



الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة غرداية



معهد العلوم الاقتصادية والتجارية وعلوم التسيير

قسم العلوم التجارية

بالتعاون مع

مخبر التطبيقات الكمية والنوعية للارتقاء الاقتصادي الاجتماعي والبيئي بالمؤسسات الجزائرية

وفرة البحث : PRFU

"المؤسسات الناشئة كمحرك للنمو الاقتصادي في الجنوب الجزائري، التحديات وآليات الدعم"

ينظم الملتقى الوطني عن بعد حول:

دور التجارة الإلكترونية في دعم نمو المؤسسات الناشئة في الجزائر

يوم 14 جوان 2023

عنوان المداخلة:

الأمن السيبراني ودوره في حماية خصوصية المستهلك في ظل التجارة الإلكترونية

Cyber security and its role in protecting consumer privacy in the context of electronic commerce

إعداد:

الاسم و اللقب	صواق عبد القادر	هوارى معراج
الدرجة العلمية	طالب دكتوراة	أستاذ التعليم العالي
الجامعة	جامعة غرداية	جامعة غرداية
رقم الهاتف	0697472931	0668600086
البريد الإلكتروني	souag.abdelkader@univ-ghardaia.dz	m_houari@yahoo.fr

الملخص:

تهدف الدراسة إلى تسليط الضوء على أهمية دور الأمن السيبراني لحماية خصوصية المستهلك في ظل التجارة الالكترونية، وذلك انطلاقاً من تعريف مصطلح الأمن السيبراني ومعرفة عناصره وأهدافه، ثم الحديث عن حماية خصوصية المستهلك وإظهار مختلف الانتهاكات التي تواجهه في الفضاء السيبراني، بعدها التطرق إلى أكبر تحدي واجهته شركة Facebook لحماية خصوصية مستخدميها خاصة بعد تعرضها لحادثة سرقة البيانات الشخصية الخاصة بثلاثون (30) مليون مستخدم، وفي الأخير الخروج بأفضل الآليات المتبعة لخفض مختلف المخاطر السيبرانية، حيث كانت أهم نتيجة توصلنا إليها أن التربع على عرش النجاح لا يعني عدم وجود تحديات، وأنه كلما زادت المخاطر السيبرانية وانتهاكات خصوصية المستهلكين كلما انعكس سلباً على استمرارهم في التعامل إلكترونياً، فاحترام المستخدم والحرص على إرضاءه هو سر بقائه.

الكلمات المفتاحية: الأمن السيبراني – الفضاء السيبراني – خصوصية المستهلك – التجارة الالكترونية – خفض المخاطر.

Summary :

The study aims to highlight the importance of the role of cyber security in protecting consumer privacy in light of electronic commerce, this is based on defining the term cyber security and knowing its elements and objectives, then talking about protecting consumer privacy and showing the various violations it faces in cyberspace, to protect the privacy of its users, especially after it was exposed to theft of personal data of thirty (30) million users, in the end, we came up with the best mechanisms used to reduce the various cyber risks, as the most important result we reached was that being on the throne of success does not mean that there are no challenges, and that the greater the cyber risks and violations of consumers' privacy, the more negatively it will be reflected on their continued dealing electronically, so respect the user and ensure his satisfaction It is the secret of his survival.

Keywords : Cyber security – cyberspace - consumer privacy - electronic commerce - risk reduction.

مقدمة:

لقد زاد التطور الهائل والسريع لتكنولوجيا المعلومات والاتصال من سهولة وسلاسة التواصل بين الأفراد والمؤسسات في مختلف دول العالم، وقد أصبح العالم اليوم أشبه بقريّة صغيرة، حيث أن العديد من الأنشطة الاجتماعية والاقتصادية في معظم دول العالم اليوم تتم بمساعدة الأنظمة الالكترونية عبر شبكة الإنترنت، ما سمح لعمليات التجارة الالكترونية بتحسين تجربة المستخدمين

وتوسيع رقعة الأسواق العالمية وكذا الوصول إلى منتجات وخدمات واسعة النطاق، وسهولة التسوق عالميا والدفع عبر الانترنت، ومع ذلك تنطوي هذه المزايا على تحديات أمنية متعددة مثل تسرب المعلومات الشخصية والمالية، التلاعب بالمعاملات الالكترونية، الاحتيال عبر الانترنت، الاختراق، الجوسسة، السرقة، التدمير، تعطيل الخدمة الالكترونية، المساس بحمة الحياة الخاصة... الخ وبهذا تُنزل الضرر المادي والمعنوي وبعمليات صُنع القرار لدى الدول والمؤسسات على اختلاف أشكائها ونشاطها، وهذا ما شهدته على سبيل المثال شركة Facebook التي ستتطرق إليها كنموذج لأفضل الشركات الناشئة التي أصبحت خلال فترة قصيرة أحد الشركات العملاقة العابرة للقارات تعرضت يوما ما لحادثة سرقة البيانات الشخصية الخاصة بثلاثون (30) مليون مستخدم، وهذا ما يستدعي البحث عن آليات للحد من انتهاكات خصوصية المستهلك في الفضاء السيبراني.

