ISSN : 2353 – 0030
EISSN: 2602-697X
مجلة أبعاد
مجلد 09، العدد 01 (خ)، 2022

الجريمة الإلكترونية وممارساتها في العالم الإفتراضي

Cybercrime and its practices in the virtual world

بوزارة أحلام [1] Bouzara Ahlem bouzara.alm.13@hotmail.com	علم المكتبات والعلوم الوثائقية	جامعة جيلالي ليابس سيدي بلعباس- الجزائر

****

تاريخ الإرسال: 2022/02/25	تاريخ القبول: 2022/04/28	تاريخ النشر: 2022/05/05

ملخص: إن الاستعمال الواسع للتكنولوجيا قاد إلى الكثير من المنافع والفوائد بجانب المشاكل والمَخاطر؛ فالتغيرات العالمية الناجمة عن هذه الثورة التكنولوجية، خلفت آثار إيجابية وسلبية ناتجة عن حسن أو سوء استخدامها. فلا شك أن هذه التكنولوجيا مثل ما تسهل الاتصالات حول العالم كذلك تجلب معها تهديدات جديدة وكثيرة. فهذا النوع من الجرائم أصبح واقع يهدد وبشكل مريب سمعة وحياة الأفراد ؛ وتسبب بأضرار جسيمة لأشخاص بعينهم أو مؤسسات كاملة من أجل خدمة أهداف سياسية، مادية أو شخصية، هذا ما سنتطرق إليه في هذه الدراسة بداية من مفهوم الجريمة الإلكترونية وكيفية ظهورها وأنواعها، خصائصها، ومخاطرها لنختم في الأخير بكيفية مواجهتها ومكافحتها وطرق الحد من انتشارها.

الكلمات المفتاحية: الأنترنت؛ الجريمة الإلكترونية؛ العالم الإفتراضي؛ التكنولوجيا الحديثة؛ الفرد والمجتمع.

Abstract : The widespread use of technology has led to numerous benefits but also problems and risks; It is well established that the global changes resulting from the technological revolution have a negative and positive impact due to its on good or misuse. On the same token, technology like the one that facilitates communications around the world, also brings with it many new threats. This type of crime has become a reality that suspiciously threatens the reputation and lives of individuals; but it causes severe damage to certain to people or entire institutions in order to serve political, material or personal goals. On this basis, this study deals with the concept of electronic crime, how it appears, its types, characteristics, and risks, in addition to solutions to combat it and limit its spread.

Keywords : Internet; electronic crime; virtual world; modern technology; individual and society.

[1] المؤلف المرسل: bouzara.alm.13@hotmail.com

1. مقدمة:

لقد احتلّ التقدّم في مجال المعلومات والاتّصالات جانباً كبيراً ومُهمّاً في حياة النّاس وتعاملاتهم؛ فصار الحاسوب أساس التّعامل بين الأشخاص والشّركات والمؤسسات، وقد ازداد التوجّه لاستخدام شبكات المعلومات الإلكترونيّة في الفترة الأخيرة بصِفَتها أداة اتّصال دولية في مُختلف مناحي الحياة، مُوفِّرةً بذلك الكثير من السّرعة والمسافات والجهد على الإنسان. وأصبحت صفة المعلوماتية هي التي تسود العصر الذي نعيش فيه، وبات استخدام التقنية والأنظمة المعلوماتية من قبل الدول والأفراد، مقياس يقاس به مدى تطور البلدان في العالم، فازدهار الحضارة وانتشار التقدم التقني، ساعد في تسهيل الكثير من أمور حياتنا ولكنه في نفس الوقت جلب لنا العديد من المخاطر والأضرار المتعلقة بالحواسيب والشبكة العنكبوتية؛ مما جعل الحكومات والمجتمعات تنتبه إلى ضرورة نشر التوعية والتعريف بهذه الجرائم، عن طريق شرحها وتحليلها للناس وبيان وسائل وطرق الوقاية منها. (رضوان، 2018)

فظاهرة الجريمة الإلكترونية أصبحت تهدد أمن واستقرار الأمم (فرد ومجتمع) مما أوجب محاربة هذه المشكلة في البيئة الرقمية. وذلك بالتكتل بينها وإقرار إجراءات صارمة تحد من انتشارها. فمنذ بضع سنين لم تكن المؤسسات على اختلافها تولي اهتماما كبيرا لاستخدام الإنترنت في نشاطاتها اليومية، ولكن مع التطور المذهل الذي تشهده هذه الأخيرة لم نعد نتصور أنه يمكن لأي مؤسسة عبر العالم أن تتجاهلها؛ فالوعي بأهمية استعمال الانترنت كقاعدة تجارية وتسويقية أصبح حتميا. (فرج يوسف، 2009)

ومن خلال ما سبق تكمن إشكالية الدراسة في طرح التساؤل التالي:

ما هي ممارسات الجريمة الإلكترونية في ظل التطورات السريعة للتكنولوجيا وما هي أهم تحديات اللجوء إلى العالم الإفتراضي؟

ومنه تتفرع مجموعة من الأسئلة الفرعية: وخصائصها ومخاطرها وسمات مرتكبيها ودوافعهم

* ماهية الجريمة الإلكترونية؟وكيف تطورت؟

* بما تتميز هذه الجريمة ومخاطرها وما هي سمات مرتكبيها؟

* وما هي آليات التصدي لها في ضوء التطور الكبير والمتواصل لهذه الجرائم؟

أهداف الدراسة :

- الوقوف على ماهية الجريمة الإلكترونية أسبابها وأنواعها.
- التعرف على أهم مراحل التطور التاريخي للجريمة الإلكترونية.
- معرفة مجمل الخصائص والمميزات التي تخص الجريمة الإلكترونية وكذا مرتكبيها.
- التطرق إلى أهم آليات تصدي ومكافحة مثل هذه الجرائم بشقيها الأمني والقانوني والتعرف على كيفية مواجهة هذه الجريمة الإلكترونية في الجزائر.

