الجريمة الإلكترونية في الفضاء الإلكتروني
المفهوم- الأسباب-سبُل المكافحة مع التعرض لحالة ليبيا

د. عبدالسلام محمد المايل
جامعة المرقب أستاذ إدارة الأعمال المساعد/
كلية الاقتصاد والتجارة– الخمس، ليبيا
amelmael@elmergib.edu.ly

د. عادل محمد الشربجي
أستاذ إدارة الأعمال المساعد/
جامعة المرقب ليبيا
كلية الاقتصاد والتجارة– فرع القره بولي
shurbagi@yahoo.com

د. على قابوسة
مخبر الاقتصاد السياسي بين التنمية الاقتصادية
والتحديات السياسية للدول العربية والأفريقية
بجامعة الوادي الجزائر

ملخص:

هدفت الدراسة إلى إلقاء الضوء على الجريمة الإلكترونية في الفضاء الإلكتروني، والأسباب الدافعة إلى ارتكاب الجريمة، واقتراح بعض الحلول التي من شأنها الحد من هذه الظاهرة ومكافحتها. تم استخدام المنهج الوصفي من خلال الكتب، والمقالات، والدوريات العلمية، والأبحاث التي تناولت الموضوع قيد الدراسة، أكدت الدراسة بأن الأسباب الحقيقية الدافعة إلى ارتكاب الجريمة الإلكترونية ترجع إلى جُملة من الدوافع منها: الدوافع الذاتية، الدوافع النفسية، الدوافع الاجتماعية، الدوافع المالية (الربح وكسب المال)، الدافع السياسي والعسكري، الدافع القومي والوطني، وتتفاوت أسباب الجريمة الإلكترونية وفق نوعها ونوع المستهدف ونوع الجاني ومستوى تنفيذه (فردي، مجتمعي، كوني). فجرائم الشباب والهواه والصغار تختلف عن أسباب جرائم المحترفين، وتختلف وفق هدفها سرقة معلومات أو تجارة بالمعلومات أو جرائم شخصية. وجاء في أهم نتائج الدراسةبأن التشريعات والقوانين تعتبر عاملاً مهماً في مواجهة الجريمة الإلكترونية (المعلوماتية) التي ترتكب في الفضاء الإلكتروني، بالإضافة إلى نقص الخبرة لدى العاملين في قطاع أمن المعلومات يتسبب في حدوث جرائم إلكترونية، كذلك قصور مؤسسات التعليم والمجتمع المدني في القيام بدورهم التوعوي والوقائي في مكافحة تلك الجرائم، وأن مكافحة الجرائم المعلوماتية في ليبيا مازالت بلا غطاء تشريعي يحددها ويجرم كافة صورها. أوصت الدراسة بضرورة تدخل المشرع القانوني لمواجهة الجريمة الإلكترونية (المعلوماتية) التي ترتكب في الفضاء الإلكتروني. تفعيل الأجهزة الخاصة بالخبرة الجنائية للجريمة الإلكترونية (المعلوماتية). العمل على إعادة النظر في المناهج الدراسية بالجامعات، وضرورة تضمينها مادة عامة عن الحاسب الآلي والشبكات المعلوماتية وكيفية التعامل مع الأجهزة الإلكترونية. إعداد الملتقيات العلمية وورش العمل حول تقنية الاتصالات والمعلومات والقانون. الاهتمام باتفاقيات التعاون الدولية والإقليمية والعربية لمكافحة الجرائم الإلكترونية (المعلوماتية).

كلمات مفتاحية: الجريمة الإلكترونية، الفضاء الإلكتروني، الحكومة الإلكترونية، الإدارة الإلكترونية.

Abstract

.

The research aims to shed light on the electronic crime in the electronic space, its causes, and to suggest some solutions to hinder such phenomenon .
Through descriptive approach (books, articles, scientific tours, and other researches), the research demonstrates the motives behind the electronic crime, to state some: personal drives, psychological drives, sociological drives, financial drives, military and political drives and patriotic and national drives. These crimes differ according to their types, the type of the target, the kind of the executor and the level of his execusion (individual, social, cosmos). Hence, the drives of the crimes of youth and amateurs differ from those who are experimented in stealing information or .trading with it
The most important results of the research show how law and legislation are indispensable to face the electronic crimes. In addition to the lack of experience in the workers in the security sector. Also, institutions of education and the civic society are not doing their role to make people aware of this phenomenon and how to fight it. In .Libya, for example, there is no legislation to demarcate or fight it
The research recommands the intervention of the legislator to face the electronic crimes; empower the sectors specialized in the electronic crimes; reevaluation of the syllabuses in schools and universities and the importance to include the subject of computer science and information webs and how to deal with electronic machines; organize conferences and workshops on communication, information and law; the consideration of the international and Arabic agreement contracts to fight the electronic crimes
.
Keywords: electronic crimes, electronic space, electronic government, electronic .administration

مقدمة:

انتشر الحاسوب وتقنية المعلومات والاتصالات في المنظمات بشكل كبير مع بدايات القرن العشرين، وأوضحت بعض التقديرات بأن حوالي 50% من استثمار رأس المال الجديد أصبح يوجد في مجال استخدام تقنية المعلومات والاتصالات (Westland & Clark, 2000)، إذ أن هذا الاستثمار يُحسن من معدل الإنتاج للمنظمات، ولن تقبل الفرد أو المستخدم لهذه التقنية الجديدة يعتبر مكسباً ونقطة قوة للمنظمة (المايل، 2017).

لذا، فإن الوقت الحاضر، هو عصر تقنية المعلومات والاتصالات، والتي تعتبر بحق أهم دعائم وأُسس تقدم الدول وتطورها وتحقيق الاستقرار الاقتصادي، وبهذا تتحول المنظمات إلى منظمات إلكترونية تستخدم شبكة الإنترنت في إنجاز كل معاملاتها وأعمالها الإدارية، بواسطة التبادل غير المادي للبيانات الرقمية فيما بين المؤسسات الحكومية (امحمد، 2010)، وذلك لتسهيل الحصول على البيانات والمعلومات لإتخاذ القرارات المناسبة وتقديم الخدمات للمستفيدين بكفاءة وفاعلية وبأقل تكلفه وبأسرع وقت ممكن.

