

الآثار الاقتصادية للجرائم الإلكترونية

اعداد :

أ.د. يحيى برويقات عبد الكريم

كلية العلوم الاقتصادية والتسيير و العلوم التجارية ، جامعة تلمسان، الجزائر

ab_berrouiguet@yahoo.fr

ملخص :

أصبحت أجهزة الحاسوب و الهواتف الذكية جزءا لا يتجزأ من حياتنا اليومية ، و تعتمد استعمال شبكات الاتصال كالانترنت ؛ ولقد قدمت هذه الوسائل الحديثة فوائد جمة للمجتمعات و لكنها حملت معها أيضا أضرار بسبب سوء استخدامها من طرف البعض أي بسبب الجرائم الإلكترونية .

تحاول هذه الدراسة عرض الآثار الاقتصادية الناجمة عن الجرائم الإلكترونية وكيفية الوقاية أو التقليل من آثارها .

الكلمات المفتاحية : تكنولوجيا المعلومات ، الجرائم الإلكترونية ، الآثار الاقتصادية.

Abstract :

In our modern society, the use of the computers, smartphones and communication networks are widely diffused. This technology has advantages but also disadvantages because some people make cybercrime.

The aim of study is to present the economic impact of the cybercrime and how to prevent it or to minimize it impact.

Keywords : information technology , cybercrime, economic impact.

JEL Code : O17

مقدمة :

منذ القدم و الإنسان يطور باستمرار أدوات تسهل حياته ، و كلما طور أداة أو طريقة كان لها مزايا على واقعه و لكن أيضا أضرارا بسبب سوء استعمالها من طرف البعض . وحدث هذا الأمر مع دخول العالم مرحلة تكنولوجيا المعلومات بفضل التطور الهائل في الإلكترونيك ، فلقد أصبحت أجهزة الحاسوب و الهواتف الذكية جزءا لا يتجزأ من حياتنا اليومية ، و تعميم استعمال شبكات الاتصال كالانترنت التي جعلت العالم كالفقرية الصغيرة ، فبينما كان عدد مستعملي الأنترنت سنة 2005 حوالي 1 مليار مستعمل أصبح في 2015 حوالي 3.2 مليار مستخدم ؛ ولقد قدمت هذه الوسائل الحديثة فوائد جمة للمجتمعات و لكنها حملت معها أيضا أضرارا بسبب سوء استخدامها من طرف البعض أي بسبب الجرائم الإلكترونية ، والتي تمثل أضرارا حادا قد يفوق الجرائم التقليدية .

تحاول هذه الدراسة عرض الآثار الاقتصادية الناجمة عن الجرائم الإلكترونية وكيفية الوقاية أو التقليل من آثارها . نقسم بحثنا إلى ثلاث عناصر : نتطرق في العنصر الأول لتعريف مفهوم الجرائم الإلكترونية ، ثم لتبيان آثارها الاقتصادية ، أما العنصر الثالث فنتطرق إلى أساليب الوقاية والحد من آثارها .

1- تعريف الجرائم الإلكترونية : يرتبط ظهور الجرائم الإلكترونية ارتباطا وثيقا بانتشار استعمال شبكات الاتصال على نطاق واسع ، ففي البداية كان استعمال تلك الشبكات في نطاق ضيق من طرف مراكز البحوث و الباحثين و التي كانت جد محمية ، و لكن مع انتشار و تعميم استعمال الشبكات لدى كل فئات المجتمع أصبح بإمكان بعض الأفراد القيام بإساءة استعمال تلك التكنولوجيا ، وهو ما يعرف بالجرائم الإلكترونية . و لكن ما المقصود بالجرائم الإلكترونية ؟

يعرف Elsie Bale الجريمة الإلكترونية على أنها " كل فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسة " ، و يعرفها خبراء منظمة التعاون الاقتصادي و التنمية بأنها " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و نقلها " ¹.