منهج الدراسة:

اعتمدت في دراستنا على المنهج التاريخي، والمنهج الوصفي لدراسة ظاهرة الجريمة الإلكترونية في العالم الافتراضي كالتالي:

.1المنهج التاريخي :تم من خلاله البحث في الكتب والمقالات والتقارير والأبحاث الصادرة عن الجهات ذات العلاقة بظاهرة الجريمة الإلكترونية سواء على المستوى المحلي أو الدولي.

.2المنهج الوصفي :وتم التطرق من خلال هذا المنهج إلى الجوانب المتعلقة بالجريمة الإلكترونية في العالم الافتراضي، وذلك للإجابة على تساؤلات الدراسة.

تقسيم الدراسة:

للإجابة عن الإشكالية المطروحة وتماشيا مع العنوان المقترح، ارتأينا أن نتبع الخطة التالية لدراسة الموضوع حيث قسمناه إلى محورين، أولهما إطار مفاهيمي للجريمة الإلكترونية يضم كل من ماهيتها،، أنوعها،خصائصها، أهدافها...إلخ.أما المحور الثاني فخصصناه لآليات التصدي لهذه الجرائم، وإجراءاتها المتبعة من أجل محاربة هذه الظاهرة التي تؤدي إلى بروز عدة جرائم تقنية تلحق الضرر بالإنسان، لنتطرق في الأخير إلى نظرة عامة حول سبل مكافحتها في الجزائر. ويسبق هذين المحورين مقدمة وننتهي بخاتمة تشمل النتائج المتوصل إليها وبعض الاقتراحات.

2. ماهية الجريمة الإلكترونية :

للجريمة الالكترونية عدة مسميات فمنهم من ينعتها بجرائم الحاسوب أو الانترنيت، أو جرائم التقنية العالية أو جرائم الياقات البيضاء، أما التعاريف الأخرى فيطغى عليها الجانب القانوني. فمنهم من يعرف الجريمة المعلوماتية على أنها: "فعل ضار يستخدم الفاعل، الذي يفترض أن لديه معرفة بتقنية الحاسوب، نظاماً حاسوبياً أو شبكةً حاسوبيةً للوصول إلى البيانات والبرامج بغية نسخها أو تغييرها أو حذفها أو تزويرها أو تخريبها أو جعلها غير صالحة أو حيازتها أو توزيعها بصورة غير مشروعة". (حفوظة

وغرداين،2016).

تعريف آخر يقول هي " المخالفات التي ترتكب ضد الأفراد أو المجموعات بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر؛ باستخدام شبكات الاتصالات كالإنترنت، غرف الدردشة، البريد الإلكتروني، والموبايل". (البداينة، 2014،ص. 52) . ويعرفها أحمد صياني بأنها " تصرف غير مشروع يؤثر في الأجهزة والمعلومات الموجودة عليها." (جبريل،2021) .

*وهذا التعريف يعتبر جامع مانع من الناحية الفنية للجريمة الالكترونية.

وقد اصطلح المشرع الجزائري على تسمية الجرائم الالكترونية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وعرفها بموجب المادة 02 من القانون 09-04 المؤرخ في 05 غشت 2009: "على أنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية". (جريدة رسمية، 2009 ص.05)

*وكاستنتاج لما سبق من تعريفات مختلفة ومتنوعة، نقول أن الجريمة الإلكترونية ما هي إلا كل فعل إجرامي؛ يستخدم الكمبيوتر في ارتكابه كأداة رئيسية وعن طريق شبكة الانترنت، بواسطة شخص على دراية فائقة. لتحقيق مكاسب شخصية أو مالية أو ضرر نفسي.

3. التطور التاريخي للجريمة الإلكترونية :

مرت جرائم الإنترنت بتطور تاريخي تبعا لتطور التقنية واستخداماتها، ولهذا مرت بثلاث مراحل كما يلي:

1.3.المرحلة الأولى :

من شيوع استخدام الحواسيب في الستينات على السبعينات اقتضت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر، وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم مجرد شيء عابر أم ظاهرة إجرامية مستحدثة، ومع تزايد استخدام الحواسيب الشخصية في السبعينات ظهرت عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة. (عرب، 2002)

2.3. المرحلة الثانية :

في الثمانينات، حيث طفا على السطح مفهوم جديد لجرائم الكمبيوتر والانترنت ارتبطت بعمليات اقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الالكترونية التي تقوم بعملية تدميرية للملفات أو البرامج. شاع اصطلاح "الهاكرز" المعبر عن مقتحمي النظم، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل محصورًا في رغبة المحترفين تجاوز أمن المعلومات وإظهار تفوقهم التقني. وظهر المجرم المعلوماتي المدفوع بأغراض إجرامية خطيرة القادر على ارتكاب أفعال تستهدف الاستيلاء على المال أو التجسس أو الاستيلاء على البيانات السرية والاقتصادية الاجتماعية والسياسية والعسكرية. (الأشقر، 2008)

3.3. المرحلة الثالثة :

شهدت التسعينات تنامياً هائلاً في حقل الجرائم الالكترونية وتغييراً في نطاقها ومفهوماً. ظهرت أنماط جديدة كأنشطة إنكار الخدمة التي تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد؛وأكثر ما مورست ضد مواقع الانترنت التسويقية الهامة التي يتسبب انقطاعها عن الخدمة لساعات في خسائر مالية بالملايين. ونشطت جرائم نشر الفيروسات عبر المواقع الالكترونية لما تسهله من انتقالها إلى ملايين المستخدمين في ذات الوقت. وظهرت الرسائل المنشورة على الانترنت أو المراسلة بالبريد الالكتروني المنطوية على إثارة الأحقاد أو المساس بكرامة واعتبار الأشخاص؛ أو المروجة لمواد غير القانونية، رغم تزايد الأبحاث ومحاولات ابتكار أنظمة تكفل لأي كمبيوتر الحماية اللازمة، إلاّ أنه في المقابل يتم تطوير الإجراءات المضادة لهذه الحصون الأمنية، ومعنى ذلك أن خطر انتهاك أمن وسلامة الكمبيوتر مستمرة مدى استمرارية هذه التحصينات. (الصمدعي وردينة، 2012، ص.139).