وانطلاقا من هذا الطرح يُطرح الإشكال المعرفي التالي:

كيف يُسهم الأمن السيبراني في حماية خصوصية المستهلك في ظل التجارة الالكترونية؟

وتندرج تحت هذه الإشكالية الرئيسية، أسئلة فرعية تتمثل في الآتي:

- 1- فيما تتمثل عناصر الأمن السيبراني؟
- 2- ما مضمون تجربة شركة فايسبوك في حماية خصوصية مستخدميها؟
- 3- ما هي أهم الآليات المتبعة لخفض المخاطر السيبرانية للشركات والمؤسسات؟

أهداف البحث:

تهدف الدراسة من خلال الإجابة عن تساؤلات مشكلة الدراسة إلى ما يلي:

- إثراء المعرفة العلمية في مجال الأمن السيبراني.
- التعرف على المخاطر السيبرانية بما فيها انتهاك خصوصية المستهلكين من خلال التطرق الى حادثة شركة فايسبوك أنموذجا.
- تسليط الضوء على أهم الآليات المتبعة من قبل الشركات والمؤسسات الناشطة في مجال التجارة الالكترونية في التقليل من مخاطر التهديدات السيبرانية.

أهمية البحث:

يكتسي الموضوع أهمية بالغة نظرا لما يلي:

- أهمية الأمن السيبراني في الوقت الراهن، إذ يلعب دورا حاسما في نجاح واستدامة التجارة الالكترونية.
- أهمية موضوع الجرائم السيبرانية بما فيها انتهاك خصوصية المستهلكين التي أضحت تهدد أمن الأفراد واستمرار المؤسسات.
- أهمية أمان الأنظمة وبيانات ومعلومات المستخدم في التجارة الالكترونية.

من أجل الإجابة على التساؤلات المطروحة اعتمدنا في البحث على المنهج الوصفي الذي يتناسب مع موضوع الدراسة من أجل تعريف مصطلح الأمن السيبراني وخصوصية المستهلك، وكذا التعرف على أهم الانتهاكات في الفضاء السيبراني وأفضل الآليات المتبعة لخفض مختلف المخاطر من خلال التطرق إلى نموذج واقعي، وصولاً بذلك إلى تحليل وتفسير، حيث أنه في بعض أجزاء البحث قمنا بتكوين القاعدة النظرية المستقاة من مختلف المراجع، بالإضافة إلى اعتماد بعض الإحصائيات الميدانية، ولهذا الأسلوب الوصفي يعتبر مناسباً لتقرير الحقائق والتعريف بمختلف المفاهيم.

1- مفهوم الأمن السيبراني :

تناولت الدراسات والمعاجم اللغوية العربية والأجنبية كلمة "الأمن" فعدته مرادفاً للطمأنينة، أو نقيضاً للخوف أو مساوياً لانتفاء الخطر، وهو مفهوم نسبي متغير يتسع ويضيق وفقاً لطرق تناوله، كما أنه مفهوم مركب ذو مستويات عدة: "فردية، قومية، إقليمية، دولية" (الحري، 2008، ص 30).

وبهذا بعد ظهور الانترنت وتطور التكنولوجيا وأنظمة الاتصالات أصبحنا نتحدث عن أمن آخر يسمى الأمن السيبراني، إذ يعتبر مصطلح الأمن السيبراني **Cyber Security** واحداً من المصطلحات التي تعرف تعدداً في التعريفات المقدمة له، فمصطلح سيار **Cyber** هو لفظ يوناني الأصل، مشتق من كلمة **Kybernetes** ؛ بمعناها القيادة أو التحكم، مصدرها **Cybernetics** يعني: "علم الاتصالات وأنظمة التحكم الآلي في كل من الآلات والأشياء الحية" (Lehto et Neittaanmaki, 2015, p. 8).

كما قدمت وزارة الدفاع للولايات المتحدة الأمريكية تعريفاً لمصطلح الأمن السيبراني، أين اعتبرته: "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها (الإلكترونية والمادية) من مختلف الجرائم، الهجمات، التخريب، والتجسس، والحوادث". (Ventre, 2011, p.103).

➤ أهداف الأمن السيبراني:

- تأمين الفضاء الإلكتروني بما فيه المعاملات الرقمية بمختلف أنواعها.
- الحفاظ على سرية المعلومات وقصر النفاذ على الجهات المصرح لها فقط.
- الحفاظ على سلامة البيانات والبرامج وعدم فساد حالتها.
- احترام الخصوصية الرقمية للمستخدمين والمتعاملين الإلكترونيين.
- الحفاظ على توافر تقديم الخدمات الإلكترونية بشكل مستمر وبدون انقطاع أو تدهور.

