Revue des Réformes Economiques et Intégration En Economie Mondiale
Vol 14 N° 1 bis 2020
EISSN 2600- 6502

الأبعاد الاقتصادية للجريمة الإليكترونية

Economic dimensions of cybercrime

حورية قويقح [1*]
[1] جامعة الجزائر 1، الجزائر العاصمة (الجزائر)

تاريخ الاستلام : 2019/09/16 ؛ تاريخ المراجعة : 2020/01/10 ؛ تاريخ القبول : 2020/02/05

الملخص:

يعالج هذا المقال موضوعا حديثا نسبيا يتعلق بالجريمة الالكترونية وما مدي تأثيرها على الاقتصاد كلية خاصة في ظل التغيرات السريعة والمتلاحقة المترتبة على التقدم العلمي والتقني الذي تشهده الدول، وخاصة أنّ العالم الافتراضي أو ما يعرف بالوسيط الالكتروني اليوم أصبح يعتبر مجالا خصبا مؤثرا على الاقتصاد الوطني والدولي برمتيه. ولقد تم عرض أفكار هذا الموضوع بصفة تسلسلية وفق محاور رئيسية على النحو الآتي:

تناولنا ابتداء مفهوم الجريمة الاقتصادية الالكترونية، وتم طرح أهم خصائص هذه الجريمة المستحدثة تمييزا وتفصيلا لها عن الجريمة التقليدية، ثم ذكرنا أهم الانعكاسات الاقتصادية لها لنصل في الأخير لأهم العوامل المساعدة للحد من هذه الجريمة.

وتكمن أهمية هذه الدراسة كونها تناولت موضوعا سريعا ومتجددا، خاصة في ظل ارتفاع نسبة الجريمة الالكترونية فغزت ومازالت تغزوا العالم الافتراضي، أما عن حداثة الموضوع فتتمثل في أنّ جل الجرائم التقنية لم تكن معروفة من قبل وإنّما ظهرت في الفترة الأخيرة واستفحلت أكثر اليوم، كما تظهر أهمية هذا الموضوع كونه يبرز أهم الانعكاسات الاقتصادية لهذه الجرائم الالكترونية سواء على المستوى الفردي أم الجماعي.

الكلمات المفتاحية: الجريمة الاقتصادية، الجريمة الالكترونية، الشبكة المعلوماتية، الانعكاسات الاقتصادية.

تصنيف JEL: L81

Abstract

This article discusses a relatively recent topic on cybercrime and the extent of its impact on the economy, given the rapid and successive changes resulting from the scientific and technical progress observed by countries, such as the virtual world or what is called electronic media, is seen as fertile ground for the national and international economy as a whole. . The ideas of this subject have been presented in sequence according to the following main axes:

We started with the concept of electronic economic crime and the most important features of this new crime to distinguish and detail them from traditional crime, and then we talked about the most important economic impacts of this crime in order to reach the most important factors to help reduce this crime.

The importance of this study lies in the fact that it dealt with a fast-paced topic, especially in light of the high rate of cybercrime invading the virtual world, but the novelty of the topic is that most technical crimes were not known before, but appeared recently and are growing in number, it also shows the importance of this topic because it points out the most important economic repercussions of these cyber-crimes, whether at the individual or collective level, at the national or international level.

Keywords : economic crime, cybercrime, Information Network, economic repercussions

JEL classification : L81

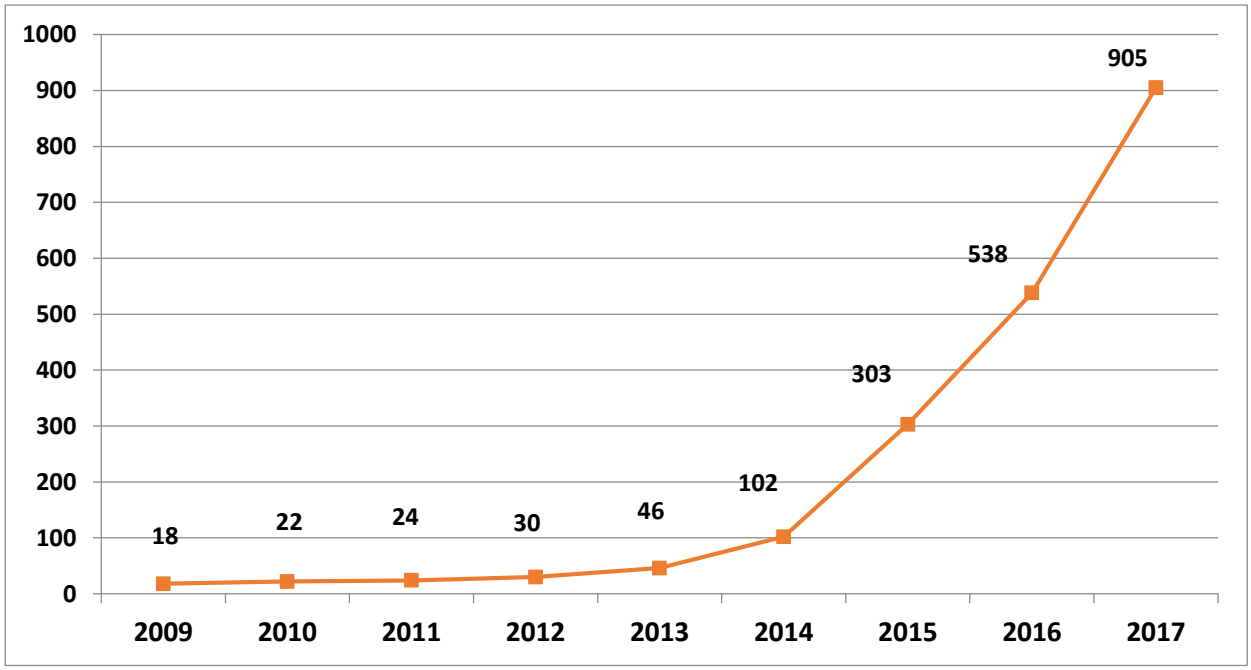
* حورية قويقح : h.gouigah86@gmail.com

مقدمة:

إنّ التطور التقني الذي شهده العالم كان له بالغ الأثر في ظهور واستفحال الجرائم الاقتصادية بكل أنواعها بما فيها الجرائم الاليكترونية ذات الانعكاسات والآثار الاقتصادية، إذ صارت أحد أكثر وأسرع أنواع الجرائم المستحدثة انتشارا على المستوى العالمي حسب احصائيات وبيانات دولية قدِّمت في هذا المجال، ولقد جرَّت معها هذه الجرائم بشكل تلقائي انعكاسات بعضها مسَّ الأموال وبعضها مسَّ الأشخاص وبعض منها مسّ الاقتصاد، إذ الجرائم المعلوماتية تتحدد أساليبها وتتنوع طرق ارتكابها خاصة في ظل ظهور التجارة الاليكترونية والتي تعتبر قيمة مضافة في مجال الفضاء الاليكتروني، وظهور ما يعرف بالتسويق الشبكي والذي يتمثل في تقديم برنامج تسويقي عبر الشبكة المعلوماتية من أجل القيام بعملية التسويق التي يحصل فيه المسوق على حوافز مالية نتيجة لبيعه المنتج أو الخدمة. وكذلك باتجاه الدول نحو نظام اقتصادي جديد يرتكز في أساسياته على اقتصاد السوق والتداول الالكتروني المتمثل في بيع وشراء لمنتجات مالية عبر الانترنت.