4. خصائص الجريمة الإلكترونية :

– مرتكب الجريمة الإلكترونية في الغالب شخص يتميز بالذكاء ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب الآلي؛ وكيفية تشغيله وتخزين المعلومات والحصول عليها، في حين أن مرتكب الجريمة التقليدية – في الغالب–شخص أمي بسيط، متوسط التعليم وعادة ما تتراوح أعمار تلك الفئة من المجرمين ما بين 18-45 عامًا. (رضوان، 2018)

– مرتكب الجريمة الإلكترونية–في الغالب–متكيفا اجتماعيا وقادرا ماديا، باعثه من ارتكاب جريمته الرغبة في قهر النظام أكثر من الرغبة في الحصول على الربح أو النفع المادي، في حين أن مرتكب الجريمة التقليدية –غالبا– ما يكون غير متكيف اجتماعيا وباعثه من ارتكابه الجريمة هو النفع المادي السريع. (المطردي،2012، ص.16) .

– الجريمة الإلكترونية ذات بعد دولي، باعتبار أن تنفيذها يتم عبر الشبكة وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية، وسياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية. (عبد الفتاح، 2005)

– هي جريمة ناعمة، تنفذ بسرعة وهي صعبة الإثبات: أي أنها لا تتطلب العنف ولا استعمال الأدوات الخطيرة كالأسلحة وغيرها، فنقل بيانات ممنوعة أو التلاعب بأرصدة البنوك مثلا لا تحتاج إلا إلى لمسات أزرار، فأغلب الجرائم المعلوماتية ترتكب في وقت قصير جداً قد لا يتجاوز الثانية الواحدة، وفي المقابل فهي صعبة الإثبات لعدم وجود الآثار المادية التقليدية (مثل بقع الدم، تكسير، خلع...الخ) (عبد الفتاح، شرح التحقيق الجنائي، 2006).

– الجاذبية: نظرا لما تمثله سوق الكمبيوتر والإنترنت من ثروة كبيرة للمجرمين أو الإجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب، تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها،أو استخدام أرقام البطاقات...الخ. (الديربي، 2013).

– امتناع المجني عليهم عن التبليغ: لا يتم في غالب الأحيان الإبلاغ عن جرائم الانترنيت إما لعدم اكتشاف الضحية لها وإما خشية من التشهير. (المومني، 2008)

– سرعة محو الدليل وتوفر وسائل تقنية تعرقل الوصول إليه: يسهل محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المخصصة لذلك .

– الإجرام المعلوماتي هو إجرام الذكاء، دون حاجة إلى استخدام القوة والعنف وهو مفتاح المجرم المعلوماتي لاكتشاف الثغرات واختراق البرامج. (المومني، 2008)

– أهداف الجريمة الإلكترونية :

– تحصيل مكسبٍ سياسيّ، ماديّ، معنويّ غير مشروع عبر تقنيات المعلومات كعمليّات تزوير بطاقات الائتمان، والاختراق، وتدمير المواقع على الإنترنت وسرقة الحسابات المالية. (قشقوش، 1992)

– تحصيل معلومات ووثائق سريّة المستخدمة للتكنولوجيا، كالمؤسسات والبنوك والجهات الحكومية والمصرفية والشخصية والأفراد لابتزازهم من خلالها؛ وكذلك التمكن من الوصول إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها.

– الوصول لمعلوماتٍ غير مُخوّل للعامّة الاطلاع عليها بشكلٍ غير مشروع، وسرقتها أو حذفها أو تعطيلها أو التعديل عليها لتحقيق مصالح وأهداف مرتكب الجريمة . (الحجاج، 1998)

– النيل من سمعة الضحية والتشهير بها بدافع الانتقام، وذلك من خلال الحصول على معلومات وبيانات الضحية (صور، مقاطع فيديو ...) للحصول على مكسب مادي أو معنوي. (قشقوش، 1992)

– انتهاك فكر الضحية وخطفه ذهنياً وذلك من أجل إيقاعها فريسة فكر يتعارض مع عقيدة المسلم الصافية؛ مستغلاً بذلك جهل الضحية بالتيارات الفكرية الموجودة على الساحة العالمية وطبيعة توجهها وأهدافها. (عبد الفتاح، 2012،ص.11).

– أدوات الجرائم الإلكترونية:

– حتى يتمكن القراصنة (Hackers) من تنفيذ جريمتهم يستلزم توفر أدوات، من أبرزها:

– الاتصال بشبكة الإنترنت،وتعتبر أداة رئيسية لتنفيذ الجريمة. وتوفر برمجيات خاصة لنسخ المعلومات المخزنة عند المستخدم على جهاز الحاسوب.

– وسائل التجسس ومنها ربط الكاميرات بخطوط الاتصال الهاتفي. (الحجاج، 1998)

– البار كود وهي عبارة عن أدوات تستخدم لمسح الترميز الرقمي وفك شفرة الرموز. وامتلاك طابعات (Printers) وهواتف رقمية ونقالة.

– برامج ضارة ومنها (Trojan horse) إذ تتمثل وظيفته بخداع الضحية وتشجيعه على تشغيله؛ فيلحق الضرر الشامل بالحاسوب والملفات الموجودة عليه.(الصمدعي وردينة،2012، ص.100)

5. أسباب الجريمة الالكترونية:

1.5 أسباب الجريمة على المستوي الفردي:

❖ البحث عن التحدي: 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. (البشري، 2008)

❖ الفرصة: لقد وفرت التقنيات الحديثة والأنترنت فرصاً غير مسبوقة لانتشار الجريمة الالكترونية؛ وتلعب البيئة وترتيباتها دورا كبيرا في إنتاجها والخروج على قواعد اجتماعية فوقت الانحراف عن قواعد الامتثال ليلا ونهارا وفي أي مكان. وعدم وجود رقابة كلها عوامل تزيد من فرصة ارتكابها. وقد تشكل المعلومات هدفاً سهل المنال ويحقق المنفعة السريعة، وبالتالي يمكن سرقتها فهي فرصة مربحة وقليلة المخاطر واحتمالية الكشف للفاعل فيها ضئيلة. فتكنولوجيا المعلومات والاتصالات والاستخدام المتزايد للأنترنت قد خلق فرص جديدة للمجرمين. (البشري، 2008)