- ضمان الصدق في التصرفات الإلكترونية والاستدلال على الفاعل من خلال تتبع الأثر.
- الوصول إلى الوضع الأمثل لأداء نظام المعلومات جنبا إلى جنب مع مستوى أداء الأمن المطلوب.
- خلق الثقة في التطبيقات والمعاملات الإلكترونية.
- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة (الإتحاد الدولي للاتصالات، 2009، ص 101).

1-1 عناصر الأمن السيبراني:

يمكننا تعريف عناصر الأمن السيبراني بأنها مجموعة العناصر الواجب توافرها للحماية المطلوبة، بحيث يُغطي كل عنصر من هذه العناصر جانبا من جوانب الحماية فتتکامل هذه العناصر فيما بينها، وفي حال فقد أي منها سيكون هناك خلل أمني، وتتمثل هذه العناصر فيما يلي:

• سرية البيانات: (Confidentiality)

إن سرية البيانات الشخصية والسرية الرقمية هي من حقوق الإنسان الأساسية، فهي تعني الحفاظ على سرية البيانات وتدفق المعلومات والمعاملات والخدمات أو الإجراءات التي تجري في الفضاء السيبراني ومنع الوصول إلى البيانات إلا من الأشخاص المصرح لهم فقط.

وتعني أيضا الحفاظ على المعلومات والبيانات من أن يُطلع عليها، حيث يمكن تنفيذ السرية عن طريق مراقبة النفاذ والتشفير. حيث أن التشفير يساعد على حماية البيانات أثناء تخزينها أو معالجتها أو عند نقلها عبر وسائل الاتصال.

• التكنولوجيا المستخدمة: (Technology Used)

يعني الخدمة التي من خلالها يمكن الحفاظ على المعلومات والبيانات من التعديل أو الحذف أو الإضافة أو إعادة التركيب أو التوجيه طالما أنها إلكترونية، وهذا بفضل دقة الأنظمة المعالجة لها وسلامتها من التلاعب أو التغيير ويتطلب ذلك أن تعمل الأجهزة والبرامج وأنظمة الشبكات بانسجام تام للمحافظة على المعلومات والبيانات ومعالجتها ونقلها ومراقبتها، وهذا الأمر من المفروض أن يولد الثقة لدى المتعامل. وللحيلولة دون التلاعب، يلزم وجود طريقة للتصديق على أنها لم تتعرض للتعديل أثناء الخزن أو النقل.

بالإضافة إلى سلامة ومتانة البنية التحتية من خلال وجود المعدات التكنولوجية والأجهزة الفنية التي توفر الحماية التقنية ضد الأعطال والقصور في الموارد الأصلية وغالبا ما تعمل هذه المكونات بشكل آلي دون التدخل البشري.

• التوافر والديمومة (Availability):

خدمة التوافر هي الخدمة التي تحمي النظام ليبقى متاحا دائما وهي موجهة خصيصا إلى أي خلل أو هجوم يمكن أن يؤدي إلى عدم التوافر، ومن الأمثلة على ذلك هجوم الفيروسات وهجمات حجب الخدمة أو منعها (Denial of Service - DoS) ويتطلب هذا في غالب الأحيان الحماية المادية التقنية، والهدف العام من عنصر التوافر والديمومة هو أن تكون الشبكة والأجهزة والأنظمة والبرامج والخدمات متاحة في جميع الأوقات التي يحتاج إليها المستخدم لتأمين توافر الخدمات والنظم والبيانات، يجب تحديد الأحجام المناسبة لنظم البنية التحتية، وتوفير الادارة التشغيلية للموارد والخدمات. بمعنى بقاء البيانات متوفرة للمستخدم وإمكانية الوصول إليها في أي وقت وعدم تعطل ذلك نتيجة لخلل في أنظمة إدارة قواعد البيانات أو وسائل الاتصال .

• تتبع الأثر (Traceability):

هي الخدمة التي من خلالها تضمن عدم إنكار أي شخص قام بتصرف ما متصل بالبيانات أو مواقعها على سبيل المثال: إذا منحت جهة معينة الصلاحية لجهة أخرى لشراء منتج معين ثم أنكرت بعد ذلك أنها منحت هذه الصلاحية فإن خدمة عدم الإنكار ستكشف ذلك، بمعنى توفر قدرة إثبات وقوع العملية التفاعلية. وكذلك قدرة الاستدلال على الفاعل وإمكانية الاقتفاء والقابلية للمراجعة لتحديد المسؤولية، كما يفترض مسبقا وجود آليات للتحقق من العمليات والإجراءات الإلكترونية في أوقات وتواريخ معينة عن طريق إلحاق بصمة التاريخ والوقت ويسمى هذا بقابلية التدقيق لدى النظام.

