان وكرامته:

تعد من الجرائم الالكترونية واسعة الانتشار عبر الشبكات، حيث تستخدم أسلوب القذف والسب وتشويه السمعة وغيرها من الأفعال اللاأخلاقية، بغرض المساس بشرف الشخص أو النيل من كرامته، وقد يكون عبر خطوط الاتصال أو عبر البريد الالكتروني أو عبر صفحات الويب، أو عبر غرف المحادثة والدردشة. (محمد الكعبي، ص 114)

الفرع الثاني: جريمة إلكترونية تطل الأموال:

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

أولاً: جرائم الالكترونية تطل بطاقات الائتمان والتحويلات المالية الالكترونية:

تتم الجريمة الالكترونية في هذه الحالة من خلال الحصول على كلمة السر المدرجة في أنظمة الكمبيوتر الخاصة بالمجني عليه، مما يسهل على المجرم الالكتروني الولوج إلى النظام المعلوماتي، ويكون ذلك سواء بالتواجد على الشبكة أثناء إتمام عملية ما، أو بإدخال بيانات إلى ذاكرة الجهاز، ويكون ذلك باستخدام الاحتيال، وكذلك بواسطة بطاقات الدفع الالكتروني. (صغير يوسف، 2013، ص 44)

1- الاحتيال:

يتم الاحتيال على الضحية من خلال تضليله بوجود مشروع يحصل من وراءه على أموال، مما يدفعه إلى الانسياق وراء تغريير المجرم الإلكتروني، هذا الأخير يحصل بواسطة استعماله أفعال تضليلية على أموال ملك للغير دون مسوغ قانوني، ويكون ذلك سواء باتصال عبر الشبكة بين الجاني الإلكتروني والمجني عليه، أو من خلال استخدام المجرم الإلكتروني البيانات الكاذبة التي تساعد على إيهام الكمبيوتر والاحتيال عليه بغاية الحصول على الأموال. (يونس عرب 2006، ص 16)

2- الاحتيال بواسطة بطاقات الدفع الالكتروني:

يتم الدفع الالكتروني بواسطة الدفع الإلكتروني بتحويل مالي من المصدر وهو بنك العميل إلى رصيد متعامل آخر قد يكون تاجر أو دائن أو....، كل ذلك يتم بواسطة شبكة التسوية الإلكترونية الدولية (مثلاً ماستر كارد)، حيث يقوم المجرم بكسر كلمة السر للبطاقة الالكترونية أو خداع الصراف الآلي، وبالتالي

يمكن من الحصول على السلع والخدمات من خلال ملء نموذج الكتروني ببيانات بطاقة الائتمان الخاصة بالمشتري. (يوسف صغير ص 45 مشار إليه)

ثانيا: سرقة أموال البنوك:

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

ثالثا: غسيل الأموال:

يعد غسيل الأموال من أبرز الأنشطة التي تقوم بها شبكات منظمة تحتترف الإجرام الإلكتروني، وتأخذ درجة عالية من التنسيق والتخطيط والانتشار في كافة أنحاء العالم، وتشير إحصائيات الأمم المتحدة وصندوق النقد الدولي إلى أن 30 مليار دولار أمريكي من الأموال القدرة تغسل سنويا عبر الشبكات الإلكترونية مخترقة حدود ما يقارب أو يزيد عن 76 دولة في العالم. (محمود حجازي، مشار إليه، ص 18)

الفرع الثالث: جريمة الكترونية تظال أمن الدولة:

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

أولا: الإرهاب والجريمة الإلكترونية:

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

كما يتم تبني الأعمال الإرهابية والدعاية لهذه التنظيمات وأعمالها من خلال مختلف الوسائط والمواقع الإلكترونية مما يحقق أهدافها. (يوسف صغير، ص 21)

ثانيا: التجسس والجريمة الإلكترونية:

غير خاف أن التطور في المجال الإلكتروني المعلوماتي سهل من مهمة التجسس، فالمجرم الإلكتروني سواء كان شخص واحد أو تنظيم يمكنه التجسس سواء على أشخاص أو منظمات وحتى دول، ويأخذ التجسس عدة صور، فقد يكون تجسس اقتصادي أو سياسي أو عسكري.