❖ ضبط الذات المنخفض: تنطلق هذه الدراسة من النظرية العامة في السلوك الطائش؛ وتؤكد هذه النظرية أن احتمالية انخراط الأفراد في فعل إجرامي تحدث بسبب وجود الفرصة مع توفر سمة شخصية من سمات الضبط الذاتي المنخفض. (الصريفي،2009،ص.91)

❖ النشاط الروتيني: ويمكن 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 الخ. وحتى استخدام النت وشبكات التفاعل الاجتماعي مثل الفيسبوك والايميل والمواقع وغيرها. قد خلقت فرصاً للجناة المتحفزين مع وجود أهداف قيمة وسهلة في الحيز الفضائي مع غياب الحراسة. (الصريفي، 2009)

2.5 أسباب الجريمة على المستوي المجتمعي:

❖ التحضر: إن الهجرة الكبيرة من الريف إلى المدينة والى المناطق الحضرية والمدن الكبيرة. وعادة ما يهاجر الشباب غير المتمكنين من مواجهة متطلبات الحياة الحضرية باهضه التكاليف، والتي تتطلب مهارات عالية أحيانا. مما يجعلهم يلتفتون إلى الاستثمار في الجريمة الإلكترونية حيث لا تتطلب رأس مال كبير. (سعدون،محمود، وحسن،2011)

❖ البطالة: ترتبط الجريمة الإلكترونية شأنها شأن الجريمة التقليدية بالبطالة؛والظروف الاقتصادية الصعبة؛ وتتركز البطالة بين قطاعات كبيرة من الشباب وكما يقول المثل النيجيري "العقل العاطل عن العمل هو ورشة عمل للشيطان". ولذا فان الشباب الذين يملكون المعرفة سيستثمرون ذلك في النشاط الإجرامي الإلكتروني.

❖ الضغوط العامة: تعد الضغوط التي يتعرض لها المجتمع من فقر،بطالة وأمية وظروف اقتصادية صعبة وعوامل ضاغطة على المجتمع عامة وخاصة على قطاع الشباب، مما يولد مشاعر سلبية عند شرائح كبيرة من الناس ما يدفعهم إلى أساليب تأقلم سلبية منها الإتجار الإلكتروني بالبشر والجنس وغيرها.(سعدون،محمود،و حسن،2011)

❖ البحث عن الثراء: يسعى الإنسان إلى المتعة ويتجنب الألم، هكذا تقول النظرية العامة في الجريمة لجتفردسون وهيرشي. 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. (سمارة، 2008)

❖ 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. (خليل، 2009،ص. 221)

3.5 أسباب الجريمة عل المستوي الكوني:

❖ التحول للمجتمع الرقمي :إن من أهم سمات عصر المعلومات هي الثلاثة الرئيسة : أولها تغيرات كمية في مقدار المعلومات المتدفقة ونوعيها، فبفعل تكنولوجيا الاتصالات فإن الصور والمعلومات تغطي كافة المعمورة بسرعة ودقة. أما ثاني سمة فتتمثل في إرسال المعلومات إلى العديد من الأطراف (البشر والمعدات). أما فيما يخص ثالث سمة وهي وجود الشبكات حيث يتم تداول المعلومات بين جميع الأطراف مثل البريد الإلكتروني الجوال الخ. (أبو فارة، 2007،ص.317) .

❖ العولمة: إن ظهور "الفضاء الإلكتروني" يخلق ظواهر جديدة متميزة قد يظهر الأشخاص الفروق في امتثالهم الخاص(القانوني). وعدم الامتثال (غير القانوني) مقارنة مع سلوكهم في العالم المادي؛ فالأشخاص مثلا، قد يرتكبون جرائم في الفضاء الإلكتروني لا يرتكبونها في الواقع المادي بسبب مكانتهم وموقعهم بالإضافة إلى ذلك، فمرونة الهوية وعدم ظهورها وضعف عوامل الردع تحفز السلوك الإجرامي في العالم الافتراضي. (البحر، 1999).

❖ الترابط الكوني: إن الترابط العالمي ساهم في دفع مستويات الجريمة في سياق تحولات العالم الاقتصادية والديموغرافية. أكد تقرير صدر عن المركز الوطني لجريمة الياقات البيضاء أن فضاء الإنترنت قد خلق فرصا جديدة للمجرمين في التواصل مع الضحايا، وعدم الكشف عن اسم الشخص وسهولة الاستخدام قد وفرت طرق جديدة للمجرمين لارتكاب جرائمهم . (الملط، 1989)

❖ انكشاف البنية التحتية المعلوماتية الكونية: تتفاوت البني التحتية المعلوماتية بدرجة انكشافها إلى الكوارث الطبيعية، والإهمال البشري وسوء التصرف. (عليان، 2015 ص.319).

6. صور وأنواع الجريمة الالكترونية:

هناك عدة أنواع وصور للجريمة الإلكترونية نوردها كما يلي:

❖ الجرائم ضد الأفراد: وتسمى بجرائم الانترنت الشخصية، مثل سرقة الهوية ومنها البريد الإلكتروني أو سرقة الاشتراك في موقع شبكة الإنترنت.

❖ الجرائم ضد الملكية: انتقال برمجيات ضارة المضمنة في بعض البرامج التطبيقية والخدمية أو غيرها. لتدمير الأجهزة أو البرامج المملوكة للشركات أو الأجهزة الحكومية أو البنوك أو حتى ممتلكات شخصية (رشدى،محمد السعيد).

❖ الجرائم ضد الحكومات: مهاجمة المواقع الرسمية وأنظمة الشبكات الحكومية، والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي كالهجمات الإرهابية على شبكة الانترنت. وهي تتركز على تدمير الخدمات والبنى التحتية ومهاجمة الشبكات وغالباً ما يكون هدفها سياسي بحت. (رضوان، 2018)

❖ تخريب المعلومات وإساءة استخدامها: ويشمل ذلك قواعد المعلومات، المكتبات، تمزيق الكتب، تحريف المعلومات، تحريف السجلات الرسمية... الخ. (رضوان، 2018)

❖ سرقة المعلومات: ويشمل بيع المعلومات كالبحوث أو الدراسات الهامة أو ذات العلاقة بالتطوير التقني، أو الصناعي، أو العسكري، أو تخريبها،أو تدميرها... الخ.