لقد وفرت السهولة النسبية لاستخدام التقنية الجديدة والحصول على الإنترنت على نحو متزايد أكثر للأنترنت بأسعار معقولة والحصول على أجهزة الحاسوب مع أجهزة المودم فائقة السرعة، كل ذلك مكن الناس من التواصل وتكوين الصداقات الجديدة، والتجارة، والترفيه، والتعلم، والقيام بأعمال تجارية، ودفع الفواتير عبر الإنترنت. وكونت شبكة ويب العالمية ما يسمى العالم الافتراضي أو الفضاء الإلكتروني، والذي

يعرف بأنه "مكان لأجل غير مسمى حيث يتفاعل الأفراد والتجمعات". مما اتاح لكثير من الناس الانتقال من العالم الواقعي على العالم الافتراضي (البداينة، 2014). والجريمة ظاهرة اجتماعية ُوجدت بوجود الإنسان في المجتمع، ويحاول المجرمون اليوم الاستفادة من تكنولوجيا المعلومات والاتصالات في ارتكاب الجريمة، ولهذا ظهرت أنماط جديدة من الجرائم لم تكن معهودة من قبل تتسم بصعوبة اكتشافها وملاحقتها، حيث أنه رغم الفوائد العديدة التي لا تحصى للحكومة والإدارة الإلكترونية، إلا أنه في نفس الوقت تزايدت أساليب إساءة الاستخدام لمكوناتها، وأصبح الحاسب الآلي بشكل عام وشبكة الإنترنت على وجه الخصوص أدوات أو محل ارتكاب الجريمة بمفهومها الحديث، ومكنت مجرمي الفضاء الإلكتروني تصفح الإنترنت وارتكاب جرائم مثل القرصنة، الاحتيال، التخريب للحاسوب، الإتجار بالمخدرات، والتعامل في معلومات العدالة، المواد الإباحية، تخريب البيانات، غسيل الأموال (امحمد، 2010 : البداينة، 2014)، وهو ما يتسبب في مشاكل قانونية، واجتماعية، واقتصادية، وأمنية معقدة، مما يستدعي بالضرورة إصدار قوانين خاصة بالجريمة الإلكترونية تتماشى مع خصوصياتها، وتضمن أمن المعلومات الإلكترونية داخل إدارة المنظمات وخارجها.

مشكلة الدراسة:

أصبحت الجريمة الإلكترونيةأحدى أهم الأخطار التي تواجه الدول المتقدمة والنامية على حداً سواء، (حيث تكلف العالم 400 مليار دولار سنوياً)[1]، فهي عالمية بلا حدود حيث أن التحقيق فيها والحكم عليها عملية معقدة، ترتكب من قبل الأفراد أكثر مما ترتكب من محترفي الحاسوب وشبكات المعلومات. كما يمكن أن ترتكب من مراكز البحوث، ومن الأكاديميين، ومن مديرين يبحثون عن الثراء أو السلطة (البداينة، 2014)، أو من قبل منظمات تبحث عن معلومات عن منافسيها، أو من وسائل إعلام تبحث عن معلومات أو أخبار أو من قبل حكومات تبحث عن معلومات تجارية، أو جريمة منظمة تبحث عن ملفات موثوقة. ففي ظل التحول إلى الحكومة والإدارة الإلكترونية والتجارة الإلكترونية،...الخ، أصبح لزاما على الجهات المعنية إيجاد حلول لمختلف الصعوبات التي قد تعوق سير إدارة الخدمات الإلكترونية والعمل على إصدار التشريعات والقوانين المناسبة التي تمنع ارتكاب الجرائم الإلكترونية.

تأسيساً على ما تقدم تكمن مشكلة الدراسة للإجابة على التساؤلات التالية:

1. ماهية الجريمة الإلكترونية؟ وما هي فئات مجرمي المعلوماتية؟
2. ما هي الأسباب الدافعة إلى ارتكاب الجريمة الإلكترونية؟
3. ما أنواع الجرائم المعلوماتية أو الإلكترونية والوسائل المناسبة للحماية منها؟
4. ما هي الجرائم الإلكترونية المتواجدة بالمجتمع الليبي؟ وما موقف القانون الليبي منها؟
5. ما الُسبل والوسائل التي من شأنها مكافحة الجرائم الإلكترونية؟

أهداف الدراسة:

بُنيت الدراسة على عدة أهداف يُمكن إيجازها في الآتي :

1. التعرف على ماهية الجريمة الإلكترونية وفئات مجرمي المعلوماتية.
2. استعراض الأسباب الدافعة إلى ارتكاب الجريمة الإلكترونية.
3. التعرف على أنواع الجرائم المعلوماتية أو الإلكترونية والوسائل المناسبة للحماية منها.
4. التعرف على الجرائم الإلكترونية المتواجدة بالمجتمع الليبي وموقف القانون الليبي منها.
5. الوقوف على أهم الُسبل والوسائل التي من شأنها مكافحة الجرائم الإلكترونية.

[1] http://www.elaph.com/Web/News/**2014/6/9**12485.html#sthash.aMlqRPpO.dpuf

6. اقتراح جُملة من التوصيات التي من شأنها الحد أو التقليل من الجرائم الإلكترونية في الفضاء الإلكتروني.

أهمية الدراسة:

تنبثق هذه الدراسة من كونها تتناول موضوع مهماً في مجال تقنية المعلومات والاتصالات. وبالتالي يمكن القول أن دراسة موضوع الجريمة الإلكترونية في الفضاء الإلكتروني، وفهم جوانبها النظرية والوصفية من شأنه الاستفادة منه في كافة المؤسسات والهيئات التي تسعى إلى تطبيق نظام الحكومة والإدارة الإلكترونية، ولكونه يمس كثيراً من مصالح المجتمع. من جانب آخر، أصبح هناك حاجة للتعريف بهذه الجرائم والتوعية ومتابعة هذا النوع من الجرائم وسن القوانين والتشريعات اللازمة لمكافحتها، نظًرا لما تسببه من خسائر مادية ومعنوية كبيرة. وبهذا، فأن هذه الدراسة تساهم وبشكل مباشر في الوصول إلى جُملة من التوصيات التي من شأنها محاربة هذه الظاهرة ومكافحتها والحد منها حتى يُمكن أن يتحسن أداء القطاعات بمختلف مؤسسات الدولة.

منهجية الدراسة:

اتبع الباحثان في هذه الدراسة المنهج التاريخي، والمنهج الوصفي لدراسة ظاهرة الجريمة الإلكترونية في الفضاء الإلكتروني وفق الآتي:

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

2. المنهج الوصفي: من خلال هذا المنهج تم التطرق إلى الجوانب المتعلقة بالجريمة الإلكترونية في الفضاء الإلكتروني، وذلك للإجابة على تساؤلات الدراسة.

مصطلحات الدراسة:

الجريمة الإلكترونية: هي الجريمة التي يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، أو في بيئة إلكترونية.

الفضاء الإلكتروني: هو الوسط الذي تتواجد فيه شبكات الحاسوب ويحصل من خلالها التواصل الإلكتروني (ويكيبيديا).

الحكومة الإلكترونية: الاستخدام التكاملي الفعال لجميع تقنيات المعلومات والاتصالات بهدف تسهيل العمليات الإدارية اليومية للقطاعات الحكومية، وتلك التي تتم فيما بينها (حكومية - حكومية (G2G)، وتلك التي تربطها بالمواطنين (حكومية - مواطن (G2C) أو قطاعات الأعمال (حكومية - أعمال (G2B) أو الموظفين(G2E).

الإدارة الإلكترونية: تحويل كافة الأعمال والخدمات الإدارية التقليدية (الإجراءات الطويلة باستخدام الأوراق) إلى أعمال وخدمات إلكترونية تنفذ بسرعة عالية ودقة متناهية، باستخدام تقنيات الإدارة وهو ما يطلق عليه إدارة بلا أوراق.