كما أنّ الوسائط الاليكترونية مثل التوقيع اليكتروني وشبكات الانترنت، والبطاقات الائتمانية وغيرها أدت إلى ظهور متغيرات جوهرية في السياسة الاقتصادية للدول، ولهذا أصبحت هذه الجرائم ذات مخاطر متعددة تلحق بالفرد والدولة ومؤسساتها خسائر باهظة، باعتبارها تستهدف معطيات الحاسوب المتمثلة في البيانات والمعلومات والبرامج بكل أنوعها.

ودليلا على التزايد السريع للجرائم المعلوماتية نذكر بعض الاحصائيات الواردة بشأنها على المستوى الوطني (الجزائر) فيما يلي:



عنوان الرسم البياني: تطور نشاط تحقيقات المعلوماتية بين 2009م و2017م [1] حوصلة نشاط مركز الوقاية من جرائم الإعلام الآلي وجرائم المعلوماتية ومكافحتها للدرك الوطني الجزائري، لسنة 2017م.

_ يمثل هذا الرقم ارتفاعا بنسبة 68.21 % بالنسبة لسنة 2017 مقارنة بنفس الفترة من سنة 2016م، ونخلص من الرسم البياني السابق إلى النتائج الآتية:

أولا: تصاعد عدد قضايا الجرائم المعلوماتية بوتيرة سريعة في السنوات الأخيرة مقارنة لها بما سبق.

. ففي سنة 2009م ضبطت وحدة الدرك الوطني بالجزائر العاصمة 18 قضية من إجمالي القضايا المضبوطة وذلك بنسبة 0,91 %.

. وفي سنة 2010 ضبطت وحدة الدرك الوطني بالجزائر العاصمة 22 قضية من إجمالي القضايا المضبوطة وذلك بنسبة 1,11 %.

. وفي سنة 2011 ضبطت وحدة الدرك الوطني بالجزائر العاصمة 24 قضية من إجمالي القضايا المضبوطة وذلك بنسبة 1,21 % .

. وفي سنة 2012 ضبطت وحدة الدرك الوطني بالجزائر العاصمة 30 قضية من إجمالي القضايا المضبوطة وذلك بنسبة 1,51 %.

. وفي سنة 2013 ضبطت وحدة الدرك الوطني بالجزائر العاصمة 46 قضية من إجمالي القضايا المضبوطة وذلك بنسبة 2,31 % .

. وفي سنة 2014 ضبطت وحدة الدرك الوطني بالجزائر العاصمة 102 قضية من إجمالي القضايا المضبوطة وذلك بنسبة 5,13 % .

. وفي سنة 2015 ضبطت وحدة الدرك الوطني بالجزائر العاصمة 303 قضية من إجمالي القضايا المضبوطة وذلك بنسبة 15,24 %.

. وفي سنة 2016 ضبطت وحدة الدرك الوطني بالجزائر العاصمة 538 قضية من إجمالي القضايا المضبوطة وذلك بنسبة 27,06 %.

. وفي سنة 2017 ضبطت وحدة الدرك الوطني بالجزائر العاصمة 905 قضية من إجمالي القضايا المضبوطة وذلك بنسبة 45,52 %.

ثانيا: ومن أبرز القضايا الاليكترونية والتي تصاعدت نسبتها خلال 2017م نجدها موزعة ومرتبة تنازليا على النحو الآتي:

1. مخالفة المساس بالأشخاص بنسبة 63,09 %.
2. مخالفة الغش في شهادة الباكالوريا بنسبة 10,17 %.
3. مخالفة المساس بأمن الدولة بنسبة 8,40 %.
4. مخالفة الإخلال بالنظام العام والمساس بمؤسسات الدولة بنسبة 6,19 %.
5. مخالفة الإرهاب بنسبة 3,76 %.
6. مخالفة الاحتيال بنسبة 2,54 %.
7. مخالفة استغلال الأحداث (القصر) بنسبة 2,21 %.
8. مخالفة المساس بأنظمة المعالجة الآلية للبيانات بنسبة 2,10 %.
9. مخالفة المساس بالممتلكات بنسبة 1,55 %.

هذه العوامل كلها ساعدت على ظهور جرائم اقتصادية ومالية وشخصية كان لها بالغ الأثر على الاقتصاد الوطني والدولي، الأمر الذي تطلب منّا طرح الإشكالية الآتية:

_ ما هي الانعكاسات الاقتصادية للجريمة الاليكترونية؟

والتي تتفرع من خلالها مجموعة أسئلة نوردها على النحو الآتي:

_ ما مفهوم الجريمة الاقتصادية الالكترونية؟

_ وما هي خصائص هذه الجريمة المستحدثة؟

_ وما هي الأساليب المقترحة لمكافحة هذه الجريمة؟

ولقد تم طرح جملة فرضيات تتعلق بموضوع البحث نذكرها فيما يلي:

_ للجرائم الاليكترونية انعكاسات متعددة منها ما يتعلق بالاقتصاد الوطني ومنها ما يتعلق بالاقتصاد الدولي.

_الجريمة الاليكترونية هي جريمة تحتاج الى تظافر جهود دولية ووطنية للحد من سرعتها وانتشارها.

_ الجريمة الاليكترونية تمس جهات متعددة على المستوى الوطني (البنوك، المؤسسات، الشركات، الأفراد).

وإجابةً عن الإشكالية المطروحة آنفا تناولنا الموضوع وفق التسلسل التقسيمي الآتي:

المحور الأول: مفهوم الجريمة الاقتصادية الاليكترونية

ذكرت عدة تعريفات للجريمة الاقتصادية تراوحت بين الضيق والتوسع نقتصر في ذلك على ما يلي: "هي كل سلوك إنساني فعلا كان أو امتناعا، يرتب أضرارا بمصلحة اقتصادية يحميها القانون، أو يمثل اعتداءً على الموارد الاقتصادية المملوكة أو التي يحوزها الأفراد والمؤسسات والدولة بما يترتب عليها ضررا."(2)

يعتبر هذا التعريف من بين أهم التعريفات المذكورة في هذا الشأن، كونه جاء جامعا ومانعا إذ اعتبر كل الجرائم المنصوص عليها في القانون المضرة بمصلحة اقتصادية هي من قبيل الجرائم الاقتصادية، أو مثّل الفعل اعتداء على الموارد الاقتصادية هي من هذا القبيل وإن كان مصدرها فردا أو مؤسسة أو دولة.