¹ محمد علي قطب ، الجرائم المعلوماتية وطرق مواجهتها ، مركز الاعلام الأمني ، البحرين www.policemc.gov.bh

و يعرفها Halder, D., & Jaishankar, K على أنها " المخالفات التي ترتكب ضد الأفراد أو المجموعات بدافع الجريمة ويقصد تشويه سمعة الضحية أو إحداث أذى مادي أو عقلي باستخدام شبكات الاتصالات مثل الانترنت " .¹

ويعرف سمير سعدون و آخرون الجرائم الإلكترونية هي كل فعل يأتيه الفرد عبر استعماله الوسائط الإلكترونية مثل : الحواسيب ، أجهزة الموبايل ، شبكات الاتصال الهاتفية ، شبكات نقل المعلومات ، شبكة الانترنت ، أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية عموماً².

و نستخلص من التعاريف السالفة الذكر أن الجريمة الإلكترونية تتسم بما يلي :

- تهدف إلى الإضرار بالآخرين سواء ضرراً مادياً أو معنوياً.
- تقع في الواقع الافتراضي باستعمال شبكات الاتصال.
- جريمة عابرة للحدود الجغرافية .

و للجرائم الإلكترونية عدة طرق أهمها :³

- تخريب المعلومات و اساءة استعمالها .
- سرقة المعلومات .
- تزوير المعلومات .
- انتهاك الخصوصية .
- التصنت .
- التجسس و يشمل اعتراض معلومات و معرفة ما يقوم به الأفراد.

¹ Halder, D., & Jaishankar, K. , Cyber crime and the victimization of women: Laws, rights, and regulations. Hershey, PA, USA, 2011.

² سمير سعدون مصطفى ، محمود خضر سليمان ، حسن كريم عبد الرحمان ، الجريمة الإلكترونية عبر الأنترنت أثرها و سبل مواجهتها ، مجلة التقني ، عدد 24 ، 2011 ، ص 45-53.

³ ذياب موسى البداينة ، الجرائم الإلكترونية : المفهوم و الأسباب ، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات و التحولات الاقتصادية و الدولية ، كلية العلوم الاستراتيجية ، عمان ، 2-4 سبتمبر 2013.

- التشهير بقصد الاساءة الى شخص ما .
 - السرقة العلمية.
 - سرقة الاختراعات.
 - الدخول غير القانوني للشبكات.
 - قرصنة البرمجيات من أجل استخدامها أو اعادة بيعها.
 - قرصنة البيانات .
 - القنابل الإلكترونية.
 - نشر مواد غير أخلاقية.
 - الاحتيال المالي و الغش و اجراء الصفقات التجارية الكاذبة و سرقة الأموال¹.
 - سرقة الأرقام السرية والمتاجرة بها.
- ويمكن أيضاً تصنيف المجرم الإلكتروني في أربع مجموعات رئيسية وهي²:
- المجموعة الأولى: الموظفون العاملون بمراكز الكمبيوتر وهم يمثلون الغالبية العظمى من مرتكبي الجرائم الإلكترونية وذلك بحكم سهولة اتصالهم بالحاسب ومعرفتهم بتفاصيله الفنية.
 - المجموعة الثانية: الموظفون الساخطون على مؤسساتهم أو شركاتهم والذين يستغلون معرفتهم بأنظمة الحاسب الآلي في شركاتهم وسيلة لايقاع الضرر بهم عبر نشر البيانات أو استعمالها أو مسحها.
 - المجموعة الثالثة: فئة العابثين مثل الهاكرز (Hackers) أو الكراكرز (crackers) ، وهم الذين يستغلون الكمبيوتر من أجل التسلية في أمور غير قانونية وليس بغرض التخريب.
 - المجموعة الرابعة: الأفراد الذين يعملون في مجال الجريمة المنظمة عبر استخدام الكمبيوتر.