1. الجريمة الإلكترونية

1.1. مفهوم الجريمة الإلكترونية

تعرف الجريمة عموما، في نطاق القانون الجنائي - الذي يطلق عليه أيضا تسميات قانون الجزاء وقانون العقوبات وينهض بكل تسمية حجج وأسانيد لا يسمح المقام لعرضها بأنها "فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيرا احترازيا" (حسني، 1989: السعيد، 1983)، وتعرف أيضاً بأنها كل فعل يعاقب عليه القانون أو امتناع عن فعل يقضي به القانون، ويحدد القانون عقوبات محددة للمخالفات بمعنى أنه لا يمكن معاقبة أي فعل ما لم يكن هناك نص محدد له في القانون وإلا لا يعتبر جرم (مصطفى وآخرون، 2011). من ناحية أخرى الجريمة هي كّل فعل ضار يأتيه المواطن ويكون لهذا الفعل أثر ضار على غيره من المواطنين. وبالتالي فالجريمة الإلكترونية أي فعل ضار يأتيه المواطن عبر استعماله الوسائط الإلكترونية مثل الحواسيب، أجهزة الموبايل، شبكات الاتصالات الهاتفية، شبكات نقل المعلومات، شبكة الإنترنت، أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية. ولقد ظهر أيضاً مصطلح cyber crime الذي يعني الجرائم التي ترتكب باستخدام الحاسوب وشبكة الإنترنت، فهي كلها مصطلحات تدل على الجريمة الناشئة عن استغلال تقنية المعلومات

واستخدامها، وذلك لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات (البشري، 2008 : امحمد، 2010)، وقد عرفها مؤتمر الأمم المتحدة في سنة 2000 م، بأنها الجريمة التي يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، أو في بيئة إلكترونية. وعرفها أيضاً خبراء منظمة التعاون الاقتصادي والتنمية، الجريمة الإلكترونية بأنها: كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/أو نقلها، وقد وضع هذا التعريف مجموعة من الخبراء المشار إليهم للنقاش في اجتماع باريس الذي عقد عام 1983 ضمن حلقة) الاجرام المرتبط بتقنية المعلومات(شعبان، 2009).

بناء على ما سبق يمكن أن يكون الحاسب الآلي إما موضع الجريمة كتدمير البيانات، أو التخريب لأجزاء الحاسب وبرامجه، وقد يكون الحاسب أداة لارتكاب الجريمة عن طريق استخدامه للاحتيال والتجسس وسرقة الأموال، وإجراء تحويلات من حساب لحساب آخر أو سرقة أرقام بطاقات الائتمان واستخدامها في الشراء عبر شبكة الإنترنت (امحمد، 2010)، كما قد يكون الحاسب الآلي هو ضحية للجريمة الإلكترونية سواء على الكيان المادي أي كافة الأجهزة المستخدمة في الحاسوب (hardware) أو الكيان المعنوي أي البرامج (software) كتعطيل خادم موقع مؤسسة أو إرسال الفيروسات، وهذه الجرائم لا تعترف بالحدود بين الدول ولا حتى بين القارات حيث تعد من الجرائم الحديثة التي تستخدم فيها شبكة الإنترنت باعتبارها أداة لارتكاب الجريمة أو تسهيل ارتكابها.

لقد كون الفضاء الإلكتروني فرصاً جديدة للمجرمين لارتكاب الجرائم من خلال خصائص فريدة من نوعها في هذا الفضاء، أن هذه الميزات تشكل مفاتيح تحويلية (transformative Keys) وهي:

(1) العولمة (globalization) والتي تمكن الجناة مع وجود فرص جديدة من تجاوز الحدود التقليدية. (2) شبكات التوزيع (distributed networks) فقد ولدت فرصاً جديدة لتكوين ضحايا.

(3) الإجمالية والشمولية (synopticism and panopticism) والتي تمكن الجناة من أذلال ضحاياهم عن بعد.

(4) مسارات البيانات (data trails) والتي خلقت فرصاً جديدة للجنائي لارتكاب سرقة الهوية. ويمكن مقارنة بعض نماذج الجريمة التقليدية مع الجريمة الإلكترونية في الفضاء الإلكتروني لتوضيح كيف انتقلت الجريمة من الواقع المادي إلى الواقع الافتراضي (البداينة، 2014).

جدول رقم 1: نماذج من الجريمة التقليدية والجريمة الإلكترونية

الجريمة التقليدية	الجريمة الإلكترونية
الاحتيال	الاحتيال على الشبكة، الاحتيال بالمزاد الإلكتروني....الخ
السطو	القرصنة على الإنترنت، الحرمان من الخدمة، الفيروسات
جرائم الأطفال الجنسية	استمالة الأطفال على النت، المواقع الإباحية
غسيل الأموال	أنظمة الدفع على الشبكة
السرقة	جرائم الهوية، وسرقة الملكية

وقد كّرست اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا) جزءاً من أنشطتها لتطوير نهج متقدم لوضع تشريعات تقوم بالتنسيق على الصعيد الإقليمي للتصدي لهذه الظاهرة، فأصدرت في سنة (2007)، دراسة بعنوان" نماذج تشريعات جرائم الفضاء الإلكتروني (السيبرانية) في البلدان الأعضاء في الإسكوا" وقامت بتحليل التشريعات المعتمدة في هذه البلدان وبمقارنتها مع التشريعات المطبقة في عدد من البلدان الأخرى. وقدمت الإسكوا في هذا السياق مجموعة من الإرشادات التي ترمي إلى مساعدة البلدان العربية على تحسين البيئة المناسبة لسن التشريعات فيها وتشمل المجالات الستة التالية :حماية البيانات الشخصية؛ الاتصالات الإلكترونية وحرية التعبير؛ التواقيع الإلكترونية والعمليات الإلكترونية؛ التجارة الإلكترونية وحماية المستهلك؛ الملكية الفكرية؛ والجرائم الإلكترونية (الإسكوا، 2012).

2.1. المجرم المعلوماتي أو المجرم الإلكتروني

أضافت المعلوماتية الكثير من الجوانب الإيجابية إلى حياتنا إلا أنها في المقابل جلبت معها نسلاً جديداً من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية أو المجرمين الإلكترونيين، ويعرف المجرم المعلوماتي (الإلكتروني) بأنه المجرم الذي لديه قدرة على تحويل نواياه إلى لغة رقمية باستخدام التقنية الرقمية المعلوماتية، وذلك بأداء فعل أو الامتناع عنه، مما يحدث اضطرابات في المجتمع المحلي أو الدولي نتيجة مخالفته قواعد الضبط الاجتماعي محلياً أو دولياً (امحمد، 2010).