• احترام الخصوصية (Privacy):

بالنسبة لهذا العنصر هو موضوع ومحل دراستنا واهتمامنا في هاته المداخلة، له أهمية بالغة بحيث يُغطي جانبا من جوانب الحماية وواجب توافره للحماية المطلوبة.

أما بالنسبة لتعريف الخصوصية أو الحق في الحياة الخاصة فمن الصعب وضع تعريف جامع مانع لها لأن تعريف هذا الحق يرتبط بالتقاليد والثقافة والقيم الدينية السائدة والنظام السياسي في كل مجتمع".

وبهذا يمكن القول أن الخصوصية هي: "السرية وما تحمله من معان يمكن التعبير عنها بعدة ألفاظ منها العزلة والانطواء، والخلوة وعدم تدخل الآخرين وغير ذلك من المرادفات، ولهذا كان مفهوم الخصوصية نسبيا لأن ما يعد خاصا في زمان لا يكون كذلك في زمان آخر وما يمكن أن يكون خاصا في مكان لا يمكن أن يكون كذلك في مكان آخر" ¹ (ليطوش، 2019، ص 173)

أيضا الخصوصية تعبر عن حق المستهلك الإلكتروني في عدم نشر أو بث بياناته الشخصية التي تتعلق بتعاملاته أو بحياته الخاصة، ويتم ذلك بداية من طلبه كلمة السر خاصة به عند تسجيل حساب على الموقع الإلكتروني ومعاملاته الرقمية. وهناك عدة حلول تكنولوجية تُجرى استخدامها لتحقيق عملية خصوصية البيانات والمعلومات الشخصية للمستهلك.

من المفروض أن سياسة الخصوصية هي تبني وتعزيز ثقة الزبون في المتجر الإلكتروني، ومستوى هذه الثقة يؤثر في حجم ونوعية البيانات التي يحصل عليها المتجر الإلكتروني، والمستهلك لا يقدم بياناته ومعلوماته إلى المتاجر الإلكترونية إلا من أجل الحصول على قيمة، حيث أن المتجر الإلكتروني يسعى إلى الحصول على البيانات والمعلومات الدقيقة ذات المصادقية، ولا يتحقق هذا إلا بتحقيق ثقة الزبون في المتجر الإلكتروني.¹ (القحطاني، 2015، ص91)

بالنسبة للمحافظة على الخصوصية يكون من خلال عدم التمكن من الإطلاع على البيانات إلا من الأطراف المسموح لها بذلك، وكذا التحكم بعملية الدخول وأكثر طرق التحكم انتشارا هي استخدام كلمة المرور (Passwords) وجدار النار (Firewall)، إضافة إلى شهادات الترخيص (Authorization Certificates) مثل BBB الأمريكية (Business Better Bureau) وهي هيئة أمريكية إذا حصل أي صاحب موقع تجاري على هذه الشهادة سيحني من المال الكثير وذلك لأن هذه الشهادة بمقتضاها يدخل المشتري أو الزبون وهو متأكد 100% أنه لن يُنصب عليه.

2-1 مظاهر إنتهاك خصوصية المستهلك سيبرانيا :

كلما تتطور تكتيكات الدفاع الإلكتروني تتطور أيضا تهديدات الأمن السيبراني، حيث تتخذ البرامج الضارة والمخاطر الأخرى أشكالا جديدة من بينها:

- **الاختراقات وبرامج الفدية:** تتنوع أسباب قيام الهاكر بعمليات الاختراق للمنصات والتطبيقات والمواقع من أسباب سياسية للإطلاع على قرارات حساسة أو لإحداث حالات من الفزع في قطاعات مختلفة، كما يحدث في عمليات مهاجمة مزودات أسماء النطاقات التي تسفر عن تعطل عدد من المواقع على الانترنت، وهناك أسباب عسكرية وأسباب مالية بحتة من خلال الابتزاز المباشر، ما يعرف ببرامج الفدية Ransomware التي من المتوقع أن تصل إلى نحو ثلاثة ملايين هجمة خلال العام الجاري، وأن تصل مبالغ الفدية التي ستدفع إلى نحو 20 مليار دولار ، مقارنة بـ 11,5 مليار دولار في سنة 2019 بحسب مجلة "ساير كرايم".

وقد أشار الحويماني (2021) أنه "بلغت كمية الأموال التي تم بالفعل تحويلها إلى مجرمي برامج الفدية وتم الإفصاح عنها من قبل الضحايا في 2020 نحو 370 مليون دولار وهذا نحو 3,3 أضعاف ما كانت عليه في سنة 2019 بحسب شركة Chainalysis المتخصصة بتحليل سلاسل الكتل التي تعمل عليها العملات المشفرة، وهذه فقط الأرقام الرسمية المعلنة ولا تشمل طرق الدفع الأخرى خارج العملات المشفرة، ولا تشمل المدفوعات التي تتم بسرية حفاظا على سمعة الجهة أو الفرد،

وبحسب شركة الاستجابة للاختراقات Coveware بلغ متوسط الفدية المدفوعة في الربع الأول لسنة 2021 نحو 212 ألف دولار أعلى بنسبة ثلاثة وأربعون في المائة عن الربع السابق" (فقرة 14).

- **البرمجيات الخبيثة:** هي برامج ضارة بما في ذلك برامج التجسس وبرامج الفدية والفيروسات، عادة ما تخترق الشبكات من خلال ثغرة أمنية، مثل النقر على روابط البريد الإلكتروني المشبوهة أو تثبيت تطبيق مخوف بالمخاطر أو غير ذلك، حيث أنه بمجرد الدخول إلى الشبكة يمكن للبرامج الخبيثة الحصول على معلومات حساسة، ويمكنها أيضا حظر الوصول إلى مكونات شبكة الأعمال الحيوية .

- **التصيد الاحتيالي:** هو ممارسة إرسال اتصالات ضارة (عادة رسائل بريد إلكتروني) مصممة لتظهر من مصادر حسنة السمعة ومعروفة، حيث تستخدم أسماء وشعارات وما إلى ذلك لتقليل الشكوك وجعل الضحايا ينقرون على الروابط الضارة ، مثل بطاقة الائتمان أو الضمان الاجتماعي أو معلومات تسجيل الدخول...الخ.

- **هجوم (MitM):** تحدث هجمات (MitM) Man in the Middle عندما يقطع المجرمون حركة المرور بين المعاملات بين طرفين، على سبيل المثال : يمكن للمجرمين إدخال أنفسهم بين شبكة Wi-Fi عامة وجهاز الفرد بدون إتصال Wi-Fi محمي، كما يمكن لهم أحيانا عرض جميع معلومات الضحية دون علمه.

- **هجوم: (Zero-day)** أصبحت هذه الهجمات الأكثر شيوعا ، حيث تحدث حين الإعلان عن ثغرة أمنية في الشبكة وقبل تصحيحها، حيث يغتنم المجرمون الفرصة لشن هجمات قبل أن تتمكن الشركة أو المؤسسة من التوصل إلى تصحيح أمني.

- **لغة الاستعلام الهيكلية (SQL):** يعمل هذا التهديد عن طريق إدخال تعليمات برمجية ضارة في نموذج على موقع ويب أو تطبيق خاص بالشركة ما يسمح للمهاجم بالكشف عن المعلومات الحساسة.

- **الهندسة الاجتماعية:** هي عملية التلاعب النفسي بالناس لإفشاء معلومات شخصية، حيث يستغل المجرمون فضول الأشخاص أو ثقتهم، فمثلا التلاعب بالصوت حيث يأخذ مجرمو الانترنت صوت الشخص من مصادر مثل البريد الصوتي أو منشور على وسائل التواصل الاجتماعي ويتلاعبون به لأغراض أخرى¹. (البار، 2017، ص ص 4-5)

- **الملاحقة الحاسوبية:** في هذا الأسلوب يقوم المجرمون باستغلال الثغرات الموجودة في شبكات الانترنت وأنظمة تشغيل الحاسوب (مثل نظام ويندوز) في التمكن من التحكم في جهاز الحاسوب الخاص بالضحية ويتم ذلك من خلال بناء شبكة اتصال مباشرة بين جهاز المجرم وجهاز الضحية، مما يمكن المجرم من التلاعب في المحتويات والعمليات.

• **التجسس السيرياني:** لا يتم فقط في نطاق الصراعات السياسية، بل إنه يستخدم أيضا بكثافة في مجال التجسس الاقتصادي والصناعي من خلال سرقة أسرار تجارية لمنظمة ما وذلك بغرض تحقيق النفع لحكومة دولة أجنبية أو طرف آخر.

• **الابتزاز السيرياني:** هذا النوع من الجرائم يقوم القرصان باختراق قواعد بيانات إحدى المنظمات أو الأفراد والهدف من هذا هو ابتزاز الجهة المتعرضة للهجمة من أجل تحقيق منافع معينة، وقد تكون هذه المنافع في الغالب مالية أو سياسية أو تشغيلية أو أي منافع أخرى. (Livanis, 2016, P 85)

2- تعرض شركة فايسبوك (Facebook) لانتهاك خصوصية مستخدميها:

1-2 تعريف شركة فايسبوك:

البعض يطلق على فايسبوك الأب الروحي للشركات الناشئة، نظرا لأنه بدأ صغيرا عام 2003 من غرفة طالب اسمه مارك زوكربيرج كان هدفه هو تسهيل عملية التواصل بين زملائه في جامعة هارفارد الأمريكية في عام 2012 تجاوز عدد مستخدمي الفايسبوك عتبة المليار مستخدم.