أمّا فيما يخص مفهوم الجريمة الاليكترونية فقد برزت الكثير من الجهود التشريعية والفقهية التي عنيت بتحديدها وتقريبها للأذهان وإن اختلفت التسميات المعبرة عنها، ومن بين أهم ما ذكر في الموضوع نقتصر على ما يلي:

_ عرفت هذه الجريمة وفقا لتعريف منظمة التعاون الاقتصادي والتنمية والخاصة باستبيان الغش المعلوماتي عام 1982م والذي أوردته بلجيكا في تقريرها بأنّها كل: "فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات."(3)

هذا التعريف اشتمل على مختلف أنواع الجرائم الالكترونية وذلك استنادا لعمومية الصياغة المذكورة؛ حيث اعتبر كل اعتداء مهما اختلفت نوعية الجريمة مادية أو معنوية، وسواء ارتكبت بطريق مباشر أم غير مباشر هي جريمة اليكترونية وذلك متى اتصلت واقترنت بتقنية المعلومات.

_ ومن بين التعريفات المذكورة في هذا الشأن أيضا: "أنّ الجريمة المعلوماتية هي نشاط إجرامي يتضمن اعتداء على الأفراد أو الممتلكات يرتكب باستخدام المنظومات المعلوماتية فيترتب عليه وصول غير مشروع _غير مرخص به_ إلى معلومات أو موارد تم تخزينها على المنظومات المعلوماتية، بهدف النسخ أو الإلغاء أو النقل أو التخريب أو التجسس أو العبث في هذه البيانات والمعلومات."(4)

واستخلاصا من كل ما سبق يمكن تحديد معنى الجريمة الاقتصادية الاليكترونية بأنّها: **"كل فعل غير مشروع متصل بالكيان المعنوي لجهاز الحاسب الآلي، ذو طبيعة اقتصادية مرتبا لآثار اقتصادية."**

المحور الثاني: خصائص الجريمة الاليكترونية وتمييزها عن الجريمة التقليدية

على العموم فإنَّ الجريمة الاليكترونية تنفرد بعدة خصائص تميزها وتفصلها عن غيرها من الجرائم، إلّا أنَّ هذه الخصائص تنقسم إلى ثلاثة أقسام؛ منها ما يقترن بالجريمة ذاتها ومنها ما يقترن بالمجرم المعلوماتي ومنها ما يتصل بالمجني عليه.

1_ الخصائص المتصلة بالجريمة الالكترونية:

. **الجريمة الإليكترونية هي جريمة ناعمة؛** حيث يقوم المجرم المعلوماتي بحذف البيانات أو المعلومات أو البرامج المخزنة في ذاكرة الحاسوب في هدوء تام، وينفذ ذلك من خلال نبضات إليكترونية غير ظاهرة ولا ملموسة.

وهذا ما يميز الجريمة المعلوماتية عن الجريمة التقليدية فإضافة إلى تضاعف معدل ارتكابها والزيادة في مقدار الخسائر الناجمة عنها، فإنّها تتميز أيضا بكونها ناعمة، فيمكن للجاني أن يخرب أو يفسد أو يتلف المعلومات من غير حركة أو بذل مجهود جسدي وإنما يقتصر فيها على مجهوده الذهني وقدراته التقنية ملتزما في جريمته بالهدوء والسكينة.

كما أنّ هذه الجريمة تتم من خلال نقل المعلومات والبيانات بواسطة النبضات الاليكترونية عبر الاثير، وعليه يتم النشاط الإجرامي المكون لهذه الجرائم ويملأ الفضاء والمحيط من دون أن نشعر به، ومما يزيد في هدوء هذه الجريمة ونعومتها أنّ المجرم المعلوماتي لا يعد كسائر المجرمين الآخرين؛ فالمجتمع لا ينظر إليه على أنّه مجرم بالمعنى المتعارف عليه كونه ينتمي إلى مستوى اجتماعي مرتفع نسبيا عن غيره من المجرمين.(5)

. **الجريمة الاليكترونية جريمة عابرة للحدود؛** إذ بإمكان الجاني أن يجلس في غرفته ويحاكي حاسوبه لأجل ارتكاب جرائم عابرة للقارات من غير تنقل ولا سفر فهي ذات طبيعة دولية متعدية للحدود والقارات. وبما أنّ شبكة الانترنت عابرة للحدود فإنّ الجرائم الناشئة عنها بالضرورة هي الأخرى ذات طابع دولي وأثرها يمس أكثر من دولة.

وأهم ما يميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، واكتسابها بذلك طبيعة دولية، فبعد ظهور شبكات المعلومات لم يعد هنالك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، إذ يتم تبادل كميات كبيرة من المعلومات يفصل بينها آلاف الأميال من خلال أنظمة تتمتع بها الحاسبات الآلية، وهذا أوصلنا إلى نتيجة مؤداها أنَّ أماكن متباعدة ومتعددة بين الدول تتأثر بالجريمة المعلوماتية في آن واحد.(6)

وعلى سبيل المثال فإنّه في جرائم البث والنشر الفيروسي قد يكون مرتكب الهجوم يحمل جنسية دولة ما، ويشن الهجوم الفيروسي من حواسيب موجودة في دولة أخرى، وتقع الآثار المدمرة لهذا الهجوم في دولة ثالثة.(7)

. **صعوبة اكتشاف أو إثبات أو متابعة الجريمة الاليكترونية؛** إذ عادة ما يتلاعب المجرم المعلوماتي بمعطيات الحاسوب (برامج، معلومات، بيانات) وذلك من خلال محوها أو تدميرها أو تعطيلها، ولا يكلفه ذلك سوى زرع فيروسات أو استخدام القنابل المنطقية أو غير ذلك لعرقلة وظيفة الحاسوب وشبكاته.

أما عن صعوبة اكتشافها أو إثباتها إنّما يعود ذلك إلى طابعها التقني الذي يتميز عادة بالكثير من التعقيد والتعسير، كما أنّ الجريمة المعلوماتية تعتريها الكثير من المشاكل القضائية ويصعب تحديد الدولة صاحبة الاختصاص القضائي كما يصعب أيضا تحديد الجهة القضائية المختصة بالملاحقة القضائية.

ومن خلال ما تم ذكره سلفا فيما يتعلق بخصائص الجريمة المعلوماتية عموما، والمتمثلة في خاصيتها الدولية وصعوبة اكتشافها وهدوئها ترتب عنه صعوبة في اثباتها، وهذه الصعوبة راجعة إلى عدد من الأسباب منها: أنّ هذه الجريمة لا تترك أثرا ماديا مرئيا أو ملموسا، ولعل ما يزيد في صعوبة اثبات هذه الجرائم نقص الخبرة الفنية والتقنية لدى القضاء، فهذه الجرائم لا بد لها من مضاعفة التأهيل لأفراد هذه الجهات في مجال التقنية الحديثة من حيث كيفية جمع الأدلة وإجراء التفتيش والملاحقة في بيئة النظام المعلوماتي، ومع ذلك كله فإنّ الجهود المبذولة في هذا المجال غير متناسبة وحجم خطورة هذه الجرائم، يضاف إلى ذلك أنّها جرائم لا تخلف وراءها أثرا ماديا.(8)

2_ الخصائص المتصلة بالمجرم المعلوماتي:

يعرّف المجرم المعلوماتي من الناحية الجنائية بأنّه: "ذلك الشخص الذي يمتلك مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسوب الاليكتروني والقادر على استخدام هذا التكتيك لاختراق "الكود" السري لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق استخدام الحاسوب نفسه."(9)

ويتميز المجرم المعلوماتي بالكثير من الصفات التي تجعل منه شخصا مؤهلا لارتكاب مثل هذه الجرائم وأهمها الذكاء والفطنة والمراوغة والاحتيال، لأن مثل هذه لجرائم لا يمكن ارتكابها من قبل الأشخاص العاديين.