3.1. صفات المجرم المعلوماتي (الإلكتروني)

ليس هناك اتفاق على صفات مرتكبي الجرائم الإلكترونية ومنفذيها، ولا يوجد قالب يتضمن الفئات والسمات التي يتسم بها مرتكب الجريمة المعلوماتية، إلا أن هناك صفات ذات دلالة مشتركة يجمع المختصون بأنها توجد في كل الأشخاص الذين تم التحقيق والقبض عليهم في جرائم من هذا النوع، حيث أوردت العديد من الدراسات العربية والأجنبية في هذا المجال بأن متوسط عمر مرتكبي هذه الجرائم بين 14-38 سنة، وهذا يدل بأن أغلب مرتكبي الجرائم الإلكترونية من فئة الشاب، ويتميز المجرم المعلوماتي بعدد من السمات والخصائص هي:

- المجرم المعلوماتي يتمتع بالمهارة والمعرفة والذكاء، حيث يمكنه التغلب على الكثير من العقبات التي تواجهه أثناء ارتكاب الجريمة.

- المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي، حيث أن المزايا التي يتمتع بها المجرم المعلوماتي تمكنه من ارتكاب جريمته، وقد تتمثل هذه السلطة مثلاً في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي المجرم إمكانية فتح الملفات وقراءتها وكتابتها ومحو المعلومات.

- المجرم المعلوماتي شخص ذو مهارات فنية عالية متخصص في الإجرام المعلوماتي (الإلكتروني)، قادر على استخدام خبراته في الاختراقات وتغيير المعلومات.

- المجرم المعلوماتي قادر على تقليد البرامج وتحويل الأموال، محترف في التعامل مع شبكات الحاسبات، وهو شخص غير عنيف لأن تلك الجريمة لا تلجا إلى العنف لارتكابها(امحمد، 2010).

4.1. فئات مجرمي المعلوماتية

توصلت الدراسات والأبحاث التي تناولت مجرمي المعلوماتية إلى تصنيف المجرمين الإلكترونيين إلى أنماط، لكن لابد من الإشارة إلى أن هذه التصنيفات لا تعني أن كل مجرم معلوماتي يندرج تحت فئة محددة دون غيرها من الفئات المذكورة، بل يمكن أن يكون المجرم الواحد مزيجاً من أكثر من طائفة أو فئة.

1.4.1. فئة صغار مجرمي المعلوماتية

يسميهم البعض صغار نوابغ المعلوماتية، ويقصد بهم الشباب البالغ المفتون بالمعلوماتية وأنظمتها، حيث يجب عدم التقليل من خطورة هؤلاء الأشخاص، فهذه الفئة قد تتعدى مرحلة الهواية والعبث لتدخل مرحلة متقدمة أكثر في ارتكاب الجرائم المعلوماتية، وهي مرحلة الاحتراف لهذه الجرائم، كما أنه هناك مخاوف تتمثل في احتضان منظمات الجريمة المنظمة لهذه الفئة للاستفادة من مهاراتهم وتطويرها، حيث أن هذه الفئة أكثر تقبلاً لأي أفكار تعرض أو تفرض عليها خاصة إذا كانت تحمل المغامرة والإثارة والتحدي في طياتها. ومن الأمثلة الشهيرة لجرائم الحاسوب التي ارتكبت من هذه الفئة، العصابة الشهيرة التي أطلق عليها عصابة (414)، والتي نسب إليها ارتكاب ستين فعَل تعد في الولايات المتحدة الأمريكية على ذاكرات الحواسيب (شعبان، 2009)، حيث نجم عنها أضرار كبيرة لحقت بالمنظمات العامة والخاصة.

2.4.1. فئة القراصنة

هم عادة مبرمجون من أصحاب الخبرة يدخلون إلى الأنظمة المعلوماتية غير المسموح لهم بالدخول إليها، وكسر الحواجز الأمنية المحيطة بهذه الأنظمة، وهم نوعين: القراصنة الهواة العابثون أو الهاكرز (Hackers)، وهم المتطفلون والمتسللون يتحدون إجراءات أمن الشبكات لكن لا تتوفر لديهم في الغالب دوافع التحدي واثبات الذات، وهذه الفئة أغلبها من التلاميذ وطلبة الثانويات والشباب العاطل عن العمل. أما القراصنة المحترفون الكراكرز (Crackers) أو المقتحم، هو الشخص الذي يقوم بالتسلل إلى نظام الحاسوب للاطلاع على المعلومات المخزنة فيه أو لإلحاق الضرر أو العبث بها أو سرقتها (محمد، 2010)، ويتراوح اجمالي الخسائر الناجمة عن القرصنة الالكترونية بين 375 و575مليار دولار سنوياً[2].

3.4.1. فئة الموظفون العاملون في مجال الأنظمة المعلوماتية

وهذه الفئة من المجرمين يشكل النظام المعلوماتي مجال عملهم الأساسي، ولهذا فهم يقترفون جرائم تمكنهم من تحقيق أهدافهم الشخصية، هؤلاء يعودون إلى مقر عملهم بعد انتهاء الدوام ويعمدون إلى تخريب الجهاز أو إتلافه أو سرقته، وقد يجد الموظف نفسه أحيانا مرتكبا لجريمة إلكترونية صدفة ودون تخطيط مسبق لها.

4.4.1. فئة مجرمو المعلوماتية أصحاب الآراء المتطرفة

وتتكون هذه الفئة من الجماعات الإرهابية أو المتطرفة التي تتكون من مجموعة من الأشخاص لديهم معتقدات أو أفكار اجتماعية أو سياسية أو دينية، ويرغبون في فرض هذه المعتقدات باللجوء إلى النشاط الإجرامي.

5.4.1. فئة الحاقدون

هذه الفئة يغلب عليها عدم توفر أهداف وأغراض الجريمة المتوفرة لدى الفئات الأخرى، فهم لا يسعون إلى إثبات المقدرات التقنية والمهارية، وبنفس الوقت لا يسعون إلى مكاسب مادية أو سياسية؛ إنّما يحرك أنشطتهم الرغبة بالانتقام والثأر كأثر لتصرف صاحب العمل معهم، أو لتصرف المنظمة المعنية معهم عندما لا يكونوا موظفين فيها (شعبان،2009)، ولهذا فإنهم ينقسمون إما إلى مستخدمين للنظام بوصفهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنظمة المستهدفة في نشاطهم.

6.4.1. فئة مجرمو المعلوماتية في إطار الجريمة المنظمة

الجريمة المنظمة هي تعبير عن مجتمع إجرامي يعمل خارج الشعب والحكومة، ويضم في طياته الآلاف المجرمين الذين يعملون وفقا لنظام بالغ الدقة والتعقيد يفوق النظم التي تتبعها أكثر المنظمات تطوراً وتقدماً، كما يخضع أفرادها إلى أحكام قانونية سنوها لأنفسهم، وتفرض عليهم أحكاما بالغة القسوة على من يخرج عن الجماعة، ويلتزمون في أداء أنشطتهم الإجرامية التخطيط الدقيق والمدروس، حيث يجنون من ورائه الأموال الطائلة (امحمد، 2010). ومن أمثلة هذه الجرائم، عصابات سرقة السيارات الذين يحددون بواسطة شبكة الإنترنت الأماكن التي ترتفع بها أسعار بيع قطع غيار السيارات ومن ثم يبيعون القطع المسروقة في تلك الأماكن ليضمنوا أكبر ربح ممكن.

5.1. الأسباب الدافعة إلى ارتكاب الجريمة الإلكترونية

لا تختلف الأسباب الدافعة إلى ارتكاب الجريمة الإلكترونية عن باقي أنواع الجرائم الأخرى، ومن أبرزها:

1.5.1. الدوافع الذاتية: والتي تجعل من الشخص يقوم بارتكاب عدد من المخالفات نابعة من حب الاستطلاع والتحدي والرغبة في قهر النظام المعلوماتي واثبات الذات.

2.5.1. الدوافع النفسية: وتكون من شخص لديه خلل نفسي أو أمراض نفسية تنعكس على السلوك.

3.5.1. الدوافع الاجتماعية: وتتمثل في الاختراقات للأجهزة الشخصية والتعرف على نقاط الضعف لدى الآخرين.

[2] http://www.elaph.com/Web/News/**2014/6/9**12485.html#sthash.aMlqRPpO.dpuf

4.5.1. الدوافع المالية (الربح وكسب المال): وذلك بالرغبة في تحقيق مكاسب مادية تكون هائلة أحيانا بزمن قياسي قد يكون من أكثر البواعث التي تؤدي إلى إقدام مجرمي المعلوماتية على اقتراف جرائمهم من اجل تحقيق المكاسب المالية.

5.5.1. الدافع السياسي والعسكري: التطور العلمي والتقني أديا الى الاعتماد بشكل شبة كامل على أنظمة الحاسوب، وبذلك أصبح الاختراق من اجل الحصول على معلومات سياسية وعسكرية واقتصادية مسالة أكثر أهمية.

6.5.1. الدافع القومي والوطني: وهو أن يقوم الهاكرز بالهجوم على مواقع معادية تختلف مع قيم وعادات مجتمع ما بتدمير أو تغيير هذه المواقع، مما يؤدي إلى منعها من تهديد فكر وسلوك أفراد ذلك المجتمع (امحمد، 2010).

في حين أشار البداينة إلى الأسباب التي يمكن حصرها كأسباب للجريمة الإلكترونية منها ما يقع على مستوى كوني، ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى فردي أو شخصي. كما أن أسباب الجريمة الإلكترونية تتفاوت وفق نوعها ونوع المستهدف ونوع الجاني ومستوى تنفيذه (فردي، مجتمعي، كوني). فجرائم الشباب والهواه والصغار تختلف عن أسباب جرائم المحترفين، وتختلف وفق هدفها سرقة معلومات أو تجارة بالمعلومات أو شخصية....الخ.

جدول رقم 2: أسباب الجريمة الإلكترونية وفق مستوى التحليل

أسباب الجريمة على المستوى الفردي	أسباب الجريمة على المستوى المجتمعي	أسباب الجريمة على المستوى الكوني
البحث عن التقدير: هي جرائم يرتكبها شباب طائش وصغار سن، وذلك من باب التحدي، وحب الظهور في الإعلام.	التحضر: يعد التحضر أحد أسباب الجريمة الإلكترونية عامة، حيث الهجرة الكبيرة من الريف إلى المدينة وإلى المناطق الحضرية والمدن الكبيرة.	التحول للمجتمع الرقمي: ففي الفضاء الافتراضي، تكونت التفاعلات الافتراضية وحلت محل التفاعل وجها لوجه، وتكونت السلوكيات الافتراضية والشخصية الافتراضية والمجتمع المحلي الافتراضي.
الفرصة: لقد وفرت التقنيات الحديثة والإنترنت فرصاً غير مسبوقة لانتشار الجريمة الإلكترونية.	البطالة: ترتبط الجريمة الإلكترونية شأنها شأن الجريمة التقليدية بالبطالة والظروف الاقتصادية الصعبة.	العولمة: إن ظهور الفضاء الإلكتروني يكون ظواهر جديدة متميزة عن وجود أنظمة الكمبيوتر أنفسها، والفرص المباشرة للجريمة والتي وفرتها أجهزة الكمبيوتر الآن. فالأشخاص، على سبيل المثال، قد يرتكبون جرائم في الفضاء الإلكتروني لا يرتكبونها في الواقع المادي بسبب مكانتهم وموقعهم.
ضبط الذات المنخفض: إن توفر صفة الضبط الذاتي المنخفض مع وجود الفرصة لارتكاب السلوك الطائش يعدان عاملين مؤثّرين في ارتكاب السلوك الطائش.	الضغوط العامة: تعد الضغوط العامة التي يتعرض لها المجتمع، من فقر وبطالة وأمية وظروف اقتصادية صعبة عوامل ضاغطة على المجتمع عامة وخاصة على قطاع الشباب.	التزابط الكوني: هناك عامل يمكن أن يساهم في دفع مستويات الجريمة هو ظهور التزابط العالمي في سياق تحولات العالم الاقتصادية والديمغرافية.
الضغوط العامة: تلعب العوامل الاجتماعيةوالاقتصادية دورا هاما في زيادة الجريمة الإلكترونية.	البحث عن الثراء: يلجأ بعض الناس إلى الجريمة الإلكترونية، حيث المستهدف مجتمع أكبر وسهولة التنفيذ وسرعة المردود وقلة الخطورة.	انكشاف البنية التحتية المعلوماتية الكونية: حيث تتفاوت البني التحتية المعلوماتية بدرجة انكشافها إلى الكوارث الطبيعية، والإهمال البشري، وسوء التصرف الإنساني. من الصعب ربط التهديدات الإلكترونية بمكان أو زمان، أو جماعة، فقد تصدر من هاو أو من طفل أو محترف، أو جماعة إرهابية، أو جماعة تنافسية، أو استخبارات أجنبية.
النشاط الروتيني: إن التغيرات في أنشطة الناس الروتينية، من استخدام النت وشبكات التفاعل الاجتماعي مثل الفيس بوك،	ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية: هناك الكثير من الدول التي لم تطور تشريعاتها وأجهزة العدالة فيها لكي تتمكن	

والإيميل والمواقع وغيرها، قد كونت فرصاً للجناة المتحفزين مع وجود أهداف قيمة وسهلة في الحيز الفضائي مع غياب الحراسة.	من مجاراة التقدم في الجرائم الإلكترونية وأساليبها.	

6.1. أنواع الجريمة الإلكترونية (المعلوماتية)

تصنف الجريمة الإلكترونية (المعلوماتية) إلى عدة أصناف فهناك من يصنفها تبعا لمرتكبها، وهناك الجرائم التي صنفت تبعا لطريقة تنفيذها، وأخرى تبعا لغرض أو هدف الاعتداء، ويمكن الإشارة إلى التصنيفات التالية:

- الجرائم الإلكترونية التقليدية: كالسرقة الإلكترونية مثل استنساخ برامج الحاسب الآلي والمتاجرة فيها، والانتحال ..الخ.
- الجرائم الإلكترونية الجديدة: كنشر الفيروسات الرقمية أو عمليات الاختراق لقواعد البيانات.
- الجرائم التي تستهدف النظام المعلوماتي: كجرائم الاختراق وجرائم إتلاف المعلومات.
- الجرائم المنفذة باستخدام النظام المعلوماتي: كجرائم التعدي على البيانات وانتهاك الخصوصية.
- الجرائم المنفذة في بيئة النظام المعلوماتي: كجرائم التشهير والجرائم الإباحية والأخلاقية، المواقع الإرهابية، التنصت والتجسس على أجهزة الحاسوب، قرصنة الكتب الورقية وتحويلها إلى نسخ رقمية وبيعها، الاحتيال للاستيلاء على الأموال من خلال البريد الإلكتروني(مصطفى وآخرون، 2011).
- الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (جرائم قرصنة البرمجيات): التي تشمل نسخ وتقليد البرامج وإعادة انتاجها وصنعها دون ترخيص، والاعتداء على العلامة التجارية وبراءة الاختراع (شعبان، 2009).

وهناك جرائم أخرى إلكترونية مثل:

- السطو على أرقام البطاقات الائتمانية، اختلاس من البنوك، تزوير وثائق ومستندات مالية.
- المقامرة غير الشرعية.
- التزوير، كجرائم تزوير التوقيع الإلكتروني.
- غسيل الأموال.
- نشر رسائل الكراهية.
- احتيال القروض.
- تجارة المخدرات.
- المطاردة الإلكترونية (ياسين، 2012).
- الابتزاز والتشهير وتشويه السمعة في المواقع الإلكترونية.
- تلقي البضائع المسروقة.

7.1. خصائص الجريمة الإلكترونية

تتّسم بسهولة الوقوع في فخها، حيث إنّ غياب الرقابة الأمنية تساهم في انتشارها وتسهيل ذلك. إن الضرر الناجم من الجريمة الإلكترونية غير قابل للقياس، إذ إنّها تخلق أضراراً جسيمة. فيما يلي مجموعة من خصائص الجريمة الإلكترونية والتي تؤدي إلى ارتكاب الجريمة الإلكترونية منها:

صعوبة الكشف عن مرتكب الجريمة إلا بأساليب أمنية وتقنية عالية.

سلوك خارج عن المألوف وغير أخلاقي مجتمعيّاً ذات عنف وجهد أقل من الجرائم التقليديّة.

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

سهولة إخفاء آثار الجريمة والأدلة التي تدلّ على الجاني، نظراً للترميز والتشفير الذي يحدث على الرموز المخزّنة على وسائط التخزين المغنطة.

سرعة التنفيذ، حيث لا يتطلب تنفيذ الجريمة الإلكترونية الوقت الكثير وبضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر. وهذا لا يعني أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة (البداينة، 2014).

التنفيذ عن بعد، حيث لا تتطلب الجريمة الإلكترونية في أغلبها (إلا جرائم سرقة معدات الحاسوب) وجود الفاعل في مكان الجريمة. بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن مكان الجريمة سواء كان من خلال الدخول للشبكة المعنية أو اعتراض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب .الخ.

إخفاء الجريمة، إن الجرائم التي تقع على الحاسبات الآلية أو بواسطتها (كجرائم الإنترنت) جرائم مخيفة، إلا أنه تلاحظ آثارها والتخمين بوقوعها.

الجاذبية، نظراً لما تمثله سوق المعلومات والحاسب والإنترنت من ثروة كبيرة للمجرمين أو للإجرام المنظم، فقد غدت أكثر جذباً لاستثمار الأموال وغسيلها 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...إلخ.

عابرة للحدود الدولية، حيث إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمراً ممكناً وشائعاً، لا يعترف بالحدود الإقليمية للدول، ولا بالمكان، ولا بالزمان، بل أصبحت ساحتها العالم أجمع.

8.1. سبل مكافحة الجريمة الإلكترونية

توجد سبل متنوعة لمكافحة الجريمة الإلكترونية، حيث تتباين هذه السبل بدرجة فاعليتها وتعقيدها، وذلك حسب البرامج المصممة لهذا الغرض. ومن بين هذه السبل:

عمل نسخ من ملفات البيانات Backups.

استخدام البرامج المضادة للفيروسات Anti–Virus software.

برامج جدران النار Firewalls software. نظام أو برنامج حماية تحجز البيانات بين الشبكة الداخلية والشبكة الخارجية، إي هو الجهاز الذي يتحكم في تدفق المعلومات بين جهاز الحاسوب والإنترنت، والهدف هو حجز كل ما هو غير مرغوب فيه من خارج البيئة المحمية. يستطيع المستخدم اذن الخروج الى عالم الإنترنت ولكن لا يستطيع من في الخارج الدخول الى الجهاز من خلاله.

استخدام الخصائص الفسيولوجية Biometrics, fingerprint لحماية النظام مثل بصمة الإبهام، حدقة العين، الصوت وغيرها.

التشفير Encryption.

وتستخدم معظم نظم المعلومات الإدارية الشبكية برامج جدران النار، والبرامج المضادة للفيروسات بالإضافة إلى التشفير Encryption لحماية الرسائل والملفات المخفية، وهناك تشفير باستخدام المفتاح العام Public Key Encryption المعروف اختصاراً باسم (PKE) وهو نظام تشفير يستخدم مفتاحين، مفتاح رئيس يمكن أن يستخدم أو أن يحصل عليه أي شخص ومفتاح خاص Private key للشخص المستلم فقط (ياسين، 2012).

9.1. نماذج من الجرائم الإلكترونية

بريد الكتروني يحتوي على ذم وقدح وتحقير: عبارة عن رسائل تحوي عبارات ذم وقدح وتحقير لأشخاص مستهدفين بذاتهم أو غير مستهدفين، قد يكون كتابياً أو غيابياً، أو بواسطة المطبوعات ترتكب عبر الإنترنت من خلال المبادلات الإلكترونية الكتابية أو الصوتية أو الفيديو.

سرقة بريد الكتروني: يعاني عدد كبير من مستخدمي الإنترنت في الفترة الأخيرة من سرقة عنوان بريدهم(حيت تم سرقة ما يقارب من 20 ألف بريد إلكتروني في سنة 2014)3، لذلك يجب التأكد من سلامة نظام التشغيل في الجهاز من الفيروسات وبرامج التروجان، حيث يعتبر من أكبر العوامل التي تهدد أمن البريد الإلكتروني وأي معلومات أخرى مخزنة في الجهاز. فالبريد الإلكتروني يشكل هوية L'identité للشخص في الفضاء الإلكتروني، خصوصاً وأنه يحتوي على اسم الشخص الحقيقي، في أغلب الحالات، ومهنته في حالات أخرى، وقد يشير عنوان البريد الإلكتروني فوق ذلك إلى بلد الشخص أو جنسيته، وغيرها من المعلومات الخاصة فإن الاعتداء عليه يشكل اعتداءً على الحياة الخاصة للشخص؛ فالهوية تدخل في نطاق الحياة الخاصة للشخص. إن أغلب التشريعات المعنية بالحياة الخاصة تعتبر عنوان البريد الإلكتروني للمستخدم معلومة من المعلومات الاسمية التي يجب المحافظة عليها ببقائها طي السرية والكتمان (Mallet, 2009: الزوي، 2017).

2. الجريمة الإلكترونية في المجتمع الليبي والتشريعات القانونية

1.2. الجرائم الإلكترونية (المعلوماتية)

تعددت الجرائم الإلكترونية في ليبيا وفق النظرة التي نظر من خلالها المختصين والباحثين بهذا المجال، والتي في الواقع تعاني منها أغلب البلدان بصفة عامة وفي ليبيا بشكل خاص، ومن هذه الجرائم :

- جريمة استنساخ برامج الحاسب الآلي والمتاجرة فيها، وتكون هذه الجريمة إما بنسخ البرامج من مواقع الشركات من أشخاص يعملون فيها ثم يقوم بوضعها في أقراص ممغنطة أو اسطوانات وبيعها، أو من برنامج متداول في السوق فيقوم الشخص بكسر حماية الملكية ويتم إنشاء نسخة منه ثم يبدأ بنسخه إلى نسخ متعددة وبيعه، وكذلك يمكن أن يقوم شخص بأخذ برامج من الإنترنت دون إذن من الشركة المنتجة، ويقوم بجمعها ثم نسخها على أقراص وبيعها في السوق بطرق غير مشروعة.
- تحميل برمجيات مضادة للفيروسات غير أصلية ومقرصنة من الإنترنت.
- قرصنة الأناشيد والأغاني والأفلام والحصص الوثائقية والدروس وإعادة نشرها عن طريق الاستنساخ على الأقراص المضغوطة.
- الدخول غير المصرح به لشبكة الإنترنت المتاحة بواسطة الماي فاي من منظمات تتسرب منها كلمات السر الممنوحة للموظفين فيها، مما يسمح لبعض المجرمين الإلكترونيين بالدخول إلى شبكة الإنترنت مجانا واستنساخ برامج بطرق غير مشروعة.
- التزوير والانتحال، حيث أنه مع تطور التكنولوجيا وظهور أنظمة الحاسبات الآلية بمختلف انواعها مثل، طابعات الليزر والماسحات المتقدمة وغيرها، قد ساهمت بشكل كبير في تسهيل تزوير البيانات والمعلومات التي تحتوي عليها هذه الأنظمة، كالبيانات المتعلقة بالميلاد والوفاة وجوازات السفر ورخص القيادة،...الخ.

2.2. التشريع الليبي في مجال الجرائم الإلكترونية (المعلوماتية)

في الواقع لا يوجد أي تشريع في ليبيا للوقاية من الجرائم الإلكترونية المتصلة بتكنولوجيا المعلومات والاتصال وأمن المعلومات، يوجد فقط مسودة قانون لمكافحة الجرائم الإلكترونية (المعلوماتية) تقدمت بها وزارة العدل لمجلس النواب لم يناقشها بعد ويصادق عليها.

بهذا، لم يظهر في القانون الليبي تشريع خاص يحدد الجرائم الإلكترونية أسوة بالتشريعات المقارنة، وإن كان لهذا النوع من الجرائم دلائل ظهرت في نصوص القانون رقم 3 لسنة 2014 الصادر عن مجلس النواب، كنص المادة الأولى في تحديد مفهوم الأموال، ونص المادة الثانية في تحديد العمل الإرهابي ونص المادة 15 والمادة 17 من قانون مكافحة الإرهاب4. لقد حان الوقت لتدخل المشرع الليبي لمكافحة الجرائم

[3] البنك المركزي الأوروبي، (7-2014).

[4] - مكالمة هاتفية مع الدكتورة الغزيز، نعيمة (2018)، أستاذ القانون العام المساعد، الجامعة المفتوحة، طرابلس، ليبيا.

الإلكترونية، وذلك بالنص على تجريم الاعتداء على المال المعلوماتي المعنوي سواء بالنص على كل جريمة على حده، أو أن يقرر التجريم بنص واحد، يشمل بالحماية الجنائية كل صور الاعتداء، السرقة أو الإتلاف أو غيرهما(المطردي، 2012).

3.2. إجراءات التحقيق في الجرائم الإلكترونية (المعلوماتية)

للتحقيق في الجرائم الإلكترونية يجب الإلمام والمعرفة الجيدة بمجال الحاسب الآلي والإنترنت، وكيفية الاستفادة من هذه المعرفة واستخدامها بكفاءة في التحقيق والتحري واستخلاص الأدلة، ثم معرفة ما يمكن استخدامه كدليل في المحكمة، وأخيراً معرفة الخطوات اللازمة لتجريم المشتبه به من الناحية القانونية. بالإضافة إلى ذلك لابد من توفر مجموعة من المتخصصين والمحققين لديهم معرفة وخبرة طويلة في مجال جرائم الحاسوب والإنترنت، وكيفية التعامل مع الأدلة الجنائية الرقمية، حيث يتولى عملية التفتيش عن الأدلة، خبير في الحاسوب والشبكات، وآخر في تدقيق الحسابات، وخبير في التصوير، والبصمات ثم خبير الرسم التخطيطي، وتساهم هذه الإجراءات جميعها في الوصول إلي الآتي:

- التأكد من وقوع الجريمة.
- تحديد نمط وطبيعة الجريمة المرتكبة.
- التعرف على التقنيات المستخدمة في ارتكابها.
- المساعدة في تحديد الجاني والجناة المحتملين أو المشتبه بهم.
- معرفة الأسباب والدوافع المحتملة لارتكاب الجريمة.
- الاستدلال على الشهود في حالة وجودهم.
- توضيح طبيعة الأدلة الجنائية ومصادرها.

ويحتاج فريق المحققين في الجرائم المعلوماتية إلى مجموعة من البرمجيات الخاصة بالتحقيق الجنائي منها: برمجيات النسخ الاحتياطي الجنائي، برمجيات استعادة الملفات المحذوفة، برمجيات كسر كلمات سر بعض المستندات، برمجيات تتبع الاتصال الشبكي، برمجيات استعراض الصور، برمجيات عرض محتوى المفلت المختلفة (امحمد، 2010).

أخيراً، فيما يلي بعض النصائح التقليدية لخبراء الحاسوب بمكافحة الجريمة الإلكترونية:

اجتناب استخدام أجهزة الحاسوب في الأماكن العامة، كالمقاهي والفنادق وغيرها إلا للضرورة.

ضرورة إقفال البريد الإلكتروني بعد الاستخدام، وتجاهل الرسائل الواردة التي لا تعرف مصدرها، ومسح المراسلات الصادرة والواردة التي لا تحتاج الرجوع إليها.

الحرص على تغيير كلمة السر باستمرار، وأن تكون مزيجاً من الحروف الصغيرة والكبيرة والأرقام والاشارات.

ضرورة أن تكون كلمة السر بعيدة عن معلوماتك الشخصية والعائلية مثل الاسم، تاريخ الميلاد، رقم الهاتف الخاص بك، أو عن الاسماء الشهيرة مثل الاعبين أو الشخصيات السياسية.

أن لا يكون بريدك الإلكتروني مكتوبا على بطاقتك التعريفية، فلا تسلم هذه البطاقة إلا لمن تعرف أنه لن يسيء استخدامها.

نقل نسخة من عناوين الأشخاص الذين تتواصل معهم إلى مكان آخر وتحديثها باستمرار.

النتائج :

تم في هذه الورقة البحثية دراسة أدبيات موضوع الجريمة الإلكترونية، وعرض نماذج من الجرائم الإلكترونية، وتم التوصل الى النتائج التالية:

1تُعتبر التشريعات والقوانين عاملاً مهماً في مواجهة الجريمة الإلكترونية (المعلوماتية) التي ترتكب في الفضاء الإلكتروني.

2. نقص الخبرة لدى العاملين في قطاع أمن المعلومات يتسبب في حدوث جرائم إلكترونية.
3. القصور في الاهتمام بالأجهزة الخاصة بالخبرة الجنائية الرقمية يُمكن فئات مجرمي المعلوماتية الذين يتمتعون بالمهارة والمعرفة والذكاء في ارتكاب الجرائم المعلوماتية.
4. قصور مؤسسات التعليم والمجتمع المدني في القيام بدورهم التوعوي والوقائي في مكافحة تلك الجرائم.
5. الاجهزة القضائية تنقصها الخبرة في مجال إعداد أنظمة ضبطية وقضائية مؤهلة في التعامل مع الجرائم الإلكترونية.
6. مكافحة الجرائم المعلوماتية في ليبيا مازالت بلا غطاء تشريعي يحددها ويجرم كافة صورها.
7. ضعف التعاون الدولي لمكافحة الجرائم الإلكترونية وخاصة بين الدول العربية.

التوصيات :

بعد هذه الفسحة والمقاربة التحليلية للوقوف على مفهوم الجريمة الإلكترونية في الفضاء الإلكتروني، وبناء على النتائج التي تم توصل إليها، يقترح الباحثان جُملة من التوصيات كخاتمة للدراسة، والتي من شأنها العمل على الحد من ظاهرة الجريمة الإلكترونية، ومن أهم هذه التوصيات ما يلي : 1. ضرورة تدخل المشرع القانوني لمواجهة الجريمة الإلكترونية (المعلوماتية) التي ترتكب في الفضاء الإلكتروني.
2. تأهيل وتدريب العاملين في قطاع أمن المعلومات في المنظمات المالية من أجل حماية المنظومة الإلكترونية، والتعامل باحتراف مع تكنولوجيا المعلومات والاتصالات.
3. تفعيل الأجهزة الخاصة بالخبرة الجنائية للجريمة الإلكترونية (المعلوماتية)، يتكون اعضاؤها من فريق متخصص فنياً في تقنية الاتصالات والمعلومات، لأن اثبات الجريمة الإلكترونية يتطلب قواعد خاصة للتعامل مع الأدلة في هذه الجرائم.
4. العمل على اعادة النظر في المناهج الدراسية بالجامعات، وضرورة تضمينها مادة عامة عن الحاسب الآلي والشبكات المعلوماتية وكيفية التعامل مع الأجهزة الإلكترونية. على سبيل المثال : يجب أن تتضمن كليات القانون قسما خاصاً لدراسة الجرائم الإلكترونية في مادة قانون العقوبات والمعاملات المالية الإلكترونية، والتجارة الإلكترونية، والصيرفة الإلكترونية، والحكومة الإلكترونية.
5. إعداد الملتقيات العلمية وورش العمل حول تقنية الاتصالات والمعلومات والقانون، والاهتمام بمؤسسات المجتمع المدني في برامج التوعية لمكافحة الجرائم الإلكترونية، وتخصيص دورات تدريبية للقضاة ورجال النيابة العامة لرفع مستوى الكفاءة لديهم في مجال استخدام تقنية الاتصالات والمعلومات.
6. الاهتمام باتفاقيات التعاون الدولية والاقليمية والعربية لمكافحة الجرائم الإلكترونية (كاتفاقية بوداست،2001)، والتنسيق فيما بينها لتعاون أجهزة الشرطة في تبادل البيانات والمعلومات اللازمة، والتصدي للاستخدامات غير المشروعة في المعاملات الإلكترونية وملاحقة المتهمين هذه الجرائم.

المراجع

امحمد، مولاي (2010)، "صعوبات تطبيق الإدارة الإلكترونية بالجزائر: الجريمة الإلكترونية نموذجا"، المؤتمر العالمي الأول للإدارة الإلكترونية، مركز المدينة للوسائط المتعددة، 01-2010/06/03، طرابلس، ليبيا.

البداينة، دياب موسى (2014)، "الجرائم الإلكترونية: المفهوم والأسباب"، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة من 02-2014/09/04، كلية العلوم الإستراتيجية، عمان، الأردن.

البشري، محمد الأمين (2008)، "الإنترنت والإرهاب: تأهيل المحققين في جرائم الحاسب الآلي وشبكات الإنترنت"، القاهرة: جامعة عين شمس.

حسني، محمود نجيب (1983)، "شرح قانون العقوبات - القسم العام"، ط6، دار النهضة العربية، القاهرة.

الزوي، ما شاء الله (2017)، "المواجهة الجناية للبريد الإلكتروني الدعائي المزعج أو المضلل"، المؤتمر الدولي الرابع عشر حول الجرائم الإلكترونية، مركز جيل البحث العلمي، 24- 25/مارس 2017، طرابلس، ليبيا.

السعيد، كامل (1983)، "شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن"، ط2، دار الفكر للنشر والتوزيع، عمان.

شعبان، سمير (2009)، "الجريمة الإلكترونية، مقاربة تحليلية لتحديد مفهوم الجريمة والمجرم"، الملتقى الدولي حول التنظيم القانوني للإنترنت والجريمة الإلكترونية خلال الفترة من 27-2009/04/28، جامعة الجلفة، الجزائر.

المايل، عبد السلام محمد (2017)، "مدى توفر متطلبات تطبيق الحكومة الإلكترونية في المنظمات المحلية بمدينة الخمس- دراسة ميدانية تحليلية لآراء عينة من العاملين بالمجلس البلدي بمدينة الخمس"، المؤتمر الاقتصادي الأول للاستثمار والتنمية في منطقة الخمس، المجلس البلدي بالخمس وبالتعاون مع جامعة المرقب، 25-2017/12/27، الخمس، ليبيا.

مصطفى سعدون، سلمان محمود، عبد الرحمن حسن (2011)، "الجريمة الإلكترونية عبر الانترنيت أثرها وسبل مواجهتها"، الكلية التقنية، كركوك، العراق.

المطردي، مفتاح بوبكر (2012)، "الجريمة الإلكترونية والتغلب على تحدياتها"، المؤتمر العلمي الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان، 23-2012/09/25، السودان.

ياسين، سعد غالب (2012)، "أساسيات نظم المعلومات الإدارية وتكنولوجيا المعلومات"، ط1، دار وائل للنشر والتوزيع، عمان.

الإسكوا (2012)، نشرة تكنولوجيا المعلومات والاتصالات للتنمية في المنطقة العربية، العدد (18) اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، الامم المتحدة، نيويورك.

Mallet-Poujol, N. (2009), “Protection de la vie privée et données á caractère personnel”, Université Motpellier1.

Westland, J.C., Clark, T. (2000), “Global electronic commerce: theory and case studies”, Cambridge, MA: MIT Press.