الشركة العملاقة فايسبوك هي أكبر شركة اجتماعية في العالم حاليا بأكثر من 2,45 مليار مستخدم يقع المقر الرئيسي لها في مينلو بارك في كاليفورنيا الولايات المتحدة الأمريكية، يعود تأسيسها لسنة 2004، لدى الشركة حاليا مكاتبها في 70 مدينة حول العالم و44.942 موظفا و15 مركزا للبيانات حول العالم، يعمل الفايسبوك كشركة للتواصل الاجتماعي حول العالم وتشارك في تطوير تطبيقات الوسائط الاجتماعية لإتاحة الفرصة للمستخدمين للاتصال من خلال الأجهزة المحمولة وأجهزة الكمبيوتر الشخصية، تمكن الشركة المستخدمين من مشاركة الآراء والأفكار والصور ومقاطع الفيديو ومختلف الأنشطة منها التجارية عبر الانترنت، تكسب الشركة حوالي 85 % من أموالها من الإعلانات في عام 2017 كسبت الشركة حوالي 39,9 مليار دولار من إيرادات الإعلانات.¹ (الموقع الإلكتروني: <https://ar.m.wikipedia.org>، 12-05-2023)

فايسبوك وتحدي خصوصية المستخدمين: على الرغم من أنه من المستحيل تحديد الطرق التي ساعد بها فايسبوك الأشخاص على التواصل، إلا أنه الآن لا يعد وسيلة بريئة للتواصل أو على الأقل وسيلة آمنة، وأظن أننا تعلمنا أمرا أو اثنين حول خصوصية البيانات، وكيف يتعامل فايسبوك مع بيانات مستخدميها وأمانها هذا الجانب من فايسبوك كان موجود منذ فترة ليست بالقصيرة، والعديد من خبراء تكنولوجيا المعلومات أبدوا تخوفهم منه من قبل، لكنه بدأ في التجلي والظهور بشكل أكبر عندما فُتح أكثر من تحقيق في فضيحة تسريب بيانات المستخدمين الشخصية، والتي كان المسؤول عنها شركة Cambridge Analytica (وهي شركة استشارات سياسية بريطانية) في هذه الفضيحة تم الوصول إلى معلومات خاصة بـ: 87 مليون مستخدم من مستخدمي الفايسبوك بدون علمهم، واكتشفت شركة متخصصة في الأمن السيرياني أن بيانات 540 مليون مستخدم لم تكن محمية من قبل فايسبوك، هذه الحادثة أثرت على فايسبوك كثيرا وأفقدته ثقة العديد من مستخدميها حول العالم، لكنه لم ينهار بشكل كامل بل

تعافى، وبعد هذه الحادثة كل من مارك زوكربيرج وإدارة فايسبوك قدموا وعودا للمستخدمين بعدم تكرار هذا الحادث مجددا.¹ (بن زايد، 2021، ص 30)

الحادثة المذكورة أعلاه، أدت إلى رفع دعاوى قضائية أطلقت في عام 2018 للمطالبة بتعويضات من شركة فايسبوك العملاقة المتهمه بالسماح لأطراف ثالثة بما في ذلك شركة "كومبريدج أناليتيكا" بالوصول إلى بيانات المستخدمين دون علمهم واستخدامها لأغراض سياسية، حيث وافق محامو الدفاع في وثيقة قضائية تم رفعها إلى محكمة سان فرانسيسكو أن شركة فايسبوك وافقت على دفع مبلغ 725 مليون دولار تعويضا للضحايا، ومنذ اندلاع هاته الفضيحة أغلقت شركة كامبريدج أناليتيكا، وأزالَت شركة فايسبوك الوصول إلى بياناته من آلاف التطبيقات المشتبه في إساءة استخدامها، وقيد كمية المعلومات التي يمكن للمطورين الوصول إليها بشكل عام، كما سهّل على المستخدمين معايير قيود مشاركة البيانات الشخصية¹. (الموقع الإلكتروني: Euronews، 19-05-2023 <https://arabic.euronews.com>).

2-2 أهم الآليات المتبعة لخفض المخاطر السيبرانية للمؤسسات والشركات:

- بعد الانتهاء من إجراءات تشخيص وتقييم المخاطر السيبرانية، يمكن للمؤسسات والشركات وضع خطة لخفض تلك المخاطر لسد الفجوة بين وضعيتها الحالية من ناحية الأمن السيبراني وبين القدرات السيبرانية اللازمة لتصحيح مواضع القصور.
- ينبغي أن تكون جهود خفض المخاطر بقيادة وتضافر جهود كفاءات مختصة في مجال الأمن السيبراني وذات مكانة عالية في درجات المؤسسات لتقديم التوجيهات وتنسيق الإجراءات ومراقبة تنفيذ الخطة وتقييم النتائج وتحقيق وتصحيح مواضع القصور.
- تحديد الموارد اللازمة وترتيبها حسب الأولويات المطلوبة وتركيزها على الأصول عالية القيمة وعلى الأنظمة ذات الأثر العالي التي تتطلب مستويات إضافية من الحماية وعلى الجهات الأكثر حساسية في اعتمادها على التقنية الرقمية مثل الشركات والبنى التحتية ومختلف الخدمات وهذا من خلال فهم نقط ضعفها وإعطاء الأولوية للإجراءات الأمنية المناسبة والمتناسبة مع الخطر.
- تحديد الأمور المعرضة للخطر و زيادة الوعي العام بالمخاطر في جميع مستويات المؤسسة من القادة إلى العامل العادي، حيث أنه لا يمكن إعطاء الأهمية للأمن من دون أن يفهموا أولا مدى تعرض نشاطاتهم اليومية (وليس مجرد معلوماتهم الشخصية) للخطر، بالتالي ينبغي أن تبادر المؤسسات بزيادة الوعي العام وتعزيز التعليم والتدريب وتنمية المهارات وتمكين المستخدمين ليصبحوا جزءا من الحل ببناء ثقافة قوية للأمن السيبراني.
- إعداد أطر عمل قانونية وتنظيمية مناسبة للحماية من الجريمة السيبرانية.
- استعمال نطاق واسع من الأدوات، بما فيها السياسات والتشريعات والأنظمة والمعايير من أجل زيادة مستوى الثقة في استخدام تقنيات المعلومات والاتصال.

- تصحيح مواضع القصور في العمليات والمنتجات مثل توجيه الشبكات وأنظمة المعلومات.

- المراقبة المستمرة للكشف عن التهديدات السيبرانية التي قد تصيب المؤسسة واستعمال أحدث التقنيات لصدها واحتوائها.

- تخصيص الموارد المادية والبشرية اللازمة لخفض المخاطر بمعنى تمويل كافٍ بميزانية مخصصة وأفراد محلية ذات كفاءة، بالإضافة إلى العلاقات والشراكات المطلوبة للتنفيذ الناجح لخطط خفض المخاطر.

- التعاون بين المؤسسات والسلطات عبر الدول المختلفة على المستوى الوقائي من خلال تبادل الخبرات والتقنيات والتكنولوجيا الحديثة لمنع وتوقي ارتكاب الأنواع الخطيرة من الجرائم السيبرانية.

- بما أن الأمن السيبراني يتقاطع معه العديد من المجالات الأخرى مثل التنمية الاقتصادية، التجارة، ضبط الأسلحة، حقوق الإنسان، الاستعمال المزدوج للتقنيات، الاستقرار، الأمن، السلام وحل النزاعات ينبغي تضافر جهود جميع أصحاب المصلحة في التخطيط للدفاع بشكل أفضل ولتعيين الموارد البشرية والمالية لخفض تلك المخاطر (هاثاواي، 2018، الفقرة 39).

خاتمة :

لا يقتصر نجاح أعمال التجارة الالكترونية في أي بلد على القوة المالية وحجم النشاط أو الهيكل الضخم للمؤسسات والشركات أو إصدار مجموعة من القوانين وحسب، بل يجب العمل على تطوير رزمة من المجالات الأخرى أولها ما يتعلق بعناصر الأمن السيبراني وفي مقدمته ما يخص حماية خصوصية المستهلكين، فالتعامل في الفضاء السيبراني محفوف بالمخاطر والجرمين نظرا للانفتاح على مختلف الأسواق، والمساس بخصوصية المستهلكين هو أخطر بكثير للمؤسسات والشركات لذا سلامة المعاملات يعني سلامة المؤسسات والأشخاص، وهذا ما يوجب وضع سياسة أمنية سيبرانية تضمن استمرارية التعامل بين الأطراف وتحافظ على الصورة الذهنية الجيدة.

نتائج الدراسة:

توصلت الدراسة إلى مجموعة من النتائج أهمها :

- الأمن السيبراني هو الحقل الذي يدرس طرق حماية البيانات والمعلومات بمختلف أشكالها (شخصية، مؤسسية، دولية...) المخزنة في أجهزة الحاسوب إضافة إلى الأجهزة الملحقه وشبكات الاتصالات وغير ذلك وهذا لأجل التصدي للمحاولات الرامية إلى الدخول غير المشروع إلى مختلف قواعد البيانات المخزنة أو تلك التي ترمي إلى سرقتها أو نقلها أو تغييرها أو تخريبها أو انتهاكها.

- العناصر الواجب توافرها للحماية المطلوبة في الفضاء السيبراني لا تتأني إلا من خلال: سرية البيانات، التكنولوجيا، التوافر والديمومة، تتبع الأثر، احترام الخصوصية.