ذلك أنّ الإجرام المعلوماتي هو إجرام الأذكياء إذ لا يمكن لشخص غبي أن يمارس الإجرام المعلوماتي، لأنّ المجرمين الأغبياء يستطيعون سرقة منزل أو سيارة لأنّه مجرم منخفض الذكاء في الكثير من الأحيان، على خلاف ذلك تماما فمن يستعين بالكمبيوتر من أجل سرقة مصرف أو شركة هو مجرم على درجة كبيرة من الذكاء بحيث يمكنه التغلب على كثير من المشكلات والعقبات الفنية التقنية التي تواجهه.(10)

3_ الخصائص المتصلة بالمجني عليه:

كما تتميز الجريمة المعلوماتية أيضا بصفات تختص بالمجني عليه معلوماتيا فقط، فمن حيث ردة فعل المجني عليه اتجاهها واتجاه مرتكبيها، إذ المجني عليه في هذه الجرائم نادرا ما يقوم بالإبلاغ عنها وذلك راجع لعدة أسباب منها: ما يتعلق بسمعة المؤسسة التي يمثلها والتي قد تتأثر إذا علم المتعاملين معها تعرض أنظمة المعلومات الخاصة بها إلى التلاعب.(11)

المحور الثالث: الانعكاسات الاقتصادية للجريمة الاليكترونية

الجرائم المعلوماتية مهما اختلف نوعها ومهما تزايد حجمها تمس النظام؛ أي قد تقع على النظام المعلوماتي أو تقع بواسطته سواء تم ذلك في مرحلة إدخال البيانات أم في مرحلة إخراجها أم في مرحلة جمع البيانات، إلا أنّ الأثر الاقتصادي المترتب عنها يختلف بحسب نوع الجريمة ونوع الأنظمة المعلوماتية أو بحسب أهمية البيانات المستهدفة. ولهذا تتنوع وتتفاوت الخسائر الاقتصادية الناجمة عن الجرائم المعلوماتية، وقد تكون هذه الخسائر مباشرة أو غير مباشرة، أي يكون ضررها اقتصادي مباشر يرتبط بقيمة التجهيزات والبرمجيات موضوع الجريمة، وهو أقلها من حيث الأثر وقد يرتبط بالأثر الاقتصادي الناجم عن توقف هذه المنظومات عن العمل مثلا: اختراق وتعطيل بمنظومة شركة الطيران رغم عدم وجود أثر مالي مباشر، إلا أنّ توقف المنظومة عن العمل تؤدي إلى خسائر تقدر بالآلاف الدولارات، أو تعطيل منظومة سوق الأوراق المالية لمدة دقائق قد ينجم عنه خسائر تقدر بعشرات الدولارات أيضا، أو سرقة الأموال الاليكترونية واستخدام الشبكة للاستيلاء على أموال الغير.

ولقد أُعطي نموذجا عن هذه الخسائر وذلك في الموقع الاليكتروني لهيئة الإمارات للهوية، بأنّ خسائر الامارات العربية المتحدة عام 2012م بلغ 420 مليون دولار بسبب الجرائم الاليكترونية بينما أشارت مصادر أجنبية إلى تكلفة الجرائم الاليكترونية في السعودية بلغت 2،6 مليار دولار في عام 2013م. بينما أظهرت احصائية أجريت حول الخسائر الناجمة عن الانترنت بأنّ الخسائر الاقتصادية المتعلقة بالضرر الحاصل عن البرمجيات بلغ 17،5 مليار دولار عام 2004م، وانخفض إلى 13،3 مليار عام 2006م.(12)

وعلى العموم فإنّ الجريمة الاليكترونية حصل الاتفاق بشأنها على أنّها جريمة اقتصادية، إلا أّن ما يترتب عليها من خسائر ترتفع وتتضاعف إذ ما قورنت بغيرها من الجرائم خاصة منها التقليدية، فعلى سبيل المثال كانت الخسارة الناجمة عن 8000 حالة سرقة بالإكراه في فرنسا عام 1986م حوالي 561 مليونا من الفرنكات في حين يتضاعف هذا الرقم في حالة الجرائم المعلوماتية على الرغم من انخفاضها بنسبة ثمانية مرات حالة السرقة بالإكراه. وفي الولايات المتحدة الأمريكية توصل مكتب التحقيقات الفيدرالية "FBI" إلى أنَّ متوسط الخسائر التي تحققها الجريمة المعلوماتية حوالي 500000 دولار، في حين لا تزيد الخسائر التي تكلفها جرائم السرقة العادية عن 3500 دولار.(13)

وتتضاعف خطورة وانعكاسات وتأثيرات هذه الجرائم المعلوماتية يوما بعد يوم كونها تمس الفرد، كما تمس الشركات الخاصة والعامة أيضا، ناهيك عن خطورتها على البلدان من الناحية الاقتصادية بأبعادها الفردية والبنكية والمؤسساتية وغير ذلك كما يتبيّن لنا من خلال العناصر المتأتية:

3. 1_ التأثير الاقتصادي للجريمة الاليكترونية على المستوى الفردي:

الجريمة الاقتصادية المستحدثة مست كل فئات المجتمع إذ لم تختص بجهة دون أخرى، فأثرت على الأفراد والجماعات وأثرت على المؤسسات والشركات، وكل ذلك راجع إلى الوسيلة المستعملة في مثل هذه الجرائم والمتمثلة أساسا في شبكة المعلومات، هذه الشبكة هي التي يسرت وسهلت ونوعت من ارتكاب الجريمة وأصبحت تمارس بطرق أسرع وأسهل وبآثار أضعف، فأثرت على الفرد باعتباره المحرك الأساس في كل الجرائم.

ذلك أنّ الفرد اليوم أصبح ينجز تعاملاته ويدير كل أعماله وبحوثه ويتواصل مع العالم الخارجي بواسطة استخدام الانترنت، ولهذا فهو عرضة لمجموع من الجرائم الاليكترونية والتي تؤثر على الجانب المادي والمالي والاقتصادي لديه ومن أهم هذه الجرائم:

. سرقة الهوية الشخصية.

. سرقة بطاقات الائتمان الخاصة به.

. الابتزاز والتهديد.

. عمليات احتيال.

. تحويل أو نقل حسابه المصرفي.

. نقل ملكية الأسهم. (14)

3. 2_ التأثير الاقتصادي للجريمة الاليكترونية على مستوى الشركات والمؤسسات:

كما أنّ الشركات هي الأخرى تتأثر بصفة كبيرة بالجرائم الاليكترونية، وتتم هذه الجرائم من قبل جناة موظفي الشركة نفسها أو من قبل جناة غرباء عن الشركة، إلّا أنّ الخسائر التي تطالها من خلال عمليات الاختراق والقرصنة تتزايد وتتضاعف يوم بعد يوم وذلك نتيجة لتزايد عدد المستخدمين للشبكة المعلوماتية.

إلّا أنّ أكثر نتائج هذه الجرائم تستهدف القطاع المالي والاقتصادي، إذ أجريت دراسة بشأن الجرائم المعلوماتية في المملكة المتحدة، تبيّن من خلال نتائج هذه الجرائم أنّ أكثرها تستهدف القطاع المالي، فأغلب هذه الجرائم تخص البنوك وشركات التأمين في قطاعها ونسب أقل في القطاع العام والتعليمي.(15)

إذ تعد الجريمة الاليكترونية أحد أبرز التحديات الأمنية التي تواجهها الشركات والحكومات على المستوى العالمي وباتت تشكل خطرا حقيقيا يواجه الجميع وخصوصا من الناحية الاقتصادية، حيث تخلف وراءها خسائر كبرى بمعدل وسطي يتجاوز النصف مليون دولار أمريكي للشركات الكبرى جراء كل هجمة اليكترونية أو عملية اختراق تتعرض لها الشركة.(16)

ومعدلات الجريمة الاليكترونية في الشرق الأوسط: "وفقا لنتائج إحصاءات شبكة كاسبر سكي لأمن المعلومات، التي صدرت عن الربع الأول لعام 2016م، فقد ارتفع إجمالي عدد حالات الاختراق الاليكتروني المكتشفة من قبل منتجات كاسبر سكي لاب، في الشرق الأوسط بنسبة 15% عما كان عليه في الفترة ذاتها عام 2015م. على سبيل المثال، شهدت هجمات الفدية الخبيثة التي تمكنت برامج كاسبر سكي لاب من اكتشافها ومنعها في الشرق الأوسط ارتفاعا بنسبة 67%.

وتأتي المؤسسات المالية والمؤسسات التجارية الاليكترونية والاتصالات والمؤسسات الحكومية في طليعة المؤسسات التي تُستهدف من قبل القراصنة الاليكترونية على مستوى المنطقة والعالم، وإلى جانب الأعداد المتزايدة للهجمات المذكورة تقوم كاسبر سكي لاب كل يوم باكتشاف ومنع 310 آلاف ملف خبيث جديد بشكل تلقائي، وهناك أيضا تحدي الهجمات المعقدة والتي من الممكن أن يكون تداعيات خطيرة على الناس إذا ما نجحت في تسجيل اختراق ما لإحدى برامج مؤسسة والشركة التي تعمل في قطاع ما، في الوقت التي تعد فيه الشركات الصغيرة هدفا رئيسيا للبرمجيات."(17)

ومن الجرائم التي تتعرض لها الشركات ذات الأثر المادي والمالي والاقتصادي نتوقف على ما يلي:

. الاطلاع على معلومات سرية لصفقة أو مناقصة أو أمور تسويقية خاصة والاستفادة منها.

. العبث بمخازن المعلومات الخاصة بالشركة بحذفها أو تعديلها أو تعطيل الوصول اليها.

. سرقة الأموال أو تحويل الحسابات المصرفية الخاصة بالشركة.

. الغش في المعاملات الاليكترونية كالتغيير في المبيعات.

. عمليات الاحتيال.

. التهديد والابتزاز.

. اختراق الموقع الاليكتروني الخاص بالشركة.(18)

3.3_ التأثير الاقتصادي للجريمة الاليكترونية على مستوى البنوك:

انتقلت العمليات المصرفية من البنوك التقليدية إلى البنوك الاليكترونية وذلك لما لهذه الأخيرة من مميزات تزيد في قيمتها التنافسية بسبب ما توفره من وقت وجهد وربح سواء للعملاء أم للبنك نفسه، إذ الانترنت ساعد على تسهيل وتسويق الخدمات البنكية وسهل العمل مع عملائه وتقديم الخدمات للزبائن. إلا أنّ هذه البنوك تعد الهدف الأخطر الذي يستهدف الجرائم الاليكترونية كونها تعتمد على أنظمة التمويل اليكترونيا "EFT" فبنوك نيويورك وحدها تتناقل 200 بليون دولار يوميا، ولنا أن نتصور حجم الخسائر التي ستكون عليها هذه البنوك فيما لو وصلت إليها أيدي مجرمي المعلوماتية في حالة تمكنهم من فك رموز التحويل الاليكتروني للأموال.(19)

كما أنّ التوسع الكبير في إجراء المعاملات البنكية عبر شبكات المعلومات الدولية أدى إلى إعطاء بعد دولي لجرائم الاحتيال بصفة خاصة؛ فربط وسائل الاتصالات بالحاسبات الآلية يضاعف من المعاملات المالية الدولية التي تتم بوسائل من خلال التحول اليكتروني للأموال " Electronic Funds Transfer"، والتبادل الاليكتروني للمعلومات "Electronic Data Interchange". ولا يقتصر الأمر على المعاملات المالية فقط، بل إنّ الطبيعة الدولية للجريمة المعلوماتية تظهر في أنماط أخرى من السلوك، فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الحاسب الآلي الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصا آخر موجود في بلد ثالث. وكذلك فيما يتعلق بالإتلاف المعلوماتي، فإعداد أحد البرامج الخبيثة (الفيروسات) يمكن أن يحدث في دولة ما، ثم يتم نسخ هذا البرنامج آلاف المرات ويرسل إلى دول متفرقة من العالم.(20)

وأصبح الهاكرز يجمعون آلاف وملايين الدولارات عن طريق البنوك، ويعتمد الهاكرز في جمع المال من البنوك عن طريق اختراق قاعدة البيانات الخاصة وسحب جميع بيانات ومعلومات الخاصة بالمستخدمين بطاقات ائتمانية (ايميلات).

كما أنّ هناك أيضا اختراق الأنظمة الخاصة بالصرفات الآلية الخاصة بالبنوك أو خداع أحد الموظفين بالبنك للحصول على معلومات مهمة عن البنك وعملائه ويستخدمها ضدهم.(21)

خاصة وأنّ الأعمال البنكية الكلاسيكية من تقديم عمليات مصرفية إلى العملاء والزبائن بالطرق التقليدية لم تعد تتماشى والتطور الاقتصادي الحالي، لذلك دخلت عملية التحديث إلى الأجسام المصرفية العالمية لتصبح تلك البنوك تقوم بالعمليات المصرفية الحديثة التي سيطرت عليها العمليات الاليكترونية عبر موقعها الاليكتروني الموجود في شبكة الانترنت.(22)

والجرائم الاليكترونية التي قد تتعرض لها البنوك والتي تؤثر على الجانب المادي والاقتصادي لديها هي:

". السطو الاليكتروني.

. العبث بمخازن المعلومات الخاصة بالبنك بحذفها أو تعديلها أو تعطيل الوصول إليها.

. سرقة الاموال وتحويل حسابات مصرفية الخاصة بالمنظمة أو المؤسسة.