❖ تزوير المعلومات: ويشمل الدخول لقواعد في النظام التعليمي وتغيير المعلومات وتحريفها، مثل تغيير علامات الطلاب. (عبد الفتاح، 2005)

❖ انتهاك الخصوصية: ويشمل نشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحساباتهم الإلكترونية ونشر معلومات عنهم، أو وضع معلومات تخص تاريخ الأفراد ونشرها. كما تشمل على التصنت وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف. والتجسس ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد . (مطر،2021)

❖ التشهير ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة، ونشرها بشكل القصد منه اغتيال شخصية الأفراد أو الإساءة .

❖ السرقة العلمية: الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية. وكذا سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو لبيعها.

❖ قرصنة البرمجيات ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى . (البشري، 2008)

❖ قرصنة البيانات والمعلومات ويشمل اعتراض البيانات وخطفها، بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.

❖ خلاعة الأطفال وتشمل نشر صور خاصة للأطفال "الجنس السياحي" للأطفال خاصة، وللإناث على الشبكات بشكل عام، ونشر الجنس التخيلي (Cyber Sex). (الملط، 1989)

❖ القنابل البريدية وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة ملغومة إلكترونية. (الصريفي، 2009)

❖ الاحتيال المالي بالبطاقات وهذا ناتج عن استخدام غير الشرعي لبطاقات التسوق أو المالية أو الهاتف...الخ. وسرقة الأرقام والمتاجرة بها وخاصة أرقام الهواتف السرية، واستخدامها في الاتصالات الدولية أو أرقام بطاقات الائتمان. (حجازي، 2010)

❖ التحرش الجنسي ويقصد به المضايقة من الذكور للإناث أو العكس من خلال المراسلة أو المهاتفة، أو المحادثة، والمطاردة والملاحقة والابتزاز بقصد فرض إقامة علاقة ما، وذلك من خلال استخدام البريد الإلكتروني وإرسال الرسائل.

❖ الإرهاب الإلكتروني ويشمل جميع المكونات السالفة الذكر في بيئة تقنية متغيرة والتي تؤثر على فرص الإرهاب ومصادرة، هذه التغيرات تؤثر على تكتيكات الإرهاب وأسلحته وأهدافه ومن التكتيكات الإرهابية ما يعرف بالإرهاب الإلكتروني.(محمد السعيد،20018)

7. أنواع الجرائم الإلكترونية في قانون العقوبات الجزائري:

طبقا لقانون العقوبات الجزائري المعدل والمتمم والذي أستحدث فيه المشرع الجزائري قسما خاصا في القسم السابع مكرر من الفصل الثالث الخاص بالجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات وعلى هذا الأساس يمكن تصنيفها إلى ما يلي:

❖ 1- الغش أو الشروع فيه، في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات

❖ 2- حذف أو تغيير لمعطيات المنظمة. (المادة394)

❖ 3- إدخال أو تعديل في نظام المعطيات. (أنظرالمادة 394 مكرر1)

❖ 4 – تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار.

❖ 5- حيازة أو إفشاء أو نشر أو استعمال المعطيات. (المادة 394 مكرر2)

❖ 6- تكوين جمعية أشرار. (المادة 394مكرر5)

من خلال المواد القانونية السابقة والتي تمثل الركن الشرعي للجريمة الإلكترونية في التشريع الجزائري يمكن تكييف هذه الأفعال المجرمة بأنها جرائم ضد أموال الغير والمضرة بالمجتمع وهي تعتبر من ضمن جرائم الاختلاس وخيانة الأمانة والنصب غير السرقة لاعتبار أن السرقة فعل الاستيلاء على مال الغير ماديا. (عاقلي، 2017)

8. آليات التصدي لهذه الجرائم الإلكترونية:

إن الانترنت اختراع بشري يحمل في طياته بذور الخير والشر معا، ولم يكن منذ الوهلة الأولى موضوع الحماية المعلوماتية مطروحا حيث كان استعماله محتكرا من طرف فئة معينة. إلا أن انتشار استعمال الأنترنت أظهر عيوبا، فسجل أول اختراق للشبكة سنة 1988حيث توقف عملها لمدة ثلاث أيام، ولذلك كان لابد من إيجاد برامج أمنية وقواعد

قانونية للحماية من الجرائم الإلكترونية. (فرج يوسف، 2009)

1.8 الشق التشريعي:

سنت عدد من الدول الأوربية قوانين خاصة بجرائم الانترنت والحاسوب، مثل بريطانيا وهولندا وفرنسا والدنمارك والمجر وبولندا واليابان وكندا، كما اهتمت البلدان الغربية بإنشاء أقسام خاصة بمكافحة جرائم الإنترنت، بل إنها خطت خطوة إلى الأمام وذلك بإنشاء مراكز لاستقبال ضحايا تلك الجرائم. (سعدون، محمود، وحسن، 2011، ص.49)

أما على مستوى الدول العربية فقد قامت بالتوقيع على الاتفاقية العربية لمكافحة جرائم، تقنية المعلومات وذلك بتاريخ 2010/12/21، كما أدت هذه الاتفاقية كذلك لميلاد قوانين عديدة لمكافحة ما يسمى بالجرائم الإلكترونية في السعودية والأردن وقطر والإمارات والعراق وسلطنة عمان. وصارت الاتفاقية سارية المفعول بعد تصديق الرئيس المصري عليها سنة 2015 ليكتمل نصاب الدول السبع المطلوبة لسريانها. (مغازي، 2016)

2.8 الشق الأمني:

إن مواجهة مخاطر الجرائم المعلوماتية تعتمد على تبني إستراتيجية أمنية مجتمعية متكاملة، والتي تعمل مع أفراد المجتمع ومؤسسات القطاع الخاص، وهذه الرؤية تتسق مع نتائج الدراسات التي أجريت في بلدان مختلفة من العالم حول التعامل مع جرائم الإنترنت. والتي أوضحت أهمية مشاركة العديد من المصادر والمؤسسات الخاصة في تحمل جزءًا من المسؤولية؛ فيما يتعلق بمكافحة هذه الجرائم والسيطرة عليها وتلك المصادر تتمثل في: (عاقلي، 2017)

- مزودو خدمة الإنترنت الذين يملكون القدرة على تحديد ما يعرف ب (Internet Protocol) (IP) للمشتركين، ما يتيح إمكانية مراقبة الأنشطة الخطرة على الإنترنت وتقييد اشتراك المستخدمين المنخرطين في تلك الأنشطة.
- المواطن العادي بدوره كذلك يمكن أن يساهم من خلال تحمل مسؤولية حماية نفسه؛ من الوقوع ضحية لجرائم الإنترنت، باقتنائه برمجيات الحماية من الفيروسات. (قشقوش، 1992)

- المصارف التجارية وشركات البطاقات الائتمانية عليها أيضاً مسؤولية كبيرة في حماية عملائها؛ من خلال تطبيق إجراءات وقائية ضد الاحتيال، وكذلك تنصيب برمجيات مراقبة خاصة على خوادمها لتعقب النشاطات غير المعتادة ووضع أنظمة لتنبيه العملاء. (الملط، 1989)
- المحققين الخاصين الذين يعملون بالتنسيق مع أجهزة العدالة الجنائية. (القرني، 2014) وقد قدمت شركة فاير آي « Fire Eye » المتخصصة في مجال التصدي للهجمات الالكترونية؛ ثمانية إجراءات مهمة لتفادي الهجمات الالكترونية التي تستهدف دول الخليج العربي، بعدما كشفت عن جملة من التصورات والرؤى التحليلية بشأن مشهد الهجمات الالكترونية في مناطق أوروبا والشرق الأوسط وأفريقيا، وعلى وجه الخصوص في دول مجلس التعاون الخليجي، وتمثلت هذه الإجراءات في ما يلي: (الصريفي، 2009)
- التوقع الدائم بأن تكون تلك الشركات مستهدفة؛ وأنه من الممكن تخطي حدود الضوابط الأمنية المتوفرة لديها. والتأكد دائما من أن ليس هناك أي كيان تجاري بمنأى عن الهجمات. مع وضع إطار عمل خاص بالمخاطر ذات الصلة بالانترنت. والحصول على منصة استخبارات التهديدات الأنسب لتحسين قدرات الكشف عن الهجمات المحتملة. (الصريفي، 2009)
- إنشاء خدمة الاستجابة للحوادث الطارئة وإدارتها،والتي من شأنها تمكين الشركات من اكتشافها والتفاعل مع هجمات APT بالسرعة الممكنة.

9. نظرة عامة حول آليات مواجهة الجريمة الإلكترونية في الجزائر:

أول خطوة للحكومة الجزائرية لمواجهة ما يعرف بالجريمة الالكترونية، كان قانون صدر سنة 2009 القانون رقم 09-04 المؤرخ في 05 غشت 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. إلا أن تجسيد بنوده على أرض الواقع ضعيف،بعدما أهملت الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وتحديد العقوبة المناسبة في حق مرتكبيها، واقتصرت العقوبات في أغلب الأحيان على الغرامة المالية؛ ويتضمن القانون 19 مادة موزعة على 06 فصول، أعده نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني، من كافة القطاعات المعنية، يتضمن القانون أحكاما خاصة بمجال التطبيق، وأخرى خاصة بمراقبة الاتصالات الإلكترونية. وعددت الحالات التي تسمح

باللجوء إلى المراقبة الالكترونية، بالإضافة إلى القواعد الإجرائية المتضمنة، تفتيش المنظومات المعلوماتية وكذا حجز المعطيات المعلوماتية التي تكون مفيدة للكشف عن الجرائم الالكترونية. (جريدة رسمية، 2009)

ونص القانون في فصله الخامس على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم. وتتكفل أيضا بتبادل المعلومات مع نظيراتها في الخارج، قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم الالكترونية وتحديد مكان تواجدهم، كما أن هذا القانون أكد في فصله الأخير على مبدأ التعاون والمساعدة القضائية الدولية، من إطار مبدأ المعاملة بالمثل. (جريدة رسمية، 2009).

وفي نفس السياق، قال رئيس الكتلة البرلمانية لجبهة العدالة والتنمية لخضر بن خلاف، في تصريح خص به «يومية السلام اليوم» أن «مشكلتنا في قوانين سنّتها الحكومة فيما يخص الجريمة الإلكترونية ولم تطبّقها»، مضيفا أن هناك مراسيم متعلقة بهذا القانون المصادق عليه سنة 2009، لم تصدر لحد الساعة ولأسباب مجهولة، ما جعل حسبه، معالجة القضايا من هذا الشأن تصطدم بشبه فراغ قانوني، ما أدى في عديد الحالات إلى استصدار أحكام وعقوبات تقريبية لا سند لها، كما دعا نفس المتحدث، الحكومة إلى ضرورة مراجعة موقفها تجاه هذا القانون، وقال: لا بد من إيلائه أهمية أكبر في ظل دخول الشارع الجزائري نفق الإدمان، والاعتماد الرهيب على شبكة الإنترنت؛ وما يصاحبها من آليات وخدمات إلكترونية، فضلا عن فتح المجال السمعي البصري، مشددا في السياق ذاته على ضرورة تشريع قوانين جديدة.

وفي الجزائر وللأسف، فإن الجانب القانوني متقدم كثيرا عن الجانب التقني، ومنذ أكثر من10 سنوات، السلطات المخولة أعدت الإطار القانوني لتسيير شروط استخدام التصديق الالكتروني وتأمينه. بالمقابل وفي الوقت الذي انتظم فيه قراصنة الواب أكثر وتحولت فيه البيانات على قيمة مالية، تم المصادقة بالإجماع على قانون التجارة الالكترونية في البرلمان، بغياب التصديق الالكتروني "المصنوع في الجزائر". هذه الوضعية جد مقلقة من منطلق أن البيانات التي يتم تبادلها عبر المعاملات التجارية، ستكون

مجردة من طابع السرية والحماية.