- تعامل المؤسسة مع المستهلكين في الفضاء السيبراني واتماها على بياناتهم ومعلوماتهم الشخصية مسؤولية أخلاقية قانونية تلزمها الحفاظ على السرية واحترام الخصوصية.
- بحسب تجربة شركة فايسبوك العملاقة فإن انتهاك خصوصية المستهلك والمساس بحياته الخاصة في الفضاء السيبراني بمختلف الأشكال (اختراقات، سرقة البيانات، تشويه أو تعديل البيانات، تجسس، تهديدات، تشهير، ابتزاز، برامج خبيثة، فيروسات،...الخ) أخطر بكثير للمؤسسة أو الشركة، وبإمكانه التسبب في فقدان الزبائن وتوقفهم عن التعامل أو حتى التعطل و الإفلاس.
- الجرائم السيبرانية هي عابرة للحدود، مستمرة، ترافق الأفراد والمؤسسات على مر الزمن، ما يجعل عمليات والمراقبة والتشخيص والتقييم باستمرار من أهم المهام وأولويات الوقاية وخفض المخاطر.
- التربع على عرش النجاح لا يعني عدم وجود تحديات أو تهديدات، ومهما كانت القوة المالية والهيكلية للمؤسسة أو الشركة وترتيبها العالمي من حيث الحجم والنشاط والدخل والتكنولوجيا المستخدمة فهي عرضة لأي هجوم أو تهديد سيبراني لمجرمين مختفين وراء الحواسيب.
- كلما زادت المخاطر السيبرانية وانتهاكات خصوصية المستهلكين كلما انعكس سلبا على استمرارهم في التعامل إلكترونيا مع المؤسسة أو الشركة.
- كلما زادت المخاطر أو الجرائم السيبرانية كلما زادت النفقات المتعلقة بإجراءات الحماية لدفع تلك المخاطر وسد الثغرات الأمنية التكنولوجية الخاصة بالمؤسسات والشركات.

التوصيات :

- يجب على المؤسسات والشركات ذات البنى التحتية الرقمية الإسراع في بناء إستراتيجية فعالة بتطوير آليات أمنية للوقاية وخفض المخاطر والتهديدات السيبرانية.
- ضرورة اتخاذ المؤسسات والشركات تدابير وإجراءات تنظيمية وقانونية تعتمد على الأمن السيبراني كعنصر ضروري في التعاملات الإلكترونية.
- ضرورة التحديث المستمر للتقنيات والنظم والبرامج المضادة للاعتداءات والفيروسات.
- ضرورة المراقبة والتقييم المستمر والتعاون بين المؤسسات في المجال التقني، التكنولوجي، الأمني، التنظيمي....الخ للوقاية والتقليل من مخاطر التهديدات والهجمات السيبرانية والاستفادة من التجارب السابقة.
- احترام خصوصية المستهلك والحرص على إرضاءه هو سر بقائه واستمراره في التعامل مع المؤسسة.

قائمة المراجع:

- الإتحاد الدولي للاتصالات (ITU)، (2009)، دليل الأمن السيبراني للبلدان النامية، تم الاسترجاع من موقع : <https://www.itu.int/en/ITU>
- سليمان عبد الله الحربي، "مفهوم الأمن : مستوياته وتحدياته دراسة نظرية في المفاهيم والأطر" المجلة العربية للعلوم السياسية، العدد 19، 2008.
- دليلة لبطوش، الحماية القانونية للحق في الخصوصية الرقمية للمستهلك الإلكتروني، مجلة العلوم الإنسانية، المجلد ب، العدد 52، 2019، ص 173.
- ذيب بن عايش القحطاني، أمن المعلومات، دار قابس للطباعة والنشر والتوزيع، لبنان، 2015، ص 91.
- بن زايد مبارك، مختاري فتيحة، سعداوي مراد مسعود، المؤسسات الناشئة بين مشروع التأسيس وتحديات الواقع، مجلة حوليات جامعة بشار في العلوم الاقتصادية، المجلد 08، العدد 02، 2021، ص 30.
- مصطفى البار، أمن المعلومات والأمن السيبراني، 2017.
- ميليسيا هاثاواي، "إدارة الخطر السيبراني الوطني، 2018.
- الموقع الإلكتروني wikipedia ، 12-05-2023، تم الاسترجاع من موقع: <https://ar.m.wikipedia.org>.
- الموقع الإلكتروني: Euronews ، 19-05-2023، تم الاسترجاع من موقع: <https://arabic.euronews.com>.
- Daniel Ventre, (2011). Cyber attaque et cyber défense.
- Martti Lehto, Pekka Neittaanmaki, (2015). Cyber Security : Technology and Automation edition springer.
- Livanis, (2016) .