كلية الشريعة والقانون بدمنهور

جامعة الأزهـــر

مـــجلة البحوث الفقهية والقانونية

مجلة علمية محكمّة
تصدرها كلية الشريعة والقانون بدمنهور

بحث مستل من

العدد السابع والأربعين ـ "إصدار أكتوبر ٢٠٢٤م ـ ١٤٤٦هـ"

دور الأمن السيبراني في حماية أطراف عقود التجارة الإلكترونية

The Role Of Cybersecurity In Protecting Parties To E-Commerce Contracts

الدكتـــــور

محمد إبراهيم عبد المنعم مرسي

دكتوراه القانون التجاري والبحري
كلية الحقوق جامعة الإسكندرية

التاريخ: 2024/10/20

الرقم: L24/0260 ARCIF

سعادة أ. د. رئيس تحرير مجلة البحوث الفقهية و القانونية المحترم

جامعة الأزهر، كلية الشريعة و القانون، دمنهور، مصر

تحية طيبة وبعد،،،

يسر **معامل التأثير والاستشهادات المرجعية للمجلات العلمية العربية (ارسيف – ARCIF)**، أحد مبادرات قاعدة بيانات "**معرفة**" للإنتاج والمحتوى العلمي، إعلامكم بأنه قد **أطلق التقرير السنوي التاسع للمجلات للعام 2024**.

يخضع معامل التأثير "ارسيف Arcif" لإشراف "مجلس الإشراف والتنسيق" الذي يتكون من ممثلين لعدة جهات عربية ودولية: (مكتب اليونيسكو الإقليمي للتربية في الدول العربية ببيروت، لجنة الأمم المتحدة لغرب آسيا (الإسكوا)، مكتبة الاسكندرية، قاعدة بيانات معرفة). بالإضافة للجنة علمية من خبراء وأكاديميين ذوي سمعة علمية رائدة من عدة دول عربية وبريطانيا.

ومن الجدير بالذكر بأن معامل "**ارسيف Arcif**" قام بالعمل على فحص ودراسة بيانات ما يزيد عن (**5000**) عنوان مجلة عربية علمية أو بحثية في مختلف التخصصات، والصادرة عن أكثر من (**1500**) هيئة علمية أو بحثية في العالم العربي. ونجح منها (**1201**) مجلة علمية فقط لتكون معتمدة ضمن المعايير العالمية لمعامل "**ارسيف Arcif**" في تقرير **عام 2024**.

ويسرنا تهنئتكم وإعلامكم بأن **مجلة البحوث الفقهية و القانونية** الصادرة عن **جامعة الأزهر، كلية الشريعة و القانون، دمنهور، مصر، قد نجحت في تحقيق معايير اعتماد معامل "ارسيف Arcif"** المتوافقة مع المعايير العالمية، والتي يبلغ عددها (**32**) **معياراً**، وللاطلاع على هذه المعايير يمكنكم الدخول إلى الرابط التالي: http://e-marefa.net/arcif/criteria/

وكان **معامل "ارسيف Arcif" العام** لمجلتكم لسنة 2024 (**0.3827**). ونهنئكم بحصول المجلة على:

- **المرتبة الأولى** في **تخصص الدراسات الإسلامية** من **إجمالي عدد المجلات** (**103**) على المستوى العربي، مع العلم أن **متوسط معامل "ارسيف" لهذا التخصص** كان (**0.082**). كما صُنفت مجلتكم في هذا التخصص ضمن الفئة (**Q1**) وهي الفئة العليا .
- كما صُنفت مجلتكم في **تخصص القانون** من **إجمالي عدد المجلات** (**114**) على المستوى العربي ضمن الفئة (**Q2**) وهي الفئة الوسطى المرتفعة ، مع العلم أن **متوسط معامل "ارسيف" لهذا التخصص** كان (**0.24**).

راجين العلم أن حصول أي مجلة ما على مرتبة ضمن الأعلى (10) مجلات في **تقرير معامل "ارسيف" لعام 2024** في أي تخصص، لا يعني حصول المجلة بشكل تلقائي على تصنيف مرتفع كتصنيف فئة Q1 أو Q2، حيث يرتبط ذلك بإجمالي قيمة النقاط التي حصلت عليها من **المعايير الخمسة المعتمدة لتصنيف مجلات تقرير"ارسيف" (للعام 2024) إلى فئات في مختلف التخصصات**، ويمكن الاطلاع على هذه المعايير الخمسة من خلال الدخول إلى الرابط: http://e-marefa.net/arcif /

وبإمكانكم الإعلان عن هذه النتيجة سواء على موقعكم الإلكتروني، أو على مواقع التواصل الاجتماعي، وكذلك الإشارة في النسخة الورقية لمجلتكم إلى معامل "**ارسيف Arcif**" الخاص بمجلتكم.

ختاماً، في حال رغبتكم الحصول على شهادة رسمية إلكترونية خاصة بنجاحكم في معامل "**ارسيف**"، نرجو التواصل معنا مشكورين.

وتفضلوا بقبول فائق الاحترام والتقدير

أ.د. سامي الخزندار

رئيس مبادرة معامل التأثير

" ارسيف Arcif"

مجلـة البحـوث الفقهيـة والقانونيـة
مجلة علمية عالمية متخصصة ومُحكمة
من السادة أعضاء اللجنة العلمية الدائمة والقارئة
في كافة التخصصات والأقسام العلمية بجامعة الأزهر

المجلة مدرجة في الكشاف العربي للإستشهادات المرجعية ARABIC CITATION INDEX
على Clarivate Web of Science
المجلة مكشّفة في قاعدة معلومات العلوم الإسلامية والقانونية من ضمن قواعد بيانات دار المنظومة
المجلة حاصلة على تقييم ٧ من ٧ من المجلس الأعلى للجامعات
المجلة حاصلة على المرتبة الأولى على المستوى العربي في تخصص الدراسات الإسلامية
وتصنيف Q2 في تخصص القانون حسب تقييم معامل "ارسيف Arcif" العالمية
المجلة حاصلة على تقييم ٨ من المكتبة الرقمية لجامعة الأزهر

رقم الإيداع
٦٣٥٩

الترقيم الدولي
(ISSN-P): (1110-3779) - (ISSN-O): (2636-2805)

للتواصل مع المجلة
+201221067852
journal.sha.law.dam@azhar.edu.eg

موقع المجلة على بنك المعرفة المصري
https://jlr.journals.ekb.eg

دور الأمن السيبراني في حماية أطراف عقود التجارة الإلكترونية

The Role Of Cybersecurity In Protecting Parties To E-Commerce Contracts

الدكتـــــور

محمد إبراهيم عبد المنعم مرسي

دكتوراه القانون التجاري والبحري

كلية الحقوق جامعة الإسكندرية

دور الأمن السيبراني في حماية أطراف عقود التجارة الإلكترونية

محمد إبراهيم عبد المنعم مرسي
قسم القانون التجاري والبحري، كلية الحقوق، جامعة الإسكندرية، مصر.
البريد الإلكتروني: mohamedebrahimmorsy@hotmail.com

ملخص البحث:

تتعامل منصات ،وشركات التجارة الإلكترونية مع بيانات العملاء الحساسة مثل المعلومات الشخصية ،وتفاصيل بطاقة الائتمان، والتي يمكن الاستيلاء عليها ، واستغلالها من قبل المتسللين ،ومجرمي الإنترنت، ولذلك يجب علي الشركات ، ومنصات التجارة الإلكترونية الالتزام بتدابير ،وإجراءات الأمن السيبراني لحماية المتعاقدين في التجارة الإلكترونية، وإتمام عقودها ،لما يحققه الأمن السيبرانى من فوائد متعددة للشركات ،والتجار، والعملاء ،ولتبادل الثقة بينهم ،ويتوقع المتعاقدين في التجارة الإلكترونية أن توفر لهم المنصات ،والشركات التجارية عبر الإنترنت تجربة تسوق آمن، وموثوق به، ويتسوق العملاء تسوق أمن عبر منصات التجارة الإلكترونية الملتزمة بالأمن السيبرانى، الذي يجذب المستهلكين ،والعملاء، للتعامل ،والتعاقد مع تلك المنصات الأمنة، ومع انتشار تعاملات، وتنوع التجارة الإلكترونية ظهرت أنواع جديدة من الجرائم الإلكترونية، التي تتغير ،وتتطور باستمرار، مما يشكل تحديات للأمن السيبراني، فأصبح مجرمو الإنترنت أكثر تطوراً، وابتكاراً في الأساليب، والتقنيات في شن الهجمات الإلكترونية، ويستهدفون التقنيات الجديدة، ولذلك اصبح الأمن السيبرانى ضروري ،وحتمي لحماية المتعاقدين في التجارة الإلكترونية.