. عمليات الاحتيال.

. الابتزاز أو التهديد.

. اختراق الموقع الاليكتروني الخاص بالمنظمة أو المؤسسة."(23)

المحور الرابع: الجهود الدولية لمكافحة الجرائم المعلوماتية

لا بد أن يكون ثمة عمل دولي وإقليمي ووطني بشأن سياسة مكافحة الجرائم المعلوماتية عموما والجرائم المعلوماتية ذات الطابع الاقتصادي على وجه التخصيص والتحديد، إذ يستوجب علينا ابتداء أخذ الكثير من التدابير التشريعية والفقهية من أجل الحد أو التخفيف من هذه الجرائم، وبالتالي التخفيف من الانعكاسات الناجمة عنها ومن أهم هذه الآليات في مجال المكافحة نذكر ما يلي:

4. 1_ القيام بمجموع عمليات إجرائية تقنية للأنظمة المعلوماتية:

أول خطوة يجب أن تتخذ في مجال حماية الأنظمة المعلوماتية أو أنظمة الكمبيوتر من الجرائم، لا بد من القيام بعمليات إجرائية وفنية وتقنية لهذه الأنظمة حتى يمكن حمايتها ابتداء، هذه العمليات تخول لذوي الاختصاص في مجال المعلوماتية والتقنية المستحدثة ومن بين هذه الاجراءات نذكر ما يلي:

_ لا بد من أخذ الكثير من الحيطة والحذر فمثلا عند إنشاء بريد اليكتروني لا بد من ربطه ببريد اليكتروني آخر، أو برقم الهاتف، وعند محاولة اختراقه سيتم تسليم رسالة نصية قصيرة لعملية الاختراق. أمّا فيما يتعلق بالهواتف الذكية، يجب عدم تحميل الصور عليها والانتباه عند الدخول على موقع آبل ستور أو غوغل بلاي، وخاصة فيما يتعلق بخاصية التنسيق التلقائي والتي تنتج مشاركة الضرر مع الآخرين. (24)

_ ومن جانبه يؤكد الدكتور السيد بخيت أستاذ الاتصال بجامعة زايد: "على ضرورة رفع ثقافة مستخدمي التكنولوجيات الحديثة من أجهز وبرامج تعد خطرة لتلاقي الأخطار الناجمة من استخدام التكنولوجيا والعمل على زيادة وعي المستخدمين بمخاطر عدم المعرفة الجديدة بالتعاطي مع الانترنت، وتعريفهم بالطرق التي يستخدمها البعض للإساءة للآخرين واستغلالهم عبر الوسائط التكنولوجية، والعمل على تعلم كيفية استخدام بعض البرامج التي تساعد في حماية المستخدمين من الاستغلال السيء للتكنولوجيا وإقامة دورات وورش عمل تهدف إلى نشر الوعي لمستخدمي تلك الأجهزة التي أصبحت جزءا من حياتنا اليومية."(25)

_ إضافة إلى ذلك يستوجب استخدام البرامج الأصلية من المورد الرئيسي للبرامج وعدم استعمال البرامج مكسورة الحماية لأنّها سهلة الاختراق ولأنّ تلك البرامج غير موثقة، واستخدام برامج حماية ذات معدل مرتفع من جهات معلومة المصدر حتى ولو كانت أغلى ثمنا.(26)

_ كما أنّه ينبغي تنظيم المواقع وتنظيم محتواها وذلك راجع لتزايد المواقع التجارية على شبكة الانترنت، وظهور ونمو التجارة الاليكترونية وقيام المنافسات غير المشروعة، كما يستوجب حماية المواقع الأصلية على الشبكة من التقليد أو المنافسة غير المشروعة، بالإضافة إلى حماية الاسم التجاري والعلامة التجارية، وتنظيم آلية الدفع الاليكتروني تجنبا لجرائم السرقة أو الاحتيال أو ما يعرف بالغش المعلوماتي وهي من الجرائم المستفحلة في هذا المجال، وبالتالي تستقر المعاملات ويتم الشعور بالثقة والأمان فإساءة استخدام هذه المواقع تؤثر سلبا من الناحية الاقتصادية على حجم التجارة الاليكترونية والمبادلات التجارية الاليكترونية، بما يؤدي إلى ضياع الحقوق وانتهاكها.(27)

_ ويجب تدريب العاملين في المباحث الجنائية على تفحص الأدلة الاليكترونية، وضرورة تدريس المحققين على القيام بالكشف عما تحتويه أجهزة الكمبيوتر من برامج مخزنة عند الضرورة مما ييسر عمليات التفتيش التي تتم على كمبيوتر المتهم. وأنّه يستلزم الاستعانة بخبراء في الكمبيوتر والشبكات أثناء عمليات التقصي والتحقيق في الجرائم المعلوماتية والانترنت.(28)

4. 2_ القيام ببعض العمليات الشرطية والضبطية والتفتيشية ضد جرائم الانترنت:

الجرائم المعلوماتية تتميز بصعوبة اكتشافها ومتابعتها وضبطها وجمع الاستدلالات، وذلك راجع للطبيعة المعنوية التي تختص بها وانتقال الجرائم من الصورة المادية الملموسة إلى صورة معنوية غير ملموسة، هذه الخاصية هي التي أضفت طابعا خاصا على هذه الجرائم، ولذلك استدعى الأمر زيادة العمل التكويني للعاملين في هذا المجال، نذكر بعضا من ذلك فيما يلي:

_ استنادا إلى المثل القائل فاقد الشيء لا يعطيه فإنّه من المستحيل على أعضاء الضبطية العادية أن يقوموا بعمليات البحث والتحري في الجرائم الاليكترونية، كما أنّه يتعسر عليهم التعامل مع مرتكبيها، ولهذا لا بد من إيجاد أجهزة مختصة بهذا النوع من الإجرام، أو على العمل على تنمية خبرة ومهارات الأشخاص المخول لهم البحث والتحري فيها، وكذا وضع مناهج مدروسة لتدريس على التحقيق واثبات هذا النوع من الجرائم مراعين في ذلك خصوصية التطور التقني التشريع في مجال الاتصال.(29)

_كما أنّه ينبغي تعقب مجرمي المعلوماتية عامة وشبكة الانترنت خاصة، وتعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية، وشبكات الاتصال بحثا عن ما قد تحويه من أدلة وبراهين على ارتكاب الجريمة المعلوماتية، كلها أمور تستدعي القيام ببعض العمليات الشرطية والفنية والأمنية المشتركة، وهي من شأنها صقل مهارات القائمين على مكافحة تلك الجرائم، وبالتالي وضع حد لها.(30)

4. 3_ الزامية التعاون الدولي لمواجهة الجريمة المعلوماتية:

وذلك من خلال القيام بالكثير من المجهودات في هذا المجال خاصة وأنّ هذه الجريمة ذات ميزة عالمية عابرة للحدود والدول، هذه الخاصية تجعل الجريمة المعلوماتية جريمة متعددة الأعضاء _كما سبق وأن بيناه_، فقد ترتكب في بلد من قبل مجرم في بلد آخر ضد طرف مجني عليه في بلد ثالث، هذه الخصوصية جعلت الزامية تقديم المساعدة الدولية حاضرة وضرورية في المجال الاجرامي المعلوماتي وهذه المساعدة تأخذ عدة صور نذكر منها ما يلي:

_ تسلم المجرمين؛ والذي يقصد به:"قيام دولة ما (الدولة المطلوب منها التسليم) بتسليم شخصا موجودا في إقليمها إلى دولة أخرى (الدولة طالبة التسليم) بناء على طلبها بغرض محاكمته عن جريمة نسبت إليه ارتكابها أو لتنفيذ حكم صادر ضده من محاكمها. بمعنى آخر تسليم دولة لدولة أخرى شخصيا منسوبا إليه اقتراف جريمة ما أو صدر ضده حكما بالعقاب كي تتولى محاكمته أو تنفيذ العقاب عليه."(31)

_ تقديم المساعدة القضائية في مجال الأنظمة المعلوماتية؛ وتتمثل في الاجراءات القضائية التي تتخذها الدول والتي من شأنها تسهيل محاكمة الجناة في دولة أخرى، وتتخذ المساعدة القضائية في المجال الجنائي صور عدة منها: تبادل المعلومات، نقل الإجراءات، الإنابة القضائية الدولية.

ونضرب في هذا المقام مثالا عن أهم الدول العربية الرائدة في مجال المكافحة، إذ هناك الكثير من الجهود المبذولة في هذا المجال للحد من هذه الجرائم ولعل أهمها في الدول العربية ما بذل من قبل المملكة العربية السعودية وسبب ذلك راجع إلى تنامي استعمال الشبكة المعلوماتية واشراكها في مختلف الجوانب

الحياتية والعملية للفرد وللمؤسسات، ووفق علاقة طردية ظهرت جرائم بالحجم الموازي لهذا الاشراك جاء مصاحبا للاحتكاك بالمجال الرقمي للفرد السعودي في مختلف مؤسسات الدولة ولذلك اتخذت للتقليل من هذه الجرائم جهود متعددة في المجال نذكر ما يلي:

_ الحماية التقنية للمعلومات؛ وقد تعددت أوجه هذه الحماية واتخذت لذلك ثلاثة جوانب:

أولا: حماية تقنية من خلال اجراءات تتعلق بحماية النظام المعلوماتي بطرق فنية.

ثانيا: حماية نظامية من خلال أنظمة غير جنائية هدفها المحافظة على المعلومات وإقرار عقوبات معينة في حالة الاعتداء عليها.

ثالثا: حماية جنائية من خلال نظام جنائي حدد التجريم والعقاب وفق السياسة الجنائية للمملكة العربية السعودية، التي تعتمد على الشريعة الإسلامية مصدرا رئيسيا، والأنظمة التي تصدرها السلطة التنظيمية في ضوء أحكامها.(32)

_ الحماية النظامية للمعلومات؛ يقصد بالحماية النظامية هنا النصوص الواردة في الأنظمة السعودية غير الجنائية، التي تعنى بموضوعات محددة ولها علاقة بالنظام المعلوماتي، وتهدف هذه الأنظمة بشكل رئيس إلى:

أولا: المشاركة في تنظيم المجتمع المعلوماتي.

ثانيا: حماية البنية الأساسية للنظام المعلوماتي بشكل عام.

ثالثا: كفالة الاستفادة الفعلية من المعلومات والمعرفة.

رابعا: محاولة ملء الفراغ التشريعي قبل صدور نظام مكافحة جرائم المعلوماتية.

خامسا: تحديد السياسات والإجراءات التي تحكم مختلف أو جه النشاط المتعلق بتقنية المعلومات.

سادسا: ايضاح اهتمام المملكة بتقنية المعلومات ومواجهة المخاطر التي تواجه استخدامه.(33)

خاتمة:

من خلال ما تم عرضه حول الآثار الاقتصادية المتأتية عن الجرائم الاليكترونية، اتضح لنا حجم هذه الخسائر وزيادة ارتفاعها يوما بعد يوم، وتأثيرها على كل المجالات الحياتية بدءا من الفرد ثم المؤسسات والشركات ووصولا إلى الدول، وسبب ذلك عائد على دخول النظام المعلوماتي في كل ميادين الحياة العملية والعادية اليوم فأصبح صديق الصغير والكبير الفرد والجماعة، ولهذا بقدر ما كان له من تأثير إجابي في التنمية الاقتصادية وتسهيل العمليات المصرفية والبنكية بقدر ما كان له تأثير معاكس ومغاير، وذلك لعدم مسايرة هذا التطور بمجموعة من تشريعات تنظمه وتحدد مساره فخرج بذلك عن المألوف والمشروع، ولهذا السبب نحاول في خاتمة بحثنا عرض أهم النتائج والتوصيات التي أفصحت عنها الدراسة مسردين ذلك في شكل نقاط على النحو الآتي:

النتائج:

_ يتميز الاجرام المعلوماتي الاقتصادي عن الاجرام التقليدي بأنّه لا يحتاج إلى عنف وإنّما اجرام تقني ناعم، ويقوم فيه الجاني بالمعالجة الفنية الهادئة للمعطيات الاليكترونية.

_ وما يميز أيضا الجريمة المعلوماتية الاقتصادية عن الجريمة التقليدية أنّها كثيرا ما تتجاوز حدود الدول وذلك تماشيا مع خاصية الشبكة المعلوماتية، فهي ذات خاصية عالمية إذ يمكن أن يقوم الجاني باختراق أنظمة المعلومات من بنك فرنسي من قبل شخص جزائري مقيم في إيطاليا.

_كما تتميز الإحصائيات المتعلقة بالجرائم الاقتصادية المرتكبة عبر الشبكة المعلوماتية، بأنّها غير دقيقة وذلك محاولة من الشركات والمؤسسات إخفاء ذلك، وسببه راجع إلى المحافظة على ثقة الجمهور من جهة ولعدم الإبلاغ عنها من قبل الأفراد من جهة أخرى، ومع ذلك فإنّ الاحصائيات الواردة لدينا تؤكد تزايدها المستمر والسريع، وذلك لنقص التشريعات المتعلقة بها ونقص المختصين في مجال المتابعة والبحث والتحري، وقلة الجهات القضائية المعنية بالفصل في هذه الجرائم الاقتصادية الاليكترونية.

_ وتعتبر الجرائم المعلوماتية من أخطر وأكثر تحديات العصر وهذا مساير وموافق للفرضية المطروحة سابقا، ولذلك لا بد من مواجهتها بجهود تشريعية صارمة وسريعة وإنزال العقاب بمرتكبيها، وتكثيف الجهود لسن النصوص القانونية ذات الطبيعة الاقتصادية الالكترونية وأخذ دورها التام في التشريعات الوطنية والدولية. وخاصة أنّ الإجراءات الجنائية المتخذة لمتابعة مثل هذه الجرائم تثير الكثير من المشكلات القانونية في كل مرحلة بدءا بمرحلة جمع الاستدلالات والأدلة.

التوصيات:

_ لا بد أن تكون القواعد القانونية المتعلقة بالجرائم الاقتصادية الاليكترونية سريعة التغيير حتى تتماشى والسياسة الاقتصادية.

_كما أنّه يستوجب فرض رقابة خاصة ذات طبيعة حديثة على المصارف خاصة عندما أصبح السطو على البنوك يتم الكترونيا، إذ يقوم الجاني بتحويل أرصدة من حساب لآخر ومن دولة لأخرى.

_ ولا بد من تكوين جهة مختصة من خلال إنشاء ضبطية أو هيئة تختص بالتحري والتحقيق في مثل هذه الجرائم وتتميز هذه الهيئة بالقدرة الفنية والتقنية لمواجهة هذه الجرائم التكنولوجية، وتعزيز التعاون الدولي والثنائي والوطني في جانبيه الإجرائي التقني، وأن يأخذ التعاون صورتين، الأول سن التشريعات المتماشية مع هذه الجرائم والثاني عقد اتفاقيات ومعاهدات لمواجهتها.

المراجع:

(1)_ **حوصلة نشاط مركز الوقاية من جرائم الإعلام الآلي وجرائم المعلوماتية ومكافحتها للدرك الوطني الجزائري، لسنة** 2017م.

(2)_ عبد الله الصعيدي، **الجريمة الاقتصادية، المفهوم والأنواع**، دورية الفكر، شرطة الشارقة، (العدد 15)، ص 135.

(3)_ يوسف حسن يوسف، 2011م، **الجرائم الدولية للأنترنت**، (ط1)، القاهرة، الإصدارات القانونية، ص14.

(4)_ اتحاد المصارف العربية، يوليو 2019م، **تكاثف الجهود العربية لمكافحة الجريمة الاليكترونية وجرائم المعلوماتية وأثرها على العمليات المالية**، مجلة الاتحاد، (العدد 464)، ص 2 مأخوذ من عنوان موقع انترنت :
http://www.uabonline.org/ar/magazine/158315851575158715751578/157816031575157816011575160
4158016071608/11865

(5)_ عمار عباس الحسيني،2017م، **جرائم الحاسوب والانترنت**، (ط1)، بيروت_ لبنان، منشورات زين الحقوقية، ص 51.

(6)_ نائلة قورة، 2005م، **جرائم الحاسب الآلي الاقتصادية**، (ط1)، بيروت_ لبنان، منشورات الحلبي الحقوقية، ص 56.

(7)_ حسين بن سعيد بن سيف الغافري، 2007م، **الجهود الدولية في مواجهة جرائم الانترنت**، دكتوراه في القانون الجنائي، ص6.

(8)_ عبد الفتاح بيومي حجازي، 2002م، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت دار الكتب القانونية**، مصر، ص28، 29.

(9)_ هدى حامد قشقوش، 1992م، **جرائم الحاسب الاليكتروني في التشريع المقارن**، القاهرة، ص32.

(10)_ عمار عباس الحسيني، مرجع سابق، ص61.

(11)_ نائلة قورة، مرجع سابق، ص 51.

(12)_ اتحاد المصارف العربية، مرجع سابق، ص2، 3.

(13)_ نائلة فريد قورة، مرجع سابق، ص50.

(14)_ منى شاكر فراج العسبلي، **زيادة الفواتير بتحويل فواتير المجرم للضحية**، ص3، مأخوذ من عنوان موقع الانترنت:
http://kenanaonline.com/users/ahmedkordy/posts/320920

(15)_ محمد سامي الشوا، 2003، **ثورة المعلومات وانعكاساتها على قانون العقوبات**، القاهرة، الهيئة المصرية العامة للكتاب، ص35.

(16)_ محمد أمين حاسبيني، **ما هو أثر الجريمة الاليكترونية على اقتصاد الدول**، ص1، مأخوذ من عنوان موقع الانترنت:
https://saneoualhadath.me/التقنية/ماهو-أثر-الجريمة-الإلكترونية-على-اقتص#slide-1

(17)_ محمد أمين حاسبيني، مرجع سابق، ص1، 2.

(18)_ منى شاكر فراج العسبلي، مرجع سابق، ص4.

(19)_ عمار عباس الحسيني، مرجع سابق، ص44.

(20)_ نائلة قورة، مرجع سابق، ص 52، 53.

(21)_ خالد ممدوح العزي، **الجرائم المالية الاليكترونية الجرائم المصرفية أنموذجا**، أعمال المؤتمر الدولي الرابع عشر للجرائم الاليكترونية، طرابلس، 24_25 مارس 2017م، ص147، مأخوذ من عنوان موقع الانترنت: http://jilrc.com/wp-content/uploads/2017/03/الجرائم-المالية-الإلكترونية-الجرائم-المصرفية-انموذجا.pdf.

(22)_ محمود محمد أبو فروة، 2009م، **الخدمات البنكية الاليكترونية عبر الانترنت**، (ط1)، عمان، دار الثقافة للنشر والتوزيع، ص115.

(23)_ منى شاكر فراج العسبلي، مرجع سابق، ص4.

(24)_ **سلطان حميد الجسمي، مخاطر الجرائم الإلكترونية، ص2**، مأخوذ من عنوان موقع الانترنت:
https://www.albayan.ae/opinions/articles/2015-09-19-1.2462367

(25)_ محمد ياسين، **الجرائم الاليكترونية.... خطر عابر للحدود**، 2016/02/27م، ص2، مأخوذ من عنوان موقع الانترنت:
www.alkhaleej.ae/home/print/f53c9315-c755-48f7-a351-9dc93baa2e5a/11791ad2-ba97-4842-bcb5-b39e967cb481

(26)_ محمد ياسين، مرجع سابق، ص2.

(27)_ يوسف حسين يوسف، مرجع سابق، ص138.

(28)_ محمد الألفي، 2002م، **المسؤولية الجنائية عن الجرائم الأخلاقية عبر الانترنت**، القاهرة، المكتب المصري الحديث، ص203.

(29)_ عمر عبد العزيز موسى الدرور، **آليات تفعيل الحماية والوقاية من الجرائم الاليكترونية (إنشاء ضبطية خاصة بالجرائم الاليكترونية)**، أعمال المؤتمر الدولي الرابع عشر: الجرائم الاليكترونية طرابلس 24_25 مارس 2017م/ 2018، مأخوذ من عنوان موقع الانترنت:
http://jilrc.com/الجرا-من-والوقاية-الحماية-تفعيل-آليات/

(30)_ يوسف حسين يوسف، 2011م، **الجرائم الدولية للأنترنت**، (ط1)، القاهرة، ص149.

(31)_ يوسف حسين يوسف، المرجع نفسه، ص 155.

(32)_ ناصر بن محمد البقمي، 1430هـ/ 2009م، **جرائم المعلومات ومكافحتها في المملكة العربية السعودية**، (ط1)، الرياض، ص173.

(33)_ ناصر بن محمد البقمي، 1430هـ/ 2009م، **جرائم المعلومات ومكافحتها في المملكة العربية السعودية**، (ط1)، الرياض، ص 179.