ثالثا: الجريمة المنظمة والجريمة الإلكترونية:

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

مكافحة الجرائم الإلكترونية:

للحد من الجرائم الإلكترونية لا بد على جميع الدول والأفراد المساهمة قدر الإمكان للتصدي لها وهذا عن طريق:

- 1- الاستدلال الذي يتضمن التفتيش والمعاينة والخبرة التي تعود إلى خصوصية الجريمة الالكترونية عبر الانترنت.
- 2- تقديم الجهود الدولية والداخلية لتجسيد القوانين للوقاية من هذه الجريمة المستحدثة، فأما الدولية فتتمثل في جهود الهيئات والمنظمات الدولية والتي تتمثل في:
 - توعية الناس لمفهوم الجريمة الالكترونية وأنه الخطر القائم ويجب مواجهته والحرص على ألا يقعوا ضحية له.
 - ضرورة التأكد من العنواين الالكترونية التي تتطلب معلومات سرية خاصة كبطاقة ائتمانية أو حساب بنكي.
 - عدم الإفصاح عن كلمة السر لأي شخص والحرص على تحديثها بشكل دوري واختيار كلمة السر غير مألوفة.
 - عدم حفظ الصور الشخصية في الكمبيوتر.
 - عدم تنزيل أي ملف أو برنامج من مصادر غير معروفة.
 - الحرص على تحديث أنظمة الحماية مثل استخدام برامج الحماية مثل MacafeeNorton.....الخ.
 - تكوين منظمة لمكافحة الجريمة الالكترونية.
 - تتبع تطورات الجريمة الالكترونية وتطوير الوسائل والأجهزة والتشريعات لمكافحتها.
 - تطوير برمجيات آمنة ونظم تشغيل قوية التي تحد من الاختراقات الالكترونية وبرمجيات الفيروسات وبرامج التجسس مثل؛ مثل مضادات التجسس وهي برامج تقوم بمسح الحاسب للبحث عن مكونات التجسس وإلغائها مثل؛ lavasoft.
- نصائح لحماية جهازك الالكتروني:
 - لا تدخل المواقع المشبوهة أو تتصل بشبكات (WIFI) مجهولة فقد تكون معرض للاختراق من قبل أحد العابثين في نظم الشبكات اللاسلكية وعد استخدام كلمات السر في مقاهي الإنترنت بشكل نهائي.
 - عدم الدخول على الإنترنت من غير وجود برامج حماية أصلية يتم شراؤها من الشركة المصنعة.
 - تذكر أن المواقع لا تطلب من مستخدمها كتابة كلمات مرورهم على رسالة بريد الكتروني أبداً، لأن هذه من أساليب الهاكر.
 - أجعل دائماً نسخة لملفات حاسوبك على قرص خارجي وذلك لضمان وجود نسخة احتياطية في حال إتلاف أو مسح النسخ الأصلية الموجودة في الجهاز الآلي.
 - احرص على تسجيل إجابة على السؤال السري أو بوضع بريد الكتروني بديل أو رقم هاتف المحمول في المواقع التي تطلب منك ذلك، فهو مفيد في حالات اختراق الحساب وفي حالة نسيان كلمة السر أيضاً.

خاتمة:

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

المراجع:

- ✓ أحمد محمد اللوزي ومحمد عبد المجيد الذنيبات 2015، " الجريمة الإلكترونية كما نظمها قانون جرائم أنظمة المعلومات الأردني"، مجلة دراسات، كلية علوم الشريعة والقانون، الجامعة الأردنية، مجلد 42، العدد 03.
- ✓ أمير فرج يوسف، 2001، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية.
- ✓ رستم هشام 1999، "الجرائم المعلوماتية، أصول الجنائي الفني"، مجلة الأمن والقانون، دبي، الإمارات العربية المتحدة، العدد 2، ص11.
- ✓ صغير يوسف، 2013، "الجريمة المرتكبة عبر الانترنت"، مذكرة لنيل درجة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر.
- ✓ عبد الصبور عبد القوي علي(2007)، " الجريمة الإلكترونية، دارالعلوم للطباعة والنشر، ط1، القاهرة.
- ✓ عبد الفتاح مراد، "شرح جرائم الكمبيوتر والانترنت"، دار الكتب والوثائق المصرية، ص42.
- ✓ عمرو موسى 2006، " الجرائم المعلوماتية(جرائم الحاسب الآلي في مصر وفي الدول العربية)"، المكتب الجامعي، الإسكندرية، مصر، ص102
- ✓ القانون 04-09 المؤرخ في 05 أغسطس 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية، العدد 47 لسنة 2009.
- ✓ محمد عبيد الكعبي 2009، "الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت"، دار النهضة العربية، القاهرة، مصر، ص31.
- ✓ مفتاح بوبكر المطردي 2012، "الجريمة الإلكترونية والتغلب على تحدياتها"، مقال مقدم إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان، المنعقد في 23-25/9/2012، ص31.
- ✓ نائلة عادل محمد فريد قورة 2005، "جرائم الحاسب الآلي الاقتصادية"، منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، ص25.
- ✓ يونس خالد عرب مصطفى 1994، " جرائم الحاسوب دراسة مقارنة"، رسالة ماجستير، ط1، مصر.
- ✓ يونس عرب 2006، " قراءة في الاتجاهات التشريعية للجرائم الإلكترونية"، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، مسقط، عمان.