2- الآثار الاقتصادية للجريمة الإلكترونية :

1 فاضل عباس الملا ، الخطورة الأمنية للجرائم الإلكترونية وسبل مكافحتها ، مجلة الكلية الاسلامية الجامعة ، عدد 7 ، 2009 ، ص 173-180.

2 وائل رفعت علي خليل ، إشكاليات الإعلام و معطيات الواقع ، دار غيداء ، 2015 ، ص 186-187.

الجرائم الإلكترونية هي واقع معاش يمس مجتمعاتنا ، وكما أن للجرائم التقليدية مضار فان للجريمة الإلكترونية مضار أيضا . نهتم في هذه الدراسة بالآثار الاقتصادية لهذا النوع من الجرائم ، اذ أن تلك الآثار ليست بالآثار الهامشية التي يمكن التغاضي عنها ، حيث أن الأرقام الصادمة التي تخص الخسائر الاقتصادية الفادحة تستدعي الاحاطة بتلك الآثار ، حيث قدر مركز الدراسات الإستراتيجية الدولية الخسائر الناجمة عن الجرائم الإلكترونية بأكثر من 400 مليار دولار كل سنة¹ ، و نبين فيما يلي الآثار الاقتصادية للجرائم الإلكترونية على مستوى الفرد و المؤسسات والبنوك و الهيئات الحكومية .

الآثار الاقتصادية على مستوى الأفراد :

- صرف مبالغ لإصلاح أو إعادة شراء أجهزة كمبيوتر نتيجة تعرضها لفيروسات .
- خسائر ناجمة عن سرقة مدخرات الأفراد بسبب قرصنة بطاقات الائتمان الخاصة بهم .
- خسائر ناجمة عن سرقة هوياتهم .
- انخفاض إنتاجية وإبداع الأفراد بسبب تعرضهم للابتزاز و التهديد .
- نقل ملكية الأسهم إلى قرصنة الأنترنت.
- فقدان الأفراد لوظائفهم بسبب اتهامهم بكشف أسرار مؤسساتهم و هم في الحقيقة ضحايا لاختراق أجهزتهم .

الآثار الاقتصادية على مستوى المؤسسات والبنوك والهيئات الحكومية :

- الاطلاع على المعلومات السرية الخاصة بالمناقصات وبالتالي تضييع فرص الاستفادة من صفقات .
- خسائر ناجمة عن اتلاف نظام المعلومات الإلكتروني للمؤسسات والبنوك.
- خسائر ناجمة الاطلاع على الخطط التسويقية للمؤسسات.
- خسائر ناجمة عن سرقة التصاميم و المنتجات المطورة تكنولوجيا مما يعني ضياع الملايير التي صرفت في البحث والتطوير .

¹ Center for strategic and international studies, The economic impact of cybercrime and cyber espionage, USA, July 2013 .

- خسائر ناجمة عن سرقة أموال المؤسسات و البنوك ، حيث يقول Greg Medcraft رئيس مجلس ادارة هيئة الأوراق المالية والاستثمارات الأسترالية " أن جرائم تكنولوجيا المعلومات تحرم المشاركين في الأسواق من استخدام أجزاء أساسية من الأسواق ، وستكون على الأرجح هي الضربة القاضية التالية في العالم " ¹. ومثال على ذلك سرقة 81 مليون دولار من البنك المركزي لبنغلاديش سنة 2016 .
- خسائر ناجمة عن تعطيل عمل شبكة البنوك .
- فقدان حصص من السوق بسبب سرقة معلومات عن الزبائن مثل سرقة قاعدة بيانات شفرات مفاتيح السيارات من الشركة المصنعة للسيارات .
- خسائر ناجمة عن سرقة معلومات عن زبائن البنوك ، فمثلا تعرض بنك JP Morgan سنة 2014 الى هجمة الكترونية تم اختراق بيانات 83 مليون زبون ، و أعلن البنك عن انفاق مبالغ اضافية من أجل التدابير الأمنية المعلوماتية ب 250 مليون دولار سنويا .
- خسائر ناجمة عن تعطيل شبكات الاتصالات أو شبكات الكهرباء.
- خسائر ناجمة عن تعطيل مصانع ، فمثلا استهدف قرصنة في ألمانيا مصنعا للصلب مما تسبب له في أضرار جسيمة.
- خسائر ناجمة عن تعطيل مواقع رسمية حكومية .