الكلمات المفتاحية: الأمن السيبرانى، عقود التجارة الإلكترونية، حماية المتعاقدين ، الشركات ، والعملاء، الجرائم الإلكترونية.

The Role Of Cybersecurity In Protecting Parties To E-Commerce Contracts

Mohamed Ebrahim Morsi
Department of Commercial And Maritime, Faculty Of Law, Alexandria University, Egypt.
E-mail: mohamedebrahimmorsy@hotmail.com

Abstract:

E-commerce platforms and companies deal with sensitive customer data, such as personal information and credit card details, which can be seized and exploited by hackers and cybercriminals. Therefore, companies and e-commerce platforms must adhere to cybersecurity measures and procedures to protect contractors in e-commerce And the completion of its contracts, due to the multiple benefits that cybersecurity brings to companies, merchants, and customers, and to exchanging trust between them, and contractors in e-commerce expect that platforms and online commercial companies will provide them with a safe and reliable shopping experience, and customers will shop safely through committed e-commerce platforms. With cybersecurity, which attracts consumers and clients to deal and contract with these secure platforms, and with the spread of transactions, With the diversity of e-commerce, new types of cybercrimes have emerged, which are constantly changing and evolving, which poses challenges to cybersecurity. Cybercriminals have become more sophisticated and innovative in methods and techniques for launching cyberattacks, and they target new technologies. Therefore, cybersecurity has become necessary and inevitable to protect ,Ecommerce contractors.

Keywords: Cybersecurity, E-Commerce Contracts, Protection Of Contractors, Companies, And Customers, Cybercrime.

مقدمة

أصبحت معاملات التجارة الإلكترونية جزء لا يتجزأ من حياتنا اليومية ،وتعتبر منصات التجارة الإلكترونية سوق مفتوحة للشركات، والتجار لممارسة أعمالهم التجارية ،وتنميتها عبر الإنترنت، كبيع المنتجات ،وتسويق الخدمات، ويعد أمان المنصات ،والمتاجر الإلكترونية أهم وسيلة لحماية بيانات المتعاقدين في التجارة الإلكترونية، وركن أساسي لنجاح عقود التجارة الإلكترونية، و بناء الثقة بين العملاء ،ومنصات التسوق الإلكتروني، ويتمثل أمان تلك المنصات ،والمتاجر في تدابير، وإجراءات الأمن السيبرانى.

ويعتبر الأمن السيبراني جزءًا حيويًا، ومتكاملًا في عقود التجارة الإلكترونية، لأنه يحمى اطراف التعاقد من الهجمات الإلكترونية، حيث تؤدي الهجمات السيبرانية إلى تعريض بيانات شركات، وعملاء التجارة الإلكترونية ،وسمعتهم ،وأرباحهم للخطر، فضلاً عن فقدان الثقة بينهم، لذلك يجب أن تكون منصات ،ومتاجر التجارة الإلكترونية استباقية ،ويقظة في تنفيذ تدابير الأمن السيبراني الفعالة، وتقديم للعملاء تجربة تسوق آمنة بتبنيها تدابير الأمن السيبراني ،وتحدّيثها لمواكبة تقنيات ،وأدوات الهجوم الإلكترونية الجديدة ،والمتطورة؛ لأن المجرمون يستخدمون أدوات جديدة ، ويبتكرون استراتيجيات جديدة للوصول إلى الأنظمة بدون إذن، وبيانات ،ومعلومات المتعاقدين، وتضر الهجمات الإلكترونية المنصات ،والشركات، والمتعاقدين فى التجارة الإلكترونية من خلال وسائل مختلفة، مثل التصيد الاحتيالي ،أو البرامج الضارة، و تسبب تلك الأفعال عدم رضا العملاء، أو فقدان المبيعات ،أو الإضرار بسمعة الشركة، أو تسريب بيانات شركات التجارة الإلكترونية ،كمعلومات العميل ، أو تفاصيل المنتج ،أو سجلات المعاملات.

لـذلك يعتـبر الأمـن الـسيبراني عنـصر حيـوي،لأمـان المتعاقـدين في التجـارة الإلكترونية؛ وإتمام عقودهم، لأنه يحمى البيانات ،ويحافظ عليها ،و لة فوائد عديدة، فإلى جانـب حمايـة بيانـات المتعاقـدين ، حمـايتهم أيـضا مـن الخـسارات الماديـة ، وانتحال الشخصية، وبناء الثقة بين المتعاقدين ،ومنصات التسوق الإلكتروني، فيعتبر عامل أساسي في حياة المتعاقدين في مجال التجارة الإلكترونية؛ لحمايـة معـاملاتهم من الهجمات الخبيثة التي قد تحاول اسـتغلال نقـاط ضـعف في أنظمـة الـشركات، و سرقة البيانات، والمعلومات، و تعطيل عملياتها.

أهداف البحث:

يهدف البحث ألي بيـان دور الأمـن الـسيبرانى، في حمايـة المتعاقـدين في التجـارة الإلكترونيـة ، وتوضـيح تقنيـات الأمـن الـسيبرانى، و سـبلة في حمايـة اطـراف عقـود التجـارة الإلكترونيـة، وذلـك لانتـشار عقـود التجـارة الإلكترونيـة، وتوضـيح دورة في تسهيل حركة التجارة الإلكترونية ،و حماية المتعاقدين.

إشكالية البحث:

تدور مشكلة الدراسة حول قدرة الأمن السيبراني على تأمين المتعاقدين في التجارة الإلكترونيـة، كحمايـة بيانـاتهم ومعلومـاتهم الشخـصية، مـن خـلال تـأمين منـصات التجارة الإلكترونية، والمتاجر مما يجعل المتعاقد يثق في تلك المنصات .

منهج البحث:

سـوف نتنـاول بعـض الفرضـيات القانونيـة مـع الإجابـة عـلى بعـض الأسـئلة حـول المقصود بالأمن السيبرانى ، وأهدافه ، وفعالية الأمن السيبرانى في حماية المتعاقدين في التجارة الإلكترونية ،والفوائد التي تعود علي التجارة الإلكترونية من الالتزام بقواعد الأمـن الـسيبرانى متبعـين المـنهج التحلـيلي، عـن طريـق تقـسيم إشـكالية البحـث ألي

مبحثين نستعرض فيهم ماهية الأمن السيبرانى في التجارة الإلكترونية ، وسبل حماية المتعاقدين بالأمن السيبرانى في التجارة الإلكترونية .

خطة البحث

المبحث الأول: ماهية الأمن السيبرانى.

المطلب الأول: المقصود بالأمن السيبرانى.

المطلب الثانى: تقنيات الأمن السيبرانى.

المبحث الثانى: دفاع الأمن السيبرانى عن المتعاقدين في التجارة الإلكترونية.

المطلب الأول: سبل الأمن السيبرانى في حماية أطراف عقود التجارة الإلكترونية

المطلب الثانى: الوسائل القانونية لمكافحة الجرائم الإلكترونية.

المبحث الأول
ماهية الأمن السيبرانى

تمهيد وتقسيم:

تبحث الشركات باستمرار عن حلول مجدية ،وقابلة للتكيف بسهولة لتقليل مخاطر حوادث الهجمات الإلكترونية ، وهذا يعني ان هناك حاجة متزايدة للحلول التي تساعد منصات التجارة الإلكترونية على حماية البيانات ،وتخزينها بشكل آمن، حيث تحتاج إلى حلول تساعدها على توفير الأمان وفقًا لاحتياجاتها، متمثلة في الأمن السيبرانى ،سنقسم المبحث كالتالي:

المطلب الأول: المقصود بالأمن السيبرانى.

المطلب الثانى: تقنيات الأمن السيبرانى.

المطلب الأول
المقصود بالأمن السيبرانى

تمهيد وتقسيم:

يعد الأمن السيبراني في الوقت الحالي أهم عناصر الأمن في الدول المتحضرة ،وخاصةً مع التحول ألي الأنظمة الإلكترونية في كافة جوانب الحياة، وتقوم فكرة الأمن السيبراني على تأمين البنية التحتية المعلوماتية للمنصات، والشركات، والمؤسسات والتي تتمثل في المنشآت الهامة و نظم المعلومات الهامة و منها نظم إدارة الجهات الخاصة والحكومات الإلكترونية، سنقسم المطلب كالتالى:

الفرع الأول: مفهوم الأمن السيبرانى.

الفرع الثانى: أنواع الأمن السيبرانى.

الفرع الأول
مفهوم الأمن السيبرانى

أولا: تعريف الأمن السيبراني:

يعرف الأمن السيبراني[١]،بأنه مجموعة من الأدوات[٢]،والوسائل التقنية ،والتنظيمية، والإدارية لمنع الاستخدام الغير مشروع ،وسوء استغلال المعلومات الإلكترونية[٣]،فهو ممارسة للدفاع عن أجهزة الكمبيوتر[٤]،والأجهزة المحمولة ،والأنظمة الإلكترونية[٥]، والشبكات ،والبيانات من التهديدات ،والهجمات الإلكترونية الضارة[٦]،أو الوصول غير المشروع للمعلومات، والبيانات، ،بالوسائل الإجرامية، فهو النشاط أو العملية أو القدرة أو الإمكانية التي يتم بموجبها حماية نظم المعلومات والاتصالات والمعلومات الواردة فيها والدفاع عنها ضد الضرر

---

(١) مصطلح السيبرانيه هو واحد من أكثر المصطلحات ترددا في معجم الأمن الدولي وكلمه سيبرأني لفظ يونانية الأصل مشتقه من معنى الشخص الذي يدير دفه السفينة كاستخدام مجازي للمتحكم.

(٢) تقرير بعنوان الأمن السيبرانى في مؤسسات منظومة الأمم المتحدة، تقرير وحدة التفتيش المشتركة، الامم المتحدة ،السنة ٢٠٢١.

(٣) الدكتور / عبد الوهاب محمد عبد الوهاب السادة، التنظيم القانوني للأمن السيبراني ، دار المطبوعات الجامعية ،السنة ٢٠٢٥،ص٢.

(٤) الدكتور/ حيدر فالح سلمان، مقدمة في الأمن السيبرانى ،الذاكرة للنشر والتوزيع ،لا يوجد سنة نشر،ص١٢.

(٥) الدكتور / خالد عبد الله المطيري، دور التشريعات الجزائية في حماية الأمن السيبرانى مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية،السنة١٤٤٣،ص٣٤.

(٦) الدكتورة / أماني قرني ، دور مواقع الأعلام الرقمي في حماية الأمن السيبرانى، المجلة المصرية لبحوث الأعلام ،السنة ٢٠٢٢،ص٦٥٦.

أو الاستخدام أو التعديل غير المصرح به أو الاستغلال ، ويعمل الأمن السيبراني على إنشاء وسائل دفاعية ،يتم استخدامها من قبل الأفراد ،والشركات لحماية الأجهزة، والبرامج ،والبيانات المتصلة بالإنترنت، والمعلومات الحساسة لحمايتها من التغيير أو التلف أو الحصول عليها لابتزاز المستخدمين للاستيلاء على الأموال،كالصور الشخصية التي يحصل عليها المجرمون لابتزاز الضحايا.

يعتبر الأمن بشكل عام في الحياة اليومية تأمين عمليات الدخول، والخروج، في مكان محدد، ولكن في الفضاء السيبراني يشمل مختلف القواعد والأصول التي تحمى وسائل الاتصال، وانتقال المعلومات، وتخزينها وحفظها، ليشمل أمن المواقع، وامن الأنظمة الإلكترونية.

يعتبر الأمن[١] السيبرانى خط الدفاع الأول عن أجهزة الكمبيوتر [٢]،من الهجمات الضارة التي يشنها المتسللون[٣] ،والمخترقون، ومرسلي البريد العشوائي ،ومجرمي الإنترنت،فهو مصطلح شامل لوصف عملية الحماية ضد كل أشكال الجرائم الإلكترونية[٤]، ويعتبر مجموعة من التقنيات التي تستخدمها المؤسسات لتجنب الحوادث الأمنية ،أو خروقات البيانات ،أو فقدان الأنظمة المهمة ،وتطبيقات

---

(١) هو نقيض الخوف والأمن مصدر الفعل أمنا و أمانا من نفس وسكون القلب وزوال الخوف ويقال أمينه من الشر أي كلمه منه.

(٢) حسين بن راشد الطيار، الأمن السيبرانى في منظور مقاصد الشرع ،دراسة تأصيلية، المملكة العربية السعودية جامعة الطائف، مجلة الطائف للعلوم الإنسانية، السنة ٢٠٢٠،ص٧٠.

(٣) الدكتور / عادل راضي ،الوقاية من المخاطر السيبرانية ،جامعة تبوك ، السنة ٢٠٠٦،ص٣.

(4) Karin Kelley ,what is cybersecurity and is important ,2024
مقال منشور https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security تاريخ الاطلاع ٩/ ٢٠٢٤ (٣

البرامج[1]، وتتحمل الشركات ،والمؤسسات مسؤولية تأمين بيانات ،ومعلومات الأفراد السرية للحفاظ على ثقة العملاء، بالامتثال للقواعد التنظيمية، وتنفيذ قواعد، وأدوات الأمن السيبراني، لضمان حماية المعاملات من أي اختراق يهدد العملاء ،أو المستهلكين.

(1) https://www.comptia.org/content/articles/what-is-cybersecurity تاريخ الاطلاع ٩/ ٢٠٢٤.

الفرع الثانى
أنواع الأمن السيبراني

وفي ظل تطور الهجمات الإلكترونية ، أصبح الأمن السيبراني أكثر أهمية من أي عصر مضى، ويجب على الدول التعاون لمكافحة الجرائم الإلكترونية[١]،و خصوصاً مع تزايد مخاطر الهجمات السيبرانية الإلكترونية[٢]، حيث يستهدف المهاجمون اختراق الأنظمة بهدف الاستيلاء على المعلومات، فأصبح ضروريًا ،وبشكل متزايد تنفيذ مجموعة شاملة من التقنيات، والعمليات، والممارسات المصممة لحماية الأجهزة ،والشبكات ،والبيانات الرقمية، متمثلة في تدابير ،وإجراءات الأمن السيبرانى.

أولا: الأمن السيبرانى للهاتف المحمول:

الهاتف الذكي هو الجهاز الإلكتروني الأكثر استخدامًا في الحياة اليومية للكثيرين ، بل ،واصبح بمثابة جهاز كمبيوتر محمول،لاحتوائة على مجموعة واسعة من التطبيقات لكل شيء من شبكات التواصل الاجتماعي إلى الخدمات البنكية عبر الإنترنت، بالإضافة إلى كمية البيانات التي تحتويها، و أن أمان الهاتف المحمول أمر بالغ الأهمية،ومع زيادة اعتمادنا على الأجهزة المحمولة، تزداد أيضًا التهديدات الموجهة إلى أمان الأجهزة المحمولة ،ويتضح دور الأمن السيبرانى في حماية البيانات، واهميه تنفيذ تدابير، وإجراءات الأمن السيبرانى في حماية الهاتف المحمول[٣].

---

(١) الدكتور/ جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت،دار النهضة العربية ،السنة ٢٠٠١،ص٧٢

(٢) الدكتور / راشد المري ،الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر، دار النهضة ،السنة ٢٠١٨،ص١٣.

(3) Karin Kelley,what is cybersecurity and is important ,2024

ثانياً: الأمن السيبراني للبنية الأساسية:

من أهم مجالات الأمن السيبرانى، أمن البنية التحتية[١]،ويتضمن استراتيجية حماية الأصول[٢]،وسبل الأمن السيبراني، التي تساعد على حماية[٣]، أصول المؤسسة ضد الهجمات الإلكترونية[٤]، وهو إجراء أمني يُتخذ لحماية البنية التحتية الحيوية [٥]،كحماية مجموعة الأنظمة ،واتصالات الشبكة، أو مركز البيانات[٦]،أو الخادم ،أو مركز تكنولوجيا المعلومات، والطاقة ،والاتصالات، والهدف منها هو القضاء على نقاط الضعف، أو الثغرات الأمنية في هذه الأنظمة من فساد ،أو تخريب ، أو هجمات،وعلى أصحاب الشركات ،والمؤسسات، والمنظمات التي تعتمد على البنية التحتية ، إدراك، ومعرفة جميع الالتزامات المتعلقة بهذا الإجراء، حتى لا يستطيع المهاجمون، والمتسللون استهداف أنظمة المرافق الخاصة لمهاجمة مختلف الأعمال، باتباع تدابير الأمن السيبرانى ،والالتزام بها.

---

(١) الدكتور خالد حسن لطفي، الدليل الرقمي ودورة في أثبات الجريمة المعلوماتية ، دار الفكر الجامعي ،السنة ٢٠٢٠،ص١٣ .

(٢) الدكتور/ حيدر فالح سلمان، المرجع السابق ذكرة، ص٦٢ .

(٣) مقال منشور تاريخ الاطلاع ٨/ ٢٠٢٤

https://www.sailpoint.com/identity-library/five-types-of-cybersecurity

(4) https://www.comptia.org/content/articles/what-is-cybersecurity

تارخ الاطلاع ٨/ ٢٠٢٤

(٥) الدكتور/ خالد ممدوح إبراهيم ،الجرائم المعلوماتية ،دار الفكر الجامعي، السنة ٢٠١٩،ص٣٣.

(٦) المادة ١ من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة تقنية المعلومات ولائحته التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم ١٦٩٩لسنة ٢٠٢٠.

تعتبر البنية الأساسية أصل الأنظمة الرقمية فى المجتمع ،وتتطلب المؤسسات العاملة في هذه المجالات نهجًا منهجيًا منضبطاً للأمن السيبراني، لأن انقطاع الخدمة، أو فقدان تلك البيانات يمكن أن يزعزع استقرار المؤسسة، وهناك الكثير من المؤسسات تعمل على برامج ،وشبكات مهلكة ، مما يعرضها لهجمات أمنية ،ولذلك لابد من اتباع تقنيات الأمن السيبراني لحماية تلك المؤسسات من الهجمات الإلكترونية [١].

ثالثاً:الأمن السيبرانى لشبكة المعلومات:

الشبكة هى مجموعة من الأجهزة ،أو نظم المعلومات تكون مرتبطة ببعضها، ويمكنها تبادل المعلومات، والبيانات، والاتصال فيما بينها ،ولحماية الشبكة قد يتضمن ذلك تكوين جدران الحماية لتأمين الشبكات[٢]، وغرفة تحكم للوصول لها، و تنفيذ برامج مكافحة الفيروسات[٣]،وهى مجموعة من تقنيات البرامج، والأجهزة من أجل حماية البيانات ،والمعلومات من التهديدات [٤]،لتامين شبكات الكمبيوتر من الوصول الغير مشروع[٥]،فيعتبر تامين الشبكة من أبرز أهداف الأمن السيبراني، لأن أغلب الهجمات تحدث عبر الشبكة [٦]،ويعمل أمن الشبكة كجدار عازل بين شبكة

---

(1) https://www.fortinet.com/resources/cyberglossary/operational-security

(2) https://online.eou.edu/resources/article/main-types-of-cyber-security/

(3) https://www.comptia.org/content/articles/what-is-cybersecurity

تاريخ الاطلاع ٩/ ٢٠٢٤

(٤) الدكتور/ حيدر فالح سلمان، المرجع السابق ذكرة،ص٤٧.

(5)https://www.geeksforgeeks.org/cyber-security-types-and-importance/

مقال منشور تاريخ الاطلاع ٩/ ٢٠٢٤

(٦) الدكتور/ علاء حسين الحمامي ،الدكتور / سعد عبد العزيز ،تكنولوجيا امن المعلومات وأنظمة الحماية، دار وائل للنشر ،السنة ٢٠٠٧،ص٧٦.

المؤسسة، والأنشطة الضارة، والهجمات[١]،ومن أجل استمرار الشبكة في تقديم الخدمات[٢]، وتلبية طلبات الموظفين ،والعملاء، وحماية كيان، وسُمعة المؤسسة، يجب الالتزام بوسائل ،وتقنيات الأمن السيبراني.

وقد عاقب المشرع المصرى بالحبس مدة لا تقل عن ثلاثة أشهر ، وبغرامة لا تقل عن عشرين ألف جنيه ،ولا تجاوز مائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من أتلف ، أو عطل ،أو شوه ،أو أخفى ،أو غير تصاميم موقع خاص بشركة ،أو مؤسسة ،أو منشأة ،أو شخص طبيعى بغير وجه حق[٣].

وعاقب ايضاً المشرع المصري بالحبس مدة لا تقل عن ثلاثة أشهر ، وبغرامة لا تقل عن عشرة ألاف جنيه ،ولا تجاوز خمسين ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من انتفع بدون وجه حق عن طريق شبكة النظام المعلوماتي ،أو إحدى وسائل تقنية المعلومات بخدمة اتصالات ،أو خدمة من خدمات قنوات البث المسموع ، والمرئي [٤] .

---

(1)Types of cybersecutity
https://www.sailpoint.com/identity-library/five-types-of-cybersecurity
مقال منشور تاريخ الاطلاع٩/ ٢٠٢٤

(2) Travaux de l institute de sciences criminelles de poitiers,informatiqe et droit penal,ed cujas ,1983,p25

(٣) المادة ١٩ يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ، وبغرامة لا تقل عن عشرين ألف جنيه ، ولا تجاوز مائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من أتلف ،أو عطل ،أو شوه ،أو أخفى ، أو غير تصاميم موقع خاص بشركة ،أو مؤسسة ،أو منشأة ،أو شخص طبيعى بغير وجه حق القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة تقنية المعلومات ولائحته التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم ١٦٩٩لسنة ٢٠٢٠.

(٤) المادة ١٣ بالحبس مدة لا تقل عن ثلاثة أشهر ، وبغرامة لا تقل عن عشرة ألاف جنيه ،ولا تجاوز خمسين ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من انتفع بدون وجه حق عن طريق شبكة النظام المعلوماتي ،أو إحدى وسائل تقنية المعلومات بخدمة اتصالات ،أو خدمة من خدمات

ويعاقب المشرع المصري بالحبس مدة لا تقل عن سنة ، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من دخل عمداً ، أو دخل بخطأ غير عمدى وبقى بدون وجه حق ، على موقع أو حساب خاص ،أو نظام معلوماتي محظور الدخول عليه[١] .

رابعاً: الأمن السيبرانى المعلوماتي :

يحظر نقل المعلومات، أو البيانات ،أو الاطلاع عليها ألا في اطار القانون[٢]،ويعتبر امن المعلومات من أهم مجالات الأمن السيبراني، وهو عبارة عن عملية تصميم ، ونشر أدوات، وأليات لحماية المعلومات الحساسة ،والسرية من التدمير ،والتعطيل ، والتعديل، والسطو[٣]، ويُطبق أمن المعلومات بهدف التأكد من أن المستخدمين الموثوق فيهم فقط ، أو التطبيقات ،أو الأنظمة المعرفة، هم من يمكنهم الوصول إلى معلومات معينة، ولا يجوز لأى مصدر مجهول الوصول ألي تلك المعلومات، فيمنع

قنوات البث المسموع ،والمرئي القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة تقنية المعلومات ولائحته التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم ١٦٩٩لسنة ٢٠٢٠.

(١) المادة ١٤ بالحبس مدة لا تقل عن سنة ، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من دخل عمداً ، أو دخل بخطأ غير عمدى وبقى بدون وجه حق ، على موقع أو حساب خاص ،أو نظام معلوماتي محظور الدخول عليه القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة تقنية المعلومات ولائحته التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم ١٦٩٩لسنة ٢٠٢٠.

(٢) الدكتور / علي القهوجي ،الحماية الجنائية لبرامج الحاسب ،دار الجامعة ،السنة١٩٩٧،ص٣٣.

(3) https://www.comptia.org/content/articles/what-is-cybersecurity تاريخ الاطلاع ٩/ ٢٠٢٤

الأمـن الـسيبرانى أي شـخص مجهـول مـن الـدخول للمعلومـات، للحفـاظ عـلى سريتها.وقد عاقب المشرع المصري بالحبس ، كل من اعترض بـدون وجـه حـق أى معلومات ،أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتيـة ،أو أحـد أجهـزة الحاسب الآلي ،وما فى حكمها[١].

خامساً: الأمن السيبرانى للمستخدم :

المستخدم كل شـخص طبيعـى ،أو اعتبـاري يـستعمل، أو يـستخدم خـدمات تقنيـة المعلومات[٢]،ويُعد المستخدم هو خط الدفاع الأول ضـد الهجـمات الإلكترونيـة، إذ يمكنه الوقاية من الهجمات الأمنية ،ومنعها، ويحمى نفسة من التعـرض لأي نـوع مـن التهديدات، والهجمات الإلكترونية[٣]، وذلك يتم بالمعرفة ،والتدريب ،والتعليم حول أفضل الممارسات ،وسبل الأمن السيبرانى، وتأمين الأجهزة الخاصة به، مثـل أجهـزة الكمبيوتر ،وأجهزة الكمبيوتر المحمولة ،والهواتف الذكية، وذلك باستخدام وسـائل الأمن السيبرانى كبرنامج مكافحة الفيروسات، والأنظمة الواقية مـن التسلل، وتـشفير الجهاز، وتحديثات البرامج بصورة مستمرة،وتأهيـل المـستخدم لمعرفـة مـا يتعلـق

---

(١) يعاقب بالحبس مدة لا تقل عن سنة ، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من اعترض بدون وجه حق أى معلومات ،أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما فى حكمها المادة ١٦ القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة تقنية المعلومات ولائحته التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم ١٦٩٩لسنة ٢٠٢٠.

(٢) المادة ١ القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة تقنية المعلومات ولائحته التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم ١٦٩٩لسنة ٢٠٢٠.

(3)https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity الاطلاع ٩/ ٢٠٢٤

بالأمن السيبراني؛ لا بد من تدريبه، وتعليمة للتوعية الأمنية السيبرانية، والمامة بالتهديدات المختلفة ،وعمليات الاحتيال ،وأمن الجهاز ،وإنشاء كلمة المرور ، وكل ما يخص الأمن السيبراني، لأن نشر ثقافة الأمن السيبرانى، تعتبر وقاية من الهجمات ، والتهديدات الإلكترونية.

سادساً: ألأمن السيبرانى للتطبيقات:

أمان التطبيقات يعتمد على تنفيذ دفاعات مختلفة في برامج(١)، وخدمات المؤسسة ضد مجموعة متنوعة من التهديدات، والهجمات ،و يقوم بتلك الدفاعات ، المتخصصين ،وخبراء الأمن السيبراني ،ومنها كتابة كود آمن ،وتصميم هياكل تطبيقات آمنة، والتحقق من صحة إدخال البيانات(٢)،و كل ذلك يهدف إلى تحسين مستويات التطبيقات، وحمايتها من محاولات التضليل غير المصّرح بة(٣)،سواء في مراحل التصميم ،أوالتطوير، أوالاختبار.

سابعاً: ألأمن السيبرانى لنقطة النهاية:

يحمى الأمن السيبرانى نقطة النهاية من المخاطر، والتهديدات الأمان وهى نقطة عند وصول المستخدمين إلى شبكة المؤسسة عن بُعد(٤)، و يهدف الأمن السيبرانى إلى

---

(١) الدكتور/ حيدر فالح سلمان، المرجع السابق ذكرة، ص٥٦.

(2)Karin Kelley,what is cybersecurity and is important ,2024

مقال منشور -https://www.simplilearn.com/tutorials/cyber-security tutorial/what-is-cyber-security

تاريخ الاطلاع) ٩/ ٢٠٢٤

(٣) الدكتورة/ مني عبد الله السمحان ،متطلبات تحقيق الأمن السيبرانى لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية جامعة المنصورة، يوليو ٢٠٢٠ ،ص٢٠.

(4) https://www.comptia.org/content/articles/what-is-cybersecurity

تاريخ الاطلاع ٩/ ٢٠٢٤

حماية أمان نقاط النهاية بفحص الملفات المرسلة من الأجهزة الفردية ،الى المؤسسة، ومنع الهجمات ،وتقليل التهديدات، وتأمين كل الملفات المرسلة من الأفراد الى المؤسسات

ثامناً: التخطيط لاستمرارية القيام بالأعمال:

يعنى القدرة على الاستمرار في العمل بعد حدوث الهجمات ،والكوارث، و التخطيط من أجل استمرارية العمل بطريقة سليمة ،وسريعة[١]،وطبيعية بعد وقوع الكارثة، وبشكل عام، ويجب أن تبدأ تقنية استعادة القدرة على العمل بعد الهجمات مباشرة[٢] ،والاستعانة بالتطبيقات الحيوية، لإدارة مختلف الأنشطة، التى تسمح للمؤسسات الاستجابة بصورة اسرع لحوادث الأمن السيبراني، ومواصلة العمل بدون أي انقطاع ،وبشكل مستمر، فهي تنفّذ سياسات، ومعالجات لاستعادة البيانات سريعاً، استمرار العمل بعد الهجمات من الأمور الحيوية لبقاء المؤسسة، فيجب التدريب على خطط بديلة، لاستمرار عمل المؤسسة بشكل طبيعي بعد حدوث الحوادث ، والهجمات.

أهداف الأمن السيبراني:

أولا: حماية أنظمة التشغيل:

يهدف الأمن السيبرانى ألي حماية أنظمة التقنيات التشغيلية بكافة أشكالها ،من مكونات الأجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات،والتصدي للهجمات الإلكترونية وحوادث اختراق البيانات، والمعلومات التي تستهدف الأجهزة والخاصة، والحكومية لتوفير بيئة أمنة يثق فيها العملاء،وحماية البنية التحتية من الهجمات الإلكترونية،حيث يهدف الأمن السيبرانى

---

(١) حسن طاهر داود، الحاسب وامن المعلومات ، مركز البحوث، السنة ٢٠٠٠،ص٩٤.

(٢) المرجع السابق ذكرة.

ألي توفير مناخ امن للمتعاقدين في التجارة الإلكترونية، من خلال الدفاع عن أنظمة التشغيل الإلكترونية.

ثانيا: منع المخاطر والجرائم الإلكترونية:

يهدف الأمن السيبرانى إلى منع المخاطر، والجرائم، والتهديدات الإلكترونية، وذلك بالتخلص من نقاط الضعف، والثغرات في الأنظمة الإلكترونية[1]،ويهدف الأمن السيبرانى إلى مقاومة، وصد البرمجيات الخبيثة، ومنع ما تستهدفه من أحداث أضرار بالغة للمستخدمين،ويهدف إلى منع من التجسس والتخريب الإلكتروني على مستوى المؤسسات والأفراد،باتخاذ جميع التدابير اللازمة لحماية العملاء ،والمستهلكين من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة،وتدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية.

(١) تقرير بعنوان الأمن السيبرانى في مؤسسات منظومة الأمم المتحدة، تقرير وحدة التفتيش المشتركة، الامم المتحدة ،السنة ٢٠٢١،ص١١

المطلب الثانى
تقنيات الأمن السيبرانى

تمهيد وتقسيم:

يساعد إنشاء استراتيجية قوية للأمن السيبراني على حماية الاستثمارات في الأنظمة الإلكترونية، حيث أن الأمن السيبرانى لديه القدرة على توفير الحماية ضد الهجمات الضارة التي يمكنها الوصول إلى البيانات ،والأنظمة الحساسة الخاصة بالمؤسسة ،أو المستخدم ،أو تعديلها، أو حذفها ،أو تدميرها، لاسيما أن تأثير الهجوم الرقمي يهدف إلى تعطيل ،أو مقاطعة عمليات النظام ،أو الجهاز، مما يمكن أن تكون له عواقب وخيمة، وتقنيات الأمن السيبراني الحديثة تساعد المؤسسات على تأمين بياناتها بشكل فعال، سنقسم المطلب كالتالى:

الفرع الأول: نشر ثقافة الأمن السيبراني.

الفرع الثانى: تأمين البيانات بالأمن السيبرانى.

الفرع الأول
نشر ثقافة الأمن السيبراني

أولاً: الالتزام بمبادئ وأخلاقيات السيبرانية :

يحتاج المتعاملين في المجالات الإلكترونية لنجاح معاملاتهم إلى التمسك بمبادئ، وأخلاقيات الأمن السيبراني[1]، حيث إنهم مسؤولون عن معاملاتهم عبر الإنترنت ، فيجب عليهم الالتزام بمبادئ الأمن السيبرانى ،و التحلي الصدق، والإنصاف ،والمسؤولية ،والاحترام، والابتعاد عن أي ممارسات غير أخلاقية ،أو غير قانونية، مثل الاحتيال ،والخداع ، والانتحال، والقرصنة، التي قد تضرهم ،وينبغي لأصحاب المنصات ،و المؤسسات، والشركات أيضا تعزيز ثقافة الأمن السيبرانى، وتوفير خدمات عالية الجودة، وموثوقة ،وآمنة على الإنترنت، والتعامل مع عملائهم ،والمستهلكين بطريقة شفافة،تتعلق بالمُثُل الأخلاقية، لجذب ثقتهم، ويجب الالتزام ،ومراعاة حقوق الملكية الفكرية، حقوق النشر، والحفاظ على الخصوصية عبر الإنترنت، تلك المبادئ ،والأخلاقيات، عوامل نجاح المعاملات الإلكترونية.

ثانياً: نشر الوعى السيبرانى بين الموظفين:

أغلب الموظفين في المؤسسات غير مدركين، وواعين بمبادئ ،وتدابير الأمن السيبرانى ،وكيفية الوقاية من أحدث التهديدات، والهجمات ،ولا يعلمون أفضل ممارسات الأمن السيبرانى التي تساعدهم على حماية أجهزتهم، وشبكاتهم ،ولذلك لابد إن يتم تدريب الموظفين ،والعاملين على تدابير الأمن السيبراني، لتقليل، وتجنب مخاطر الهجمات الإلكترونية الغير مرغوب فيها[2]،ونشر ثقافة الأمن السيبرانى

---

(1) https://cypfer.com/what-are-the-6-types-of-cyber-security
تاريخ الاطلاع ٩/ ٢٠٢٤

(٢) تاريخ الاطلاع ٩/ ٢٠٢٤)https://preyproject.com/blog/how-to-educate-employees-about-cybersecurity

كحماية البيانات، والمعلومات، والتأكد من اعتمادهم كلمات مرور سرية قوية، والحفاظ، وصيانة بيانات العملاء،واستخدام تقنيات الدفاع السيبراني الآلية في البنية الأساسية للأنظمة الإلكترونية، كجهات دفاعية ضد التهديدات، والهجمات المحتملة على جميع نقاط الضعف في البيانات، و تحدّيد المخاطر ، ورصد الثغرات.

ثالثاً: نشر الوعي السيبرانى بين العملاء والمستهلكين:

تثقّيف، وتدريب العملاء، والمستهلكين بتدابير الأمن السيبرانى [١]،والممارسات الآمنة عبر الإنترنت[٢]،أمر ضروري ،و حتمي، لحماية البيانات، والمعلومات، ونجاح المعاملات الإلكترونية ،مثل عدم مشاركة العملاء بياناتهم ،و كلمات المرور السرية، وتوخي الحذر من رسائل البريد الإلكتروني المشبوهة، ومراجعة نشاط الحساب بانتظام.

رابعاً: ضرورة الالتزام باللوائح التنظيمية:

يجب على الشركات، والمنصات الإلكترونية الامتثال، والالتزام باللوائح التنظيمية[٣]،من أجل حماية البيانات، والمعلومات السرية من المخاطر السيبرانية المحتملة ،وقد وصل الأمن السيبيري الى جميع المسائل التجارية، والاجتماعية والسياسية، والإنسانية، ويمثل الأمن السيبرانى قدرة المؤسسات على حماية مصادر الثروة ، وهى البيانات، والمعلومات.وتعمل السلطات المصرية المختصة على تيسير

---

(١) تقرير الأمين العام ،المبادئ التوجيهية لاستعمال البرنامج العالمي للأمن السيبراني ،جنيف الوثيقة A-65 السنة ٢٠٢٠

(٢) الدكتور / محمد سعيد ،التامين الإلكتروني ضد المخاطر السيبرانية ،المجلة الدولية للقانون ، دار نشر قطر ،٢٠٢١ص٢١١

(3) https://cypfer.com/what-are-the-6-types-of-cyber-security
تاريخ الاطلاع ٨/ ٢٠٢٤

التعاون مع نظيراتها بالبلاد الأجنبية فى إطار الاتفاقيات الدولية ،و الإقليمية ،والثنائية المصدق عليها ، أو تطبيقاً لمبدأ المعاملة بالمثل ، بتبادل المعلومات بما من شأنه أن يكفل تفادى ارتكاب جرائم تقنية المعلومات[١].

(١) المادة ٤ من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة تقنية المعلومات ولائحته التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم ١٦٩٩لسنة ٢٠٢٠.

الفرع الثانى
تأمين البيانات بالأمن السيبرانى

أولاً: معالجة نقاط الضعف بصفة دورية:يعالج الأمن السيبرانى نقاط الضعف، والثغرات المعرضة للهجمات بصفة دورية[١]، في البنية الأساسية الإلكترونية، إما داخلياً ،أو بمساعدة خبراء من الأمن السيبراني التابعين لجهات خارجية ،ويساعد معالجة أي نقاط ضعف أمنية في منع مخاطر الهجمات الإلكترونية،وتأمين بيانات الأفراد، والمؤسسات.

ثانياً: تشفير البيانات والمعلومات: أصبحت المعلومات هى عملة العالم الرئيسية[٢]، ولابد من حمايتها من الهجمات ،والتهديدات بتشفيرها[٣]،والتشفير منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة ،وتحويل البيانات المقروءة الكتر ونيا ، ولا يمكن استخلاصها، وقراءتها ألا عن طريق مفاتيح فك الشفرة[٤]،ويعمل التشفير الحسابي على تشفير البيانات، قبل تخزينها في قواعد البيانات، وهذا يمنع الأطراف غير المسموح لها بالاطلاع على المعلومات ،من إساءة استخدام البيانات في انتهاكات محتملة، فهو وسيلة حماية للمعلومات ،من خلال تحويل نص واضح ألي نص غير واضح ،يستطيع من خلاله كلا الطرفين فك هذه الشفرات[٥]،من خلال فك

---

(1) https://cypfer.com/what-are-the-6-types-of-cyber-security/ تاريخ الاطلاع ٨/ ٢٠٢٤

(٢) هربرت لين ،النزاع السيبرانى والقانون الدولي الإنساني، المجلة الدولية للصليب الأحمر ،السنة ٢٠١٢،ص٥١٥.

(3) https://cypfer.com/what-are-the-6-types-of-cyber-security/8/2024 2)

(٤) المادة ١ القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة تقنية المعلومات ولائحته التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم ١٦٩٩لسنة ٢٠٢٠.

(٥) الدكتور/ عدنان مصطفي البار، أمن المعلومات والأمن السيبرانى، كلية الحاسبات وتقنية المعلومات ،جامعة الملك عبد العزيز،ص٢.

رموزها[١]،كما يضمن التشفير أنه في حال تمكّن أحد الأفراد غير المصرح لهم من الوصول إلى البيانات، فلا يمكنهم الاطلاع عليها بدون مفاتيح التشفير[٢]، ويجب على المنصات ،والشركات الإلكترونية استخدام بروتوكولات آمنة[٣]،لتشفير الاتصالات ،والمعلومات ،ونقل البيانات بين مواقع الويب الخاصة بها ،وعملائها، بالإضافة إلى بياناتهم، لمنع التنصت، من قبل المهاجمين، ويجب عليهم أيضًا استخدام التشفير لحماية بياناتهم غير النشطة، مثل الخوادم ،أو قواعد البيانات ،أو النسخ الاحتياطية، لمنع الوصول غير المصرح به ،أو الكشف عنها من قبل المهاجمين.

ثالثاً: تفعيل انعدام الثقة: يعتبر انعدام الثقة من أهم مبادئ الأمن السيبراني ، والذي يَفترض عدم الوثوق ،وعدم تفعيل أي تطبيقات، أو رسائل ،أو مستخدمين تلقائيًا مجهولين الهوية ، أو حتى في حالة استضافتهم داخل المؤسسة[٤].

رابعاً: تتبع الأنشطة المشبوهة وكشف التسلل :تعتبر عملية تحليلات السلوك ، ومراقبة عملية نقل البيانات من الأجهزة ،والشبكات المختلفة ،لاكتشاف ،ومتابعة أي نشاط مشبوه ، ومراقبته ،ومتابعة الحركات غير المعتادة، كتنبيه فريق الأمن السيبرانى بأي تغيير كحدوث ارتفاع مفاجئ في نقل البيانات ،والمعلومات، أو بتنزيل ملفات مشبوهة إلى أجهزة معينة[٥]، التي يستغلها المهاجمون لضعف الإجراءات الأمنية فيها للدخول إلى بياناتها، ولذلك تستخدم المؤسسات أنظمة لكشف التسلل لتحديد الهجوم السيبراني ،ومعالجته بسرعة.

---

(١) الدكتور / عبد الوهاب محمد عبد الوهاب السادة، المرجع السابق ذكرة ،ص١٩٤

(٢) المادة ٣ القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة تقنية المعلومات ولائحته التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم ١٦٩٩لسنة ٢٠٢٠.

(3) https://cypfer.com/what-are-the-6-types-of-cyber-security/ 8/2024

(4) 8/20248)https://blog.qit.company/

(5) https://blog.qit.company/8/2024 87

المبحث الثانى
دفاع الأمن السيبرانى عن المتعاقدين في التجارة الإلكترونية

تمهيد وتقسيم:

يواجه المتعاقدين في مجال التجارة الإلكترونية تحديات ،وفرصًا مختلفة لضمان أمان منصاتهم ، ومنتجاتهم ،وخدماتهم عبر الإنترنت ،وحيث تعد منصات شركات، ومتاجر التجارة الإلكترونية أساس التعاملات التجارية عبر الإنترنت، لذلك يجب تصميمها ،وتطويرها بما يتوافق مع معايير، ولوائح الأمن السيبرانى، فإن الأمن السيبراني هو أهم عوامل نجاح التجارة الإلكترونية[1]،فيجب أن تحتوي منصة التجارة الإلكترونية الآمنة على وسائل الحماية كالتشفير ،وجدارن الحماية ،ومكافحة الفيروسات ،ومكافحة البرامج الضارة ،والنسخ الاحتياطي، وتحديثها بسهولة، وتأمين أنظمة الدفع الإلكترونية، التي تؤمن عمليات الدفع ،والتحصيل الآمنة عبر الإنترنت، مثل بطاقات الائتمان ،والتحويل البنكي.

سنقسم المبحث كالتالي:

المطلب الأول: سبل الأمن السيبرانى في حماية أطراف عقود التجارة الإلكترونية.

المطلب الثانى: الوسائل القانونية لمكافحة الجرائم الإلكترونية.

---

(1) https://www.institutedata.com/blog/what-are-the-7-types-of-cyber-security/

تاريخ الاطلاع٨/ ٢٠٢٤

المطلب الأول
سبل الأمن السيبرانى في حماية أطراف عقود التجارة الإلكترونية

تمهيد وتقسيم:

ازدادت معاملات التجارة الإلكترونية في السنوات الأخيرة، مما أدى لازدياد خطر التهديدات ،والهجمات الإلكترونية [١]،ومخاطر الفيروسات الإليكترونية على تلك المعاملات[٢]،مما إدي الى وجود ضرورة مُلحّة على المنصات ،والشركات لامتلاك الوعي ،والحذر الشديدين لحماية بياناتها، بيانات عملاءها من التهديدات الرقمية ، فالمخترقون في كل أنحاء العالم يبذلون قصارى جهدهم لاختراق التدابير الأمنية للمنصات ،وللشركات الكبرى، سنقسم المطلب كالتالي:

الفرع الأول: ماهية التجارة الإلكترونية.

الفرع الثانى: فعالية الأمن السيبرانى في صد الهجمات على المتعاقدين في التجارة الإلكترونية.

---

(١) نهى مجدي السيد ،الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر ٢٠٣٠،المجلة العلمية لبحوث الأعلام، السنة٢٠٢١،ص٨

(٢) الدكتور / مصطفي كمال طة ،الأستاذ / وائل بندق ،الأوراق التجارية ووسائل الدفع الإلكتروني، دار الفكر الجامعي ،السنة ٢٠٠٥،ص٣٢٥.

الفرع الأول
ماهية التجارة الإلكترونية

أولاً: تعريف التجارة الإلكترونية:

التجارة الإلكترونية هي عملية بيع ،وشراء البضائع ،والخدمات عبر الإنترنت، من خلال أجهزة الكمبيوتر الخاصة، والهواتف الذكية.

ثانياً: أشكال التجارة الإلكترونية:

١) التجارة الإلكترونية بين الأفراد في المجتمع حيث يتم بيع ، وشراء السلع بين الأفراد عبر منصات الإنترنت عبر منصات مخصصة.

٢) التجارة الإلكترونية بين الشركات، وبعضها حيث تتم عمليات البيع ،والشراء بين الشركات عبر منصات إلكترونية مخصصة.

٣) التجارة الإلكترونية بين الشركات ،والمستهلكين حيث يتم بيع المنتجات مباشرة من الشركة إلى المستهلك عبر منصات التجارة الإلكترونية[١].

٤) التجارة الإلكترونية بين الشركات ،والحكومات حيث تتم العمليات التجارية بين الشركات ،والجهات الحكومية عبر الإنترنت.

ثالثاً: خصائص التجارة الإلكترونية:

١. **قلة التكاليف**: تساهم التجارة الإلكترونية في تقليل تكاليف التشغيل، والعمالة[٢]، مثل تكاليف الإيجار ،والتشغيل ،والتسويق، مما يسمح بتقديم أسعار تنافسية للمستهلكين، وافضل العروض.

---

(١) الدكتور / مصطفي كمال طة ،الأستاذ / وائل بندق ،الأوراق التجارية ووسائل الدفع الإلكتروني، دار الفكر الجامعي ،السنة ٢٠٠٥،ص٣٢٥

(٢) الدكتور / مصطفي كمال طة ،الأستاذ / وائل بندق ،المرجع السابق ذكرة ،ص٣٢٨.

٢. **دقة التحليلات**: يتيح النظام الرقمي للتجارة الإلكترونية متابعة ،وتحليل سلوك العملاء ،أو المستهلكين بدقة، مما يمكن الشركات من اتخاذ قرارات مستنيرة بناءً على بيانات دقيقة.

٣. **التواصل الاجتماعي**: يمكن للتجارة الإلكترونية استخدام منصات التجارة الإلكترونية للتفاعل مع العملاء ،وبناء علاقات تجارية دائمة، والتفاعل مع العملاء ، وجذبهم بشكل فعال من خلال الحملات التسويقية ،والتفاعلات الاجتماعية.

٤. **تخزين البضاعة الرقمي**: يتم تخزين المنتجات ،والخدمات بنظام رقمي، مما يقلل من الحاجة إلى مساحات كبيرة للتخزين الحقيقي ،ويسهل عمليات الإدارة ، والتوزيع.

٥. **تجربة التسوق الشخصية**: يمكن للتجارة الإلكترونية توفير تجارب تسوق شخصية مخصصة لكل عميل، أو مستهلك بناءً على تفضيلاته في التسوق.

٦. **توسع وتنوع النشاط التجاري**: يمكن للشركات في مجال التجارة الإلكترونية توسيع نطاق عملها بسهولة من خلال العرض فى منصات تجارة إلكترونية جديدة[١] ، أو إضافة منتجات جديدة إلى متاجرها الحالية دون الحاجة إلى تكاليف إضافية كبيرة.

٧. **توفير العروض والخصومات**: يمكن للشركات في مجال التجارة الإلكترونية تخصيص ،وتوفير العروض ،والخصومات بناءً على تفضيلات كل عميل فى التسوق، مما يزيد من فرص البيع ،والشراء.

---

(١) الدكتور / مصطفي كمال طة ،الأستاذ / وائل بندق ،المرجع السابق ذكرة ،ص٣٢٧.

رابعاً: تعريف عقود التجارة الإلكترونية:

عقود التجارة الإلكترونية هي العقود التي يتم إبرامها عبر شبكة الإنترنت[١]،بين جماعة العاملين في التجارة المحلية. والدولية[٢]،وتعتبر مجموع من المبادلات الرقمية المرتبطة بالأنشطة التجارية الإلكترونية[٣]،وهي تكتسب صفة الإلكترونية من طريقة إبرام العقد، فالعقد الإلكتروني ينشأ من تلاقى إيجاب ،وقبول بطريقة سمعية بصرية عبر شبكة الأنترنت[٤]، محلية ،ودولية للاتصال عن بعد[٥]، دون الحاجة إلى التقاء الأطراف المادي في مكان معين، أي انتفاء مجلس العقد الحقيقي، فمجلس العقد في عقود التجارة الإلكترونية مجلس افتراضي حكمي أي عقد متعلق بالسلع ، والخدمات يتم بين مورد ،ومستهلك (شركة ،وعميل)من خلال الإطار التنظيمي الخاص بالبيع عن بعد.

خامساً: أركان عقد التجارة الإلكتروني:

أساس العقود حرية أطراف التعاقد في اختيار شكل التعبير عن إرادتهم [٦]،و الأصل في العقود هو الرضائية[٧]،والمتعاملين في هذا الميدان هم اكثر قدرة ،ومعرفة من

---

(١) المرجع السابق ذكرة،

(٢) الدكتور/ احمد عبد الكريم سلامة، نظرية العقد الدولي الطليق ، دار النهضة العربية ، ج٢، ١٩٨٩، ص٢٦٧.

(٣) الدكتور / حسام الأهوانى ،أثبات عقود التجارة الإلكترونية ،مؤتمر القانون وتحديات المستقبل ،كلية الحقوق جامعة الكويت ،١٩٩٧،ص٢.

(4) Olivier mean ,L internet et Le adroit. Aspects juridiques du commerce electronique ed enrollers ,Paris 1996,p34

(٥) الدكتور / صالح المنزلاوي، القانون الواجب التطبيق على عقود التجارة الإلكترونية ،دار النهضة ،السنة ٢٠٠٥،ص١٤.

(٦) الدكتور/ احمد محمد ابراهيم ،القانون المدني معلقا علي نصوصه بالأعمال التحضيرية وأحكام القضاء ،دار المعارف ،السنة ١٩٦٤،ص٤٨

(٧) الدكتور/ رضا عبيد، القانون التجاري، لا يوجد دار نشر، السنة ١٩٨٣،ص٩

غيرهم في تنظيم العلاقات التي تربطهم من خلال ما يروه اكثر انسجاما مع حاجاتهم[١]،والتعبير عن الإرادة يكون باللفظ ،وبالكتابة وبالإشارة المتداولة عرفا ، وباتخاذ موقف لا يدع مجلا للشك[٢].

وتتحقق صحة عقد التجارة الإلكتروني بتحقق صحة أركانه، المحل ،والسبب ، والرضا ،والأهلية ذات القواعد العامة المنظمة للعقد التقليدي مع بعض الخصوصية لهذه الأركان، لعدم اتساع نطاق القواعد العامة؛ لتستوعب أهلية المتعاقدين لأنه من الصعب التحقق من هوية الأطراف المتعاقدة ،وأهليتها.

سادساً:خصائص عقد التجارة الإلكتروني:

١. يتم عقد التجارة الإلكتروني بمجلس عقد حكمي:

تتم عقود التجارة الإلكترونية عبر الإنترنت[٣]، دون الحاجة إلى التواجد الجغرافي في مكان معين[٤]،ويتم التعاقد في التجارة الإلكترونية عن بعد بوسائل اتصال عبر الأنترنت[٥]، وينتمي إلى طائفة العقود التي عن بعد[٦]،ولذلك فهو عقد فوري متعاصر،

---

(١) الدكتور/ احمد عبد الكريم سلامة، المرجع السابق ذكرة، ص٢٦٧.

(٢) المادة ٩٠ من القانون المدنى المصري رقم ١٣١لسنة ١٩٤٨.

(٣) المادة ١ من قانون حماية المستهلك ،القانون رقم ١٨١لسنة ٢٠١٨ ولائحته التنفيذية الصادرة بقرار مجلس الوزراء رقم لسنة ٢٠١٩

(٤) الدكتور/ مهند عزمي مسعود ،القانون الواجب التطبيق علي العقد الدولي ،رسالة دكتوراه ،حقوق عين شمس ،السنة ٢٠٠٥،ص٥١

(٥) الدكتور/ خالد ممدوح ابراهيم، إبرام العقد الإلكتروني، دار الفكر الجامعي، السنة ٢٠٠٦،ص٥١.

(٦) الدكتور / اشرف وفا محمد ،عقود التجارة الإلكترونية في القانون الدولي الخاص ،المجلة المصرية للقانون الدولي ،العدد ٥٧،السنة ٢٠٠١،ص ١٢

وقد يكون العقد الإلكتروني غير متعاصر أي أن الإيجاب غير معاصر للقبول فى وقت لاحق.

٢. **إبرام عقد التجارة الإلكتروني بالوسائط الإلكترونية**:

يتم إبرام عقد التجارة الإلكترونية بالوسائط الإلكترونية[١]،عبر الانترنت[٢]،وتلك الوسائط هي التي دفعت إلى اختفاء الكتابة التقليدية بشكلها المعتاد[٣]،التي تقوم على الدعائم الورقية لتحل محلها الكتابة الإلكترونية التي تقوم على دعائم إلكترونية، والