PISSN : 2571-9904 - EISSN : 2602-7763

الأمن السيبيراني و الجريمة الإلكترونية في الدول ما بعد الحداثية: الولايات المتحدة الأمريكية -نموذجا-

Cyber Security and Cyber Crime in Post-Modern Countries: United States of America-modele-

حاتم بن عزوز[1]*،مناني حليمة*

[1]جامعةالعربي التبسي تبسة(الجزائر)، hatem.benazouz@univ-tebessa.dz

[2]جامعة باجي مختار عنابة (الجزائر)، halima.menani@univ-annaba.dz

تاريخ الاستلام: 10/ 04/ 2022 تاريخ القبول: 21/ 05/ 2022 تاريخ النشر: 30/ 06/ 2022

ملخص:

مع انتشار و تزايد الجرائم الالكترونية التي يواجهها مستخدمي الانترنت في المعاملات المهنية أو الشخصية، و الاعتماد المتزايد على البيانات الإلكترونية ، استوجب تطوير منظومة الأمن السيبيراني على عدة مستويات، فنمو عصر المعلومات أدى إلى تغيير وتيرة ووسائل و نوعية الجرائم الإلكترونية التي يتم ارتكابها ، و أدى كذلك إلى صعوبة الوصول الى المسؤولين عنها خاصة في الدول المتطورة تكنولوجيا و معلوماتيا، على غرار الو.م.أ، التي تعاني من مشكلة الانتشار الواسع للجرائم الالكترونية ،نظرا للاستخدام الواسع للأفراد والمؤسسات لشبكة الانترنت في تعاملاتهم اليومية و معاملاتهم المهنية، حيث يخزن كم هائل من المعلومات الشخصية والمالية عبر الإنترنت ،ما يترك الأفراد عرضة للقرصنة و لانتهاكات الخصوصية ، فيما تكون المؤسسات المالية والشركات المختلفة هي الأخرى عرضة للقرصنة و لاختراقات بياناتها، كل هذه الجرائم جعلت من الأمن السيبراني للولايات المتحدة أولوية كبرى لدى المؤسسات و الشركات الاقتصادية و المالية و العسكرية و ذلك بهدف مواجهة الهجمات و الجرائم الالكترونية التي تتزايد بشكل مستمر.

الكلمات المفتاحية: الأمن السيبيراني _ الجرائم الالكترونية_ الهجمات السيبيرانية_ الاختراق_ ما بعد الحداثة.

Abstract

With the spread and increase of electronic crimes faced by Internet users in a business or personal transactions, and the growing reliance on electronic data, the Cyber Security System had to be developed at several levels. The rising age of information has changed the frequency, methods and quality of cybercrime. It is also difficult to reach those responsible, especially in technologically and computationally developed countries, such as the United States, which suffer from the problem of the widespread spread of electronic crime, Given the widespread use of the Internet by individuals and institutions in their daily and business transactions, where an enormous amount of personal and financial information is stored on the Internet, making people vulnerable to hacking and privacy breaches, while financial institutions and various businesses are also vulnerable to hacking and data breaches, all of these crimes have made US cybersecurity a priority for financial and military institutions and businesses.This is to deal with cyber-attacks and increasing crime.

Key words: *cybersecurity _ cybercrime_ cyber attacks _ penetration_ post-modernity*

* حاتم بن عزوز

I. مقدمة

ساهم التطور التكنولوجي على مدى العقود القليلة الماضية في إحداث تحول في كيفية استخدام الناس لأجهزة الكمبيوتر كما و نوعا، فالجميع "تقريبا" يستخدم جهاز الكمبيوتر في حياته اليومية، في حين أن ظهور و انتشار استخدام شبكة الويب العالمية(الإنترنت) ساهم في إحداث ثورة في الاتصالات والمعاملات الرقمية، ليعمم استخدام الشبكة العنكبوتية، مشكلة بذلك "الفضاء السيبيراني" الذي استوعب و شمل "ضمنيا" في فضائه الافتراضي كافة مجالات الحياة الاجتماعية والمهنية و الحياة الخاصة، وهذا الاستخدام الواسع الذي يجسد التغلغل في كافة مناحي الحياة ،أتاح لكم كبير من المعلومات الاقتصادية و الشخصية والمعاملات المالية المتاحة (تدفق و توفر كم هائل من المعلومات بالإضافة إلى حركية كبيرة لها) و غير المحمية عبر هذا الفضاء السيبيراني، و هذا ما أدى إلى ظهور جرائم مستجدة و مستحدثة اختلفت عن ما كان معروف و سائد من أنماط الجرائم التقليدية إلى صيغة جديدة كالجرائم الالكترونية بفضل التكنولوجيا الالكترونية على غرار التجسس السيبيراني ،الهجمات السيبيرانية ،انتحال الشخصية، التخريب الالكتروني، سرقة البيانات المالية الرقمية ، الاختراقات الالكترونية بمختلف أنواعها...الخ ،وهو ما كبد الأفراد والمؤسسات وحتى الدول خسائر سنوية كبرى ماديا ، وهو ما سيتم عرضه من خلال هذا المقال، حيث تم تقسيمه إلى ثلاثة أجزاء رئيسية :الجزء الأول سيتطرق إلى مفهوم الأمن السيبيراني لما له من أهمية بالغة ، و الجزء الثاني سيتطرق إلى الجريمة المعلوماتية و كطل ما يتعلق بها من مضامين تفصيلية للإحاطة الشاملة بهذا المفهوم ،و أخيرا سيتم التطرق إلى واقع الجرائم الالكترونية في الولايات المتحدة الأمريكية ووسائل تطويرها لمنظومة أمنها السيبيراني لمواجهة هذه الجرائم الالكترونية المتزايدة.

أولا: تعريف الأمن السيبيراني:

هو مصطلح من جزئين (كلمتين) كلمة "الأمن" و جزء (كلمة) سيبيرانيcyber ، حيث يرتبط مقطع "سيبيراني" cyberيتمحور أساسا حول مفهوم "الأمن" متعدد الأبعاد: كالأمن المرتبط بالإعلام الآلي و بالأمن المرتبط بالشبكة العنكبوتية (شبكة الأنترنت) و ذلك لحمايتها من الهجمات السيبيرانيةcyber-attaque و التي يمكن أن يكون مصدرها إما أفراد أو تنظيمات (مؤسسات) أو حتى حكومات.(GHERNAOUTIK2019 , pp1-2)؛ و يعتبر تحقيق (المحافظة) على الأمن السيبيراني من الانشغالات الرئيسية التي تعمل الدول على تحقيقها و على تطويرها معا ، من خلال تطوير برامج الحماية (الحماية من الهجمات السيبيرانية المختلفة ، كالهجمات التخريبية عبر شبكة الانترنت من خلال الفيروسات أو هجمات التجسس "الاقتصادي و المالي" للحصول على المعلومات الخاصة بالبورصة و الأسواق المالية و براءات الاختراع و كذلك التجسس "العسكري" الذي يعمل المستهدفين من خلاله على سرقة المعلومات العسكرية الإستراتيجية الخاصة بشركات صناعة الأسلحة أو المعلومات العسكرية الحساسة الخاصة بالدول (منظومات الصواريخ، الدفاع ،الأماكن العسكرية الحساسة) و غيرها، و بالتالي توجب على الدول تطوير أنظمة للحماية و الوقاية من "الهجمات السيبيرانية" التي تندرج عادة ضمن الجرائم الالكترونية و تحقيق الأمن السيبيراني ؛ و ترتبط عادة مسألة الأمن السيبيراني و ما تعلق بهذا المجال من جرائم كالجرائم الالكترونية بالدول المتطورة تكنولوجيا ،التي عرفت قفزات نوعية في مجال "أجيال الانترنت" (التدفقات السريعة جدا) و المرتبطة بالتقدم في مجال الذكاء الصناعي ، و تعرف هذه المجتمعات بمجتمعات "ما بعد الحداثة" التي تجاوزت الحداثة (العصر الصناعي) لتنتقل إلى مجتمعات ما بد الصناعة المرتبطة بتكنولوجيا الاتصال و الشبكة العنكبوتية و الذكاء الصناعي ، على غرار الولايات المتحدة الأمريكية (عينة الدراسة) و اليابان و كوريا الجنوبية و بعض دول أوروبا .

ثانيا: الجريمة الالكترونية: المفهوم ، الخصائص و الأنماط

1-تعريف الجريمة الالكترونية: تتكون الجريمة الالكترونية أو الافتراضية "Cyber Crime" من مقطعين هما: الجريمة"Crime " و " Cyber"أي الالكترونية ،ويستخدم مصطلح الالكترونية لوصف فكرة جزء من الحاسب أو للإشارة إلى عصر المعلومات، أما الجريمة فهي السلوكيات والأفعال الخارجة عن القانون ؛ والجرائم الالكترونية :هي المخالفات التي ترتكب ضد الأفراد أو مجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية، أو إلحاق أي أذى مادي أو عقلي للضحية سواء كان مباشر أو غير مباشر، باستخدام شبكات الاتصالات مثل الانترنت، غرف الدردشة والبريد الالكتروني...(Halder.2011)

و تتشابه الجريمة الإلكترونية مع الجريمة التقليدية من ناحية وجود دافع لدى المجرم لارتكاب الجريمة ووجود ضحية، إضافة إلى أداة و مكان الجريمة ،لكن الاختلاف الحقيقي بين نوعي الجريمة، يكمن في أن الأداة في الجريمة الإلكترونية ذات تقنية عالية، كما أن مكان الجريمة لا يتطلب انتقال الجاني إليه انتقالا فيزيقيا. وبالتالي فهي كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات ، فلقد عرفها "سولاز" "Artar Solaz" على أنها :أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كانت مرتبطة بتقنية المعلومات ،و عرفها كل من "هلدر و جايشنكار" "Halder & k.Jaishankar" بأنها الجرائم التي ترتكب ضد أفراد أو مجموعات من الأفراد مع وجود دافع إجرامي لإلحاق الضرر عمدا بسمعة الضحية، أو التسبب في ضرر مباشر أو غير مباشر للضحية، وتسمى أيضا بجرائم الحاسوب حيث يتم استخدام جهاز الكمبيوتر كأداة لزيادة المعاملات غير القانونية ،كالاحتيال و الإتجار في المواد الإباحية والملكية الفكرية و سرقة الهويات و انتهاك الخصوصية(Alshalan.2006).

وفي تعريف "منظمة التعاون الاقتصادي" للجريمة الإلكترونية هي " كل سلوك غير مشروع، أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو نقلها (البداينة.2009) ،كما عرفها "Bosenblatt" على أنها كل نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو التي تحول عن طريقه.

ومن التعاريف الموسعة للجريمة الإلكترونية، التعريف الذي ورد في تقرير الجرائم المتعلقة بالحاسوب الذي أقره" المجلس الأوربي" على أنه تعد جريمة إلكترونية كل حالة يتم فيها:

تغيير معطيات أو بيانات أو برامج أو محوها أو كتابتها أو أي تدخل آخر في مجال إنجاز البيانات أو معالجتها، وتبعا لذلك تسببت في ضرر اقتصادي أو فقد حيازة ملكية شخص آخر أو بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص آخر.

2-تعريف الجرائم الإلكترونية حسب تشريعات بعض الدول:

2-1-تعريف المشرع الجزائري:

أول نص تشريعي جزائري في مجال الإجرام المعلوماتي سنة 2001 بموجب القانون رقم 01-09، المواد 144 مكرر و 146 و144 مكرر 1 و144 مكرر 2 و146 قانون العقوبات الجزائري، ومن خصوصيات المادة 144 مكرر، أن المشرع أدرج فيها لأول مرة مصطلح "وسيلة إلكترونية أو معلوماتية" ليأتي بعدها القانون رقم 14-15

سنة 2004 الذي أدخل إلى قانون العقوبات قسم سابع مكرر تحت عنوان" المساس بأنظمة المعالجة الآتية للمعطيات" (المواد من 394 مكرر إلى 394 مكرر 7 ق.ع. الجزائري) (الجريدة الرسمية .2009) .

2-2-تعريف المشرع البلجيكي:

تعد ضمن الجريمة الإلكترونية " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية، ويعد استخدام مصطلح الجريمة المعلوماتية للدلالة على الجرائم الناشئة عن استخدام الأنترنت.

2-3-تعريف المشرع السويدي:

تعتبر السويد أول الدول التي سنت التشريعات الخاصة بجرائم الحاسم الآلي والأنترنت حيث صدر قانون البيانات السويدي سنة 1973 تتبعها الولايات المتحدة الأمريكية حيث شرعت قانونا خاص بحماية أنظمة الحاسب الآلي في سنة 1985 فأصدرت قانون بتاريخ 08 جانفي 1988 لمكافحة الجريمة الإلكترونية مع استحداثها لمواد جديدة تخص الجرائم الإلكترونية في قانون العقوبات .

2-4- تعريف المشرع الفرنسي:

عرفها التشريع الفرنسي في الأمر الصادر 1945/06/30 والمتعلق بالتحقيق والمتابعة وقمع الجرائم الماسة بالتشريع الاقتصادي الفرنسي، وهذا ما نصت عليه المادة الأولى من هذا الأمر(Renucci,1995).

فالمادة 1/323 من قانون العقوبات الفرنسي تعاقب على فعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للبيانات أو في جزء منه بالحبس لمدة سنتين وغرامة 30 ألف أورو، فإن نتج عن الدخول أو البقاء محو أو تغير في البيانات الموجودة.(André.2001)

2-5-تعريف المشرع الأمريكي:

تشمل الجرائم الإلكترونية أي نوع من المخططات غير القانونية التي تستخدم مكونًا واحدًا أو أكثر من مكونات الإنترنت (غرف الدردشة والبريد الإلكتروني ولوحات الرسائل والمواقع الإلكترونية والمزادات) لإجراء معاملات احتيالية أو نقل عائدات الاحتيال إلى المؤسسات المالية أو إلى جهات أخرى مرتبطة بالمخطط. . تنطبق الجرائم الإلكترونية أيضًا على إنشاء رسائل بريد إلكتروني غير مرغوب فيها ، وتنزيل فيروسات أو برامج تجسس على الكمبيوتر ، ومضايقة شخص آخر عبر الإنترنت ، واستغلال الأطفال في المواد الإباحية ، والتحريض على الدعارة عبر الإنترنت. لعل أبرز أشكال الجرائم الإلكترونية هو سرقة الهوية ، حيث يستخدم المجرمون الإنترنت لسرقة المعلومات الشخصية من المستخدمين الآخرين.(USLEGAL.2022)

3-خصائص الجريمة الإلكترونية: يمكننا إيجاز خصائص الجريمة الإلكترونية فيما يلي:

- مسرح الجريمة لا يظهر في الواقع بل هو الفضاء الإلكتروني بأسره.
- في الجريمة الإلكترونية المجرم والضحية لا يشترط أن يكونا في مكان واحد أو دولة واحدة، عكس الجرائم العادية كالمخدرات أو القتل ويكون لها مسرح جريمة ثابت للمعاينة، فهي جرائم ترتكب عن بعد.

- مبدأ إقليمية النص الجنائي، ومدى إمكانية تطبيق القوانين الوطنية على الجرائم الواقعة بالأنترنت.
- الجرائم المعلوماتية قابلة للتوسع والابتكار، فهي مرتبطة في الأساس بالتقدم التقني والمعلوماتي فكلما ظهرت تقنية جديدة ظهرت معها جرائم جديدة.
- تتسم الجرائم المتعلقة بشبكة الأنترنت بالخطورة البالغة، فهي ترتكب من طرف فئات متعددة مما يصعب معرفة من هو مرتكب الجريمة، هذا ما يجعل مكتب التحقيقات الفيدرالي الأمريكي يطلق عليها وصف الوباء "Epidemic "(حسن.2007).

- تتصف هذه الجريمة بالخفاء، أي عدم وجود آثار مادية يمكن متابعتها، فهي صعبة الاكتشاف، وكذا صعوبة الاحتفاظ بدليل الجريمة المعلوماتية، في أقل من ثانية أن يمحو أو يحرف أو يغير البيانات والمعلومات، (مليكة.2012) في زمن محدود، فضلا عن سهولة تهربه عن مسؤولية هذا العمل بإرجاعها إلى خطأ في نظام الكومبيوتر على سبيل المثال.

- عدم وجود مفهوم مشترك لماهية الجريمة المعلوماتية، وعدم وجود تعريف قانوني موحد لها، ولعل السبب في ذلك يرجع إلى عدم وجود تنسيق دولي في مجال الجريمة المعلوماتية، ذلك لغياب معاهدات دولية ثنائية أو جماعية لمواجهتها، أو لاختلاف مفهومها تبعا لاختلاف النظم القانونية.

4- أبرز الأفعال المشكلة لجرائم الإنترنت بالولايات المتحدة الأمريكية:

قسمت هذه الأفعال إلى ثلاث فئات واسعة حسب دراسة « UNODC » United Nations Office on Drug and Crime وهي كالآتي:

الأفعال ضد السرية والنزاهة وتوافر بيانات الكومبيوتر أو النظم:

- الدخول غير المشروع لنظام الحاسوب.
- الدخول غير المشروع و الاستيلاء على البيانات الخاصة.
- استنساخ المعلومات والبيانات أو النظام بشكل غير مشروع.
- إنتاج أو توزيع أو امتلاك أدوات إساءة استعمال الحاسوب.
- اختراق الخصوصية أو بيانات أساليب الحماية.(محمد.2000).

أفعال ذات صلة بالحاسوب لمصالح شخصية أو مادية:

- الاحتيال المتعلق بالحاسوب أو التزوير.
- الجرائم الالكترونية المتعلقة بالهوية.
- حقوق الطبع والنشر والجرائم المتعلقة بالعلامات التجارية التي لها صلة بالمجال الإلكتروني.
- الأعمال المسببة ضرر للحواسيب الشخصية.
- الجرائم الإلكترونية المتعلقة بإغراء أو استمالة الأطفال

الأفعال الحاسوب ذات الصلة بمحتويات الحاسوب:

- الأفعال المرتبطة بخطابات الكراهية (المتواجدة بكثرة ضمن أوساط التواصل الاجتماعي).
- إنتاج أو توزيع وحيازة المواد الإباحية عن الأطفال والمتعلقة بالحاسوب.
- الأعمال الإلكترونية المتعلقة بدعم جرائم الإرهاب.(UNODC.2013)

ثالثا: سياسة الولايات المتحدة الأمريكية في تحقيق الأمن السيبيراني:

تصنف الولايات المتحدة الأمريكية الأولى عالميا من حيث الإنفاق على "الأمن السيبيراني" ، و هذا يرجع إلى أن الولايات المتحدة الأمريكية تعتبر من اكبر الدول التي تنتشر فيها الجرائم الالكترونية مع ما يترتب عنها من آثار مادية ومعنوية على متخلف الفئات، سواء كانوا أفراد أو شركات أو حتى هيئات حكومية، لذلك تم اختيار ها كنموذج لهذا النوع من الجرائم، فحسب ما تشير له الإحصائيات والدراسات المحلية والعالمية لذا فهي تعد من التجارب الثرية التي يمكن الاستفادة منها فيما يتعلق بالجرائم الالكترونية وسبل مجابهتها من اجل تحقيق للأمن السيبيراني .فمستخدمي الانترنت في الولايات المتحدة في احتمال مستمر للوقوع ضحية للجرائم الإلكترونية فالأفراد الذين يقومون بخدماتهم المصرفية عبر الإنترنت يحملون فرصة الوقوع ضحية الهويات المسروقة بنسبة 50 ٪ من أولئك الذين يقومون بأعمالهم المصرفية شخصيًا، وأولئك الذين يشترون العناصر الموجودة عبر الإنترنت لديهم فرصة أعلى بنسبة 30٪ للتعرض للأذى في حين أن استخدام برامج المراسلة الفورية أو البريد الإلكتروني يتيح فرصة تزيد عن 50٪ ليكون ضحية للاختراق أو الابتزاز وظهور البرمجيات الخبيثة للحاسوب (Reyns.2013) .

ووفقا وفقًا لمكتب التحقيقات الفيدرالي. تعد سرقة الهوية الشخصية هوية الشركات الجريمة الالكترونية الأسرع في الولايات المتحدة، فهي في تزايد مستمر ومتسارع وتؤدي إلى تأثيرات مختلفة على المستوى الفردي مقارنة بالتأثيرات التي تخلفها سرقة هويات الشركات فعلى المستوى العالمي قد تصل سرقة هوية الشركات إلى 3.7 تريليون دولار سنويًا، إضافة إلى الغرامات التي تتحملها الشركات الأمريكية كآثار مترتبة لعدم فعالية أمنها السيبراني والذي يعد من مسؤوليتها. (Janson. 2004)

إن السرقات التي تتعرض لها الولايات المتحدة الأمريكية من الجرائم الالكترونية لا تقف ضمن حدودها بسب الامتداد العالمي للأنترنت، فقد قام"ادوارد بيرسون" Edward Pearson وهو شخص من انجلترا بسرقة أكثر من 8 ملايين هوية و 2700 رقم بطاقة مصرفية و 200.000 حسابPayPal (شركة أمريكية).(Broadhurst.& al.2014) ،وتعد عمليات التصيد الاحتيالي من بين الإشكال الأكثر انتشار بالولايات المتحدة، فحسب التقارير فإن هذه الأخيرة تعد المصدر الأول لها بنسبة34.1% من إجمالي نشاطات التصيد الاحتيالي العالمي، كما أنها تشمل نسبة 25% من إجمالي مواقع التصيد في العالم في هذا الاطار ذكرت احدى الدراسات الصادرة سنة 2005، بأن 73 مليون أمريكي قد تلقى في المتوسط 50 رسالة تصيد على الأقل خلال العام الماضي، وأكثر من مليون أمريكي فقدوا 929 مليون دولار من الاستحقاق السنوي سنة 2004.

وأدى كذلك التوسع السريع للتجارة الإلكترونية بالولايات المتحدة إلى زيادة خطر الجرائم الإلكترونية، ومن العوامل المساهمة في هذا الارتفاع زيادة تقنيات المعلومات والاتصالات ، وانخفاض تكاليف المعاملات على المتاجرة التقليدية (من خلال المحلات) ، ورفع المنافسة والإنتاجية من قبل الشركات، هذه العوامل لم تساهم في انتشار الجرائم الالكترونية فقط وانما ساهمت أيضا في تغيير الثقافة الاقتصادية للمستهلك

الأمريكي بسبب نمو و إتاحة التجارة الالكترونية، حيث تظهر الدراسات أن ن أسعار الإنترنت أرخص بنسبة 9-16٪ من أسعار المتاجر التقليدية .(Ramcharran. 2013).

ففي سنة 2018 سجل مركز شكاوى جرائم الإنترنت في الولايات المتحدة 16128 حالة سرقة هوية عبر الإنترنت وهي عبارة عن استخدام احتيالي لمعلومات أشخاص دون موافقهم في أغراض إجرامية بما في ذلك الأعمال المصرفية، والمستندات، والاحتيال على بطاقات الائتمان، كما سجل المركز 65116 حالة احتيال في حالات عدم الدفع أو عدم التسليم.ولقد وفرت المعاملات الرقمية وظهور الخدمات المصرفية عبر الإنترنت لمجرمي الإنترنت بيئة يمكنهم من خلالها استخدام المعلومات الشخصية للعملاء بطريقة احتيالية دون علمهم، هذا ما كبد ضحايا الجرائم الإلكترونية أضرارًا جسيمة ، لا سيما عند اختلاس معلوماتهم الشخصية أو المالية لأغراض إجرامية، في حين بلغت عمليات الاحتيال على الثقة عبر الإنترنت والاحتيال العاطفي إلى 362.5 مليون دولار أمريكي عبارة عن خسائر الضحايا المبلغ عنها في سنة 2018.(Rusch& J. 2003)

و تمثل مشكلة اختراق الحسابات والاحتيال في الولايات المتحدة احدى اكبر معضلات الجرائم الالكترونية لذا يسعى الأفراد لحماية حساباتهم و تدعيم حواسيبهم بأفضل برامج الحماية سعيا منهم لمنع التعرض للاحتيال أو الاختراق وتعطيل الأعمال، وفي هذه النقطة كشفت دراسة استقصائية أجريت سنة 2018 أن أكثر من 80 %من مستخدمي الإنترنت في الولايات المتحدة يعتقدون أنهم يحمون أنفسهم جيدا عبر الإنترنت ، وعلى هذا النحو ، ربما لم يكن مفاجئًا أن 56 %من المشاركين قد اتخذوا شكلاً من أشكال الاحتياطات الأمنية عبر الإنترنت خلال السنوات الثلاث الماضية ،ومع ذلك أظهر استطلاع آخر أن أكثر من ربع البالغين يستخدمون نفس كلمة المرور لجميع عمليات تسجيل الدخول على الإنترنت ، مما يدل على أن الراحة يمكن أن تقف في طريق الأمان.(Joseph.2021)

وعلى مستوى آخر نجد المعاملات الالكترونية للشركات في عالم الأعمال الرقمية، فاليوم تستفيد العديد من الشركات من الفرص المتطورة باستمرار للفضاء الإلكتروني، سواء كان الأمر يتعلق بإتمام العمليات الداخلية أو اعتماد الخدمات الإلكترونية أو التواصل مع الشركات والعملاء الآخرين، هي كلها تقنيات رقمية تتبناها المؤسسات باستمرار وتسعى لاستخدام كل ما هو جديد منها.(Janson.2004)، وخلال العقدين الماضيين، زاد عدد خروقات البيانات في الولايات المتحدة عشرة أضعاف تقريبًا ، تزامنا مع زيادة الاعتماد على البيانات الرقمية بين معظم الشركات ففي سنة 2019 ، تم الإبلاغ عن حوالي 1506 حالة اختراق ، وهو ثاني أعلى معدل حوادث الكترونية حتى الآن اعتبارا من سنة 2020 ،ويظل أكبر خرق للبيانات عبر الإنترنت في جميع أنحاء العالم هو الخرق الأمني لسنة 2018 لشركة Apollo لاستخبارات المبيعات ، والتي شهدت اختراق أكثر من تسعة مليارات نقطة بيانات، ولكن بصرف النظر عن سجلات البيانات المفقودة تواجه الشركات أيضًا عواقب قانونية وأضرارًا مالية في عقب هجوم إلكتروني سنة 2019 ، على سبيل المثال ، وافقت وكالة الائتمان Equifax ومقرها أتلانتا على دفع تسوية قدرها 575 مليون دولار أمريكي بعد خرق البيانات، واليوم يبلغ متوسط تكلفة خرق البيانات في الولايات المتحدة ما يقرب من تسعة ملايين دولار أمريكي.

وبما أن الإنترنت أصبحت أداة لا غنى عنها للشركات والصناعات في جميع أنحاء العالم ،فقد تطور المشهد عبر الإنترنت أيضًا إلى بيئة صيد مغرية للمجرمين، فسنة 2019 تجاوز عدد حوادث الجرائم الإلكترونية 31000 حالة في جميع أنحاء العالم أما عدد الخروقات مع فقدان البيانات المؤكدة ارتفع إلى ما يقرب من 4000 حالة في نفس السنة، وقد كان هذا الارتفاع واضح بشكل خاص في الولايات المتحدة حيث

وقع العديد من الشركات والمستخدمين الفرديين وحتى الحكومة ضحية للتدخلات الالكترونية.(Manky. 2013)

فمع زيادة استخدام الإنترنت والبيانات ، أصبحت قواعد البيانات الحكومية تشكل أهدافا رئيسية للقراصنة وأعمال الحرب الإلكترونية، ووفقًا للمؤلف "ريتشارد كلارك " تُعرَّف الحرب الإلكترونية على أنها أفعال تقومبها دولة قومية لاختراق أجهزة الكمبيوتر أو الشبكات الخاصة بدولة أخرى لإحداث ضرر أو تعطيل، فيما تشمل التعريفات الأوسع الجهات الفاعلة غير الحكومية ، مثل الجماعات الإرهابية والشركات والجماعات السياسية أو الأيديولوجية المتطرفة والمنظمات الإجرامية ونشطاء القرصنة.

لقد كانت الهجمات الإلكترونية في الولايات المتحدة الأمريكية مصدرا لأمنها القومي (العسكري، الاقتصادي، المالي) لسنوات ، حيث لم يقتصر الأمر على زيادة تواتر خروقات البيانات فحسب ، بل زادت تعقيداتها وتداعياتها الاقتصادية، وفي سنة 2018 كانت الولايات المتحدة الدولة الأكثر تضررًا من الجرائم الإلكترونية من حيث الأضرار المالية، حيث قدر خبراء الصناعة أن الحكومة الأمريكية واجهت تكاليف تزيد عن 13.7 مليار دولار أمريكي نتيجة للهجمات الإلكترونية فقط، على الرغم من أن الولايات المتحدة تعد احدى أبرز الدول التي لديها أعلى التزام بالأمن السيبرانيCybersecurity(كما تمت الإشارة إليه أعلاه فهو فرع من فروع التكنولوجيا يعنى بحماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقمية التي تهدف عادة للوصول إلى المعلومات الحساسة أو تغييرها، أو إتلافها أو ابتزاز المستخدمين للحصول على الأموال أو تعطيل العمليات التجارية)، ويأتي هذا التصنيف بناء على مؤشر الأمن السيبرياني العالمي. (Kaplan,Sharm,& Weinberg .2011)

وتخصص الولايات المتحدة سنويا مبالغ ضخمة للحفاظ على أمنها السيبراني ، ففي سنة 2019 بلغ الإنفاق الحكومي على تكنولوجيا المعلومات 88 مليار دولار أمريكي، وبحلول سنة 2021 تجاوز هذا الرقم 92 مليار دولار، وذلك لاعتمادها أحدث قواعد الاستراتيجيات الالكترونية لوزارة الدفاع، و تشمل أهدافها الإلكترونية بناء القوات اللازمة للقيام بعمليات الفضاء الإلكتروني، وتأمين بيانات وزارة الدفاع والدفاع عنها و الإعداد للهجمات الإلكترونية المعطلة والمدمرة ، ودمج الخيارات والتحالفات الإلكترونية في الخطط.

بالنظر إلى عدد ونطاق انتهاكات البيانات الأمريكية على مدى السنوات القليلة الماضية ، نستطيع فهم السبب وراء الإنفاق الفيدرالي المتزايد والتركيز على الأمن السيبراني، ففي سنة 2018 أبلغت الوكالات الفيدرالية عن 31107 حادث أمن إلكتروني وفي العام التالي سجلت الحكومة الأمريكية 5.6 بالمائة من خروقات البيانات و 2.1 بالمائة من جميع السجلات المكشوفة مع وجود أكثر من 198 مليون سجل تم اختراقه ، ويعد اختراق قاعدة بيانات الناخبين في الولايات المتحدة في ديسمبر 2015 من بين أكبر انتهاكات البيانات عبر الإنترنت في جميع أنحاء العالم، وقد استحوذت هذه الحادثة بشكل خاص على اهتمام عالمي خلال الانتخابات الرئاسية الأمريكية لعام 2016،حيث ارتبطت الجريمة الإلكترونية ارتباطا وثيقا بالانتخابات الأمريكية عندما تم اختراق أجهزة كمبيوتر DNC وتسريب رسائل البريد الإلكتروني مرة أخرى، الامر الذي شكل خوفا من أن الإجراءات الأمنية غير الكافية قد تؤثر على انتخابات 2020 بطريقة مماثلة خاصة وأن جائحة كورونا"Covid-19" وضعت نظام الاقتراع الأمريكي على المحك كون أغلب التصويت تم عبر الإنترنت.(Johnson.2021)

II. خاتمة:

حسب العديد من الدراسات فإن معدل نمو الجرائم الالكترونية في الولايات المتحدة على مدى السنوات القليلة القادمة سيستمر بالتزايد خاصة فيما يتعلق بالاحتيال والسرقة، والاختراقات الحسابية والمعلوماتية لذا فالحكومة الأمريكية تسعى جاهدة لتخفيف حدة هذه الجرائم وتضييق نطاقها قدر المستطاع، بهدف الحد من آثار المادية والمعنوية ورفع مستوى الأمن السيبراني مع استمرار التشريعات في تعديل وإنشاء قوانين جديدة للتعامل مع الاتجاهات والتكتيكات الحالية التي يستخدمها مجرمو الإنترنت، كتبسيط تخصيص الموارد والتداخلات ليكون لها تأثير على منع الاحتيال بأشكاله المختلفة على سبيل المثال، كذلك التأكيد على الحاجة المتزايدة للإبلاغ عن الجرائم الإلكترونية الاقتصادية واعتماد نظام موحد يمكن من خلاله الإبلاغ عن هذه الجرائم إلى سلطات المنفذة للقانون لمنع الجريمة نفسها والتحقيق فيها، هذه الاستراتيجيات وغيرها اعتمدتها الولايات المتحدة سعيا منها في مواجهة الجرائم الالكترونية التي مست العديد من المجالات والمستويات الفردية والحكومية.

الإحالات والمراجع:

- البداينة ذياب، الجريمة الافتراضية. ورقة مقدمة في الملتقى الدولي" التنظيم القانوني للأنترنت والجريمة الإلكترونية" جامعة عاشور زيان، الجلفة، الجزائر.2009.
- الجريدة الرسمية،القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، العدد 47،2009.
- حسن بن سعيد سيف الغافري ،السياسة الجنائية في مواجهة جرائم الأنترنت-دراسة مقارنة. رسالة دكتوراه، جامعة عين الشمس،مصر،2007.
- محمد عبد الرحيم،جرائم الأنترنت والاحتساب عليها. ط3، مؤتمر القانون والكومبيوتر والأنترنت ، جامعة الإمارات العربية المتحدة،2000.
- مليكة عطوي، الجريمة المعلوماتية.حوليات جامعة الجزائر.العدد 21، 2012.

- Alshalan. A, Cyber-crime and Victimization.Unpublished Ph.D. Dissertation in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Sociology in Department of Sociology, Anthropology and Social Work Mississippi State University.2006.
- André Lucas. Jean Devrèze, Droit de l'informatique et de l'Internet. Édition Dalloz, collection Thémis (Droit Privé), France,2001 .
- Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. Organizations and cyber crime: Ananalysis of the nature of groups engaged in cyber crime. International Journal of CyberCriminology2014.
- Gold.S. The evolution of payment card fraud. Computer Fraud and Security,2014, https://doi.org/10.1016/S1361-3723
- Halder. D &Jaishankar. K2011 ..Cybercrime and the Victimization of Women: Laws, Rights, and Regulations, Hershey- PA- USA.https://doi.org/10.4018/ industry. International Journal of E-Business Research,
- Janson, N, Managing financial risk. Australian Journal of Pharmacy, 85(1011),2004, https://doi.org/10.1002/
- Jean François Renucci , Droit économique, Série Droit, Masson / Armand Colin, Edition Paris, 1995.
- Joseph Johnso. U.S. consumers and cyber crime - Statistics & Facts,2021../www.statista.com/topics/3387.
- Joseph Johnson .U.S. government and cyber crime - Statistics & Facts,2021.,https://www.statista.com/topics/3387/us-government-and-cyber-crime/#dossierKeyfigures.
- Kaplan,J.Sharm,S.& Weinberg A.,Meeting the cybersecurity challenge, McKinsey Quarterly,2011.
- Manky. D. , Cybercrime as a service: A very modern business. Computer Fraud and Security,2013. https://doi.org
- Ramcharran. H. , E-Commerce growth and the changing structure of the retail sales,2013.
- Reyns, B. W. ,Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. Journal of Research in Crime and Delinquency, 2013.http ://doi.org/10.1177
- Rusch.J. J, Computer and Internet Fraud : A Risk Identification. Computer Fraud & Security,2003., https://doi.org/10.1016/
- Solange Ghernaouti, Cybersécurité :Analyser les risqué ,Mettre en oeuvre les solutions ,DUNOD, 6 éme edition, Paris, 2019.
- United Nations Office on Drugs and Crime. Comprehensive Study on Cybercrime. United Nations, 2013.
- USLEGAL,Cybercrimes Law and legal definition,2022,https://definitions.uslegal.com.