3- أساليب الوقاية و التقليل من الجرائم الإلكترونية :

إن الجرائم الإلكترونية هي ظاهرة في استفحال متزايد و لها آثار وخيمة كما تم تبيانه ، و بالتالي فان أحسن الحلول هي الوقاية منها و محاولة التقليل من آثارها ، و نقترح جملة من الأساليب والتدابير الكفيلة بتحقيق ذلك الهدف .

- نص قوانين تصب في مجال تنظيم الاتصالات والمعاملات عبر شبكات الاتصال الكترونية و حماية البيانات و مكافحة الجرائم الإلكترونية .

1 Wellisz.C, Le côté obscur de la technologie, Finance & développement, Septembre 2016 , pp 14-17.

- إيجاد مكاتب أو هيئات مكافحة الجرائم الإلكترونية ، ومدتها بالأجهزة المتطورة والكفاءات اللازمة لأداء مهامها.
- إدخال مواد تعليمية و تحسيسية من مخاطر الجرائم الإلكترونية في المدارس و الثانويات و الجامعات.
- إخضاع العاملين في المؤسسات والبنوك إلى دورات تكوينية مستمرة تهدف إلى تعلم كيفية الوقاية من الجرائم الإلكترونية.
- تشجيع البحوث العلمية حول الوقاية من الجرائم الإلكترونية في الجامعات ومراكز البحوث.

خاتمة :

تبين لنا من خلال هذه الدراسة أن الجرائم الإلكترونية أصبحت ظاهرة في نمو مستمر بسبب ازدياد عدد مستعملي شبكات الاتصال الإلكترونية ، و نظرا لخصائصها وسماتها خاصة أنها جرائم تتجاوز الحدود الجغرافية ، فان آثارها الاقتصادية هي كبيرة جدا تتجاوز المئات من الملايير من الدولارات و تلحق خسائر جمة بالأفراد و المؤسسات والبنوك والهيئات الحكومية ، وبالتالي وجب الوقاية منها باتخاذ أساليب تحد من آثارها السلبية .

المراجع :

1. ذياب موسى البداينة ، الجرائم الإلكترونية : المفهوم و الأسباب ، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات و التحولات الاقتصادية و الدولية ، كلية العلوم الاستراتيجية ، عمان ، 2-4 سبتمبر 2013.
2. سمير سعدون مصطفى ، محمود خضر سليمان ، حسن كريم عبد الرحمان ، الجريمة الإلكترونية عبر الأنترنت أثرها و سبل مواجهتها ، مجلة التقني ، عدد 24 ، 2011 ، ص 45-53.
3. فاضل عباس الملا ، الخطورة الأمنية للجرائم الإلكترونية وسبل مكافحتها ، مجلة الكلية الاسلامية الجامعة ، عدد 7 ، 2009 ، ص 173-180.
4. محمد علي قطب ، الجرائم المعلوماتية وطرق مواجهتها ، مركز الاعلام الأمنى ، البحرين www.policemc.gov.bh

5. وائل رفعت علي خليل ، إشكاليات الإعلام و معطيات الواقع ، دار غيداء ، 2015 ، ص 187-186.

6. Center for strategic and international studies, The economic impact of cybercrime and cyber espionage, USA, July 2013 .
7. Halder, D., & Jaishankar, K. , Cyber crime and the victimization of women: Laws, rights, and regulations. Hershey, PA, USA, 2011.
8. Wellisz.C, Le côté obscur de la technologie, Finance & développement, Septembre 2016 , pp 14-17.