كما أن التصديق الإلكتروني يقوم بحماية عملية بعث الرسائل انطلاقا من أجهزة الهواتف النقالة. ومع ذلك، فإن وعي الحكومة في مجال التوقيع الإلكتروني يجب أن يتم مرافقته بإجراءات ذات صلة بشروط استخدام التوقيع الالكتروني وتأمينه، مع ضمان كامل للسرية والحماية لمحتوى الوثائق الموقعة، واستحالة استخدامه من أشخاص آخرين، وتحسين تكلفة الحصول عليه، وخاصة حماية هوية صاحب التوقيع. (قاسمي، 2014)

10. الهياكل الخاصة للتصدي للجرائم الإلكترونية في الجزائر:

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال :

وأنشئت بموجب القانون رقم04-09 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. ومن مهام الهيئة الوطنية تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق العمليات الوقاية، ولمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية،في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية الاقتصاد الوطني. (أنظر القانون رقم 04-09)

ثانيا:الهيئات القضائية الجزائية المتخصصة:

أنشئت بموجب القانون 14/04المؤرخ في 2004/11/10 المعدل والمتمم لقانون الإجراءات الجزائية تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد329،37،و40 من ق.إ.ج.تتمتع اختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم 348/06 المؤرخ في 2006/01/05.بحيث تنظر في القضايا المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 09/04. (أنظر: هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية)

ثالثا:المعهد الوطني للأدلة الجنائية وعلم الجرائم :

يتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية،و دائرة الإعلام الآلي

والالكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد للعدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات. (أنظر:د/ حملاوي عبد الرحمان، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية).

رابعا:المديرية العامة للأمن الوطني:

تتصدى هده المديرية للجريمة الإلكترونية من عدة جوانب وأ منها الجانب التوعوي بحيث لم تغفل المديرية العامة للأمن الوطني عن الوقاية التوعية وهذا من خلال برمجتها لتنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الالكترونية. (عاقلي، 2017)

ودائما في إطار مكافحة الجريمة الالكترونية ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم، فأكدت عضويتها الفعالة في المنظمة الدولية للشرطة الجنائية INTERPOL هاته الأخيرة تتيح مجالات للتبادل المعلوماتي الدولي وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين، وكذا مباشرة الانابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا. (القهوجي،علي)

خاتمة:

وعلى ضوء ما تم تقديمه سابقا وصلنا إلى جملة من النتائج نستعرضها فيما يلي:

– قلة الدراسات حول الجريمة الإلكترونية في الجزائر خاصة مجال المعلوماتية. ومن هذا المنطلق رأينا الحاجة الماسة لدراسة مثل هذه المواضيع الهامة والراهنة نظرا للتزايد المستمر لها.

– عدم وجود تعاون دولي لمواجهة الجرائم الإلكترونية، وذلك من خلال إبرام اتفاقيات ومعاهدات تجرم التصرفات غير المشروعة في البيئة الرقمية.

– وجود مشكل في القوانين التي سنّتها الحكومة فيما يخص الجريمة الإلكترونية وعدم تطبيقها. فرغم اجتهاد المشرع الجزائري للتصدي لهذه الجريمة،إلا أنه لم يخصها بقانون حديث قائم بذاته للتحكم فيها بصرامة.

– عدم حث الجامعات والمراكز البحثية العربية، للبحث والدراسة في الجرائم المعلوماتية والجرائم عبر الانترنت، وعدم إنشاء دبلومات متخصصة في المجالات الفنية والقانونية المتعلقة بمكافحة تلك الجرائم.

– افتقار الاعتماد على أساليب وتقنيات متطوّرة للتمكن من الكشف عن هوية مرتكب الجريمة؛ بأقل وقت ممكن. ونقص توفر الكوادر البشرية العاملة في مجالات مكافحة الجرائم المعلوماتية.

– قصور في الوعي والثقافة، وعدم إدراك أهمية التصدي للجريمة الالكترونية لدى الكثير من المسؤولين؛ وعدم وجود جهة موحدة ومستقلة تحتوي النشاطات التوعوية وترعاها.

– عدم تعميم أو قلة استخدام بطاقات الائتمان وبطاقات الدفع الالكترونية المتطورة بالشكل المناسب؛ مما سبب محدودية الأنشطة في هذا المجال. في ظل انعدام قانوني ينظم المعاملات التجارية وعلى رأسها التوقيع والتصديق الالكترونيين. إذ لم تلقى قبولا وثقة شاملين فتفضيل الجزائريين وسائل الدفع التقليدية يعيق استخدام المعاملات الإلكترونية في غالب الأحيان.

– نقص توعية الأفراد ونصحهم لماهية الجرائم الإلكترونية وكل ما يترتب عنها من مخاطر.

اقتراحات وتوصيات الدراسة:

على ضوء ما سبق من عرض دراستنا، فان الأمر يستدعي إعطاء الأهمية لهذا النوع من الجرائم عن طريق إعادة هيكلة المنظومة بين الدولة والمساهمين والمشتركين لتحقيق الأمن ومن أجل ذلك، فإننا نوصي بـ:

– تنظيم حملات توعية لمستعملي تقنية (الحاسوب، الانترنيت، الهواتف الذكية...)، مع ضرورة أخذ الحيطة والحذر أثناء استخدام الانترنت، وعدم تصديق كل ما تحتويه البيئة الرقمية من إعلانات وغيرها. والتأكد من مصداقيتها.

– التكوين المستمر للكوادر البشرية العاملة في مجال مكافحة الجريمة الإلكترونية؛ مع إنشاء مجموعات عمل عربية لدراسة ووضع استراتيجيات وسياسات وإجراءات تنفيذية لمواجهة مثل هذه الجرائم.

– التحديث المستمر لكل التقنيات وبرامج الحماية الخاصة بأجهزة الحاسوب ومنها Norton.. MCafee ؛ومواكبة التطورات المرتبطة بالجريمة.

– رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الإنترنت؛ إذ يستلزم التدخل الحكومي والدولي وحث جامعة الدول العربية لإصدار قانون نموذجي موحد لمكافحة الجرائم المعلوماتية.

– الحرص على الحفاظ على سرية المعلومات الخاصة بالعناوين الإلكترونية، كالحسابات البنكية، والبطاقات الائتمانيّة وغيرها. وعدم الكشف عن كلمة السر نهائياً وتغييرها بشكل مستمر واختيار كلمات سر صعبة.

– تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي والحاسوب، وكذا تجنّب تحميل أي برنامج مجهول المصدر. واستخدام برمجيات آمنة ونظم تشغيل خالية من الثغرات.

– تأسيس منظمة خاصة لمكافحة الجرائم الإلكترونية والحد منها؛ والمسارعة في الإبلاغ للجهات الأمنية فور التعرض لجريمة إلكترونية.

– عدم ترك جهاز الحاسوب مفتوحاً وفصل اتصاله بشبكة الإنترنت في حال عدم الاستخدام.

– لا تضع معلومات على الانترنت لا تحب أن يراها الجميع، وتذكر أنه بمجرد أن تضع معلومات على الانترنت لن تتمكن أبدا من إرجاعها مرة أخرى حتى لو قمت بحذفها، مثل الاسم بالكامل ورقم الهاتف ورقم الهوية ورقم بطاقة الائتمان وأيضا العنوان بالتفصيل.

المصادر والمراجع

كتب = Books

*الصمدعي، محمود جاسم، ردينة عثمان يوسف، (2012).التسويق الإلكتروني. دار الميسرة للنشر، عمان.

*عبد الفتاح، مراد، (2012). كيف تستخدم الانترنت في البحث العلمي. دار الحديث، القاهرة.

*الصريفي، محمد، (2009). البيع والشراء عبر الأنترنت. المكتب الجامعي الحديث، الإسكندرية.

*سيارة، مصطفى. (2008). الجريمة الالكترونية." مجلة المعلوماتية"، (العدد 29)شهر تموز 2008.

*خليل، ناصر وسام،(2009). التجارة والتسويق الالكتروني. دار أسامة للنشر والتوزيع، الأردن.

توثيق فصل من كتاب محرر Article/Chapter in an Edited Book

*أبو فارة، يوسف أحمد،(2007). التسويق الالكتروني: عناصر المزيج التسويقي عبر الأنترنت (ط.2).دار وائل للنشر، الأردن.

*عليان، ربحي مصطفى، إيمان فاضل السمرائي، (2015).تسويق المعلومات وخدمات المعلومات (ط.2).دار صفاء للنشر، عمان.

وثائق الباور بوينت والبي.دي.إف. = PowerPoints, PDF documents

*القانون رقم 09-04 المؤرخ في 05 غشت 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية رقم 47، ص 5.

*يونس، عرب. جرائم الكمبيوتر والانترنت-إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرامية للملاحقة والإثبات . ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002 – تنظيم المركز العربي للدراسات والبحوث الجنائية-أبو ظبي 10-12 /2/2002.متاح على الخط (http://almuhamatresalah.blogspot.com/2014/03/blog-post_2785.html) تمت الزيارة يوم 2021/01/01 على الساعة 09:58.

*البحر، عبد الرحمن (1999). معوقات التحقيق في جرائم الأنترنت.)رسالة ماجستير غير منشورة أكاديمية نايف العربية للعلوم الأمنية، الرياض

*حجازى، محمد .(2010). الجريمة الالكترونية والعالم العربي (رسالة ماجستير غير منشورة).عضو مجلس إدارة المركز المصري للملكية الفكرية؛ القاهرة.

*القانون رقم 09-04 المؤرخ في 05 غشت 2009، مرجع سبق ذكره، ص 5- 8.

مقالات المجلات = Journal & Magazine Articles

*البداينة، ذياب موسي. ورقة عمل بعنوان (الجرائم الالكترونية المفهوم والأسباب)- عمان المملكة الأردنية الهاشمية – 2014- الملتقي العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة 2-4/9 / 2014.ص.52

*إسراء جبريل رشاد مرعي، الجرائم الالكترونية- الأهداف-الأسباب-طرق الجرائم ومعالجتها، مقال منشور على الموقع الالكتروني للمركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، قسم الدراسات المتخصصة، على الرابط : http://democraticac.de/?p=35426تاريخ الاطلاع 2021/02/13.

*مفتاح بوبكر المطردي، الجريمة الالكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بالسودان المنعقد في 23-2012/9/25، ص 16.

*سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبد الرحمن،(جوان،2011)، الجريمة الالكترونية عبر الانترنيت أثرها وسبل مواجهتها، "مجلة التقني"، المجلد 24(العدد 06)، ص 49.

*عزة مغازي، قانون الجريمة الإلكترونية.. التورنت يحملك إلى طرة، مقال منشور على موقع المنصة بتاريخ 2016/02/04 على الرابط : https://almanassa.com/ar/story/1019، تاريخ الاطلاع 2021/02/12.

*عبدالله بن فارع القرني، (2014/02/21)، مواجهة جرائم الإنترنت: نحو إستراتيجية أمنية – مجتمعية متكاملة، مقال منشور على موقع جريدة الرياض بتاريخ على الرابط http://www.alriyadh.com/912032 : تاريخ الاطلاع: 2021/02/12.

مواقع الإنترنت = Web Sites

*حفوظة، الأمير عبد القادر. غرداين، حسام. الجريمة الالكترونية وآليات التصدي لها. متاح على الخط " https://jilrc.com/%D8%A7%D9%84% 9تمت الزيارة يوم 2021/01/10.

*عبد العال الديربي، (2013/01/13)، الجريمة المعلوماتية. تعريفها، أسبابها، خصائصها، دوريات مفاهيم إستراتيجية، المركز العربي لأبحاث الفضاء الالكتروني، على الرابط http://accronline.com/article_detail.aspx?id=7509 تاريخ الاطلاع 2020/02/13.

*مطـــــر، كامل. الجريمة الإلكترونية. منصة لخصلي العربية. متاح على الخط-https://lakhasly.com/en/view summary/0WNxl49Jynتمت الزيارة يوم 2021/01/19.

*قاسمي. أ، (2014/01/25) 160مليار دولار سنويا مكاسب عصابات الجريمة المنظمة عبر الإنترنت، " يومية السلام اليوم"، على الرابط: http://essalamonline.com/ara/permalink/32212.html، تاريخ الاطلاع 2020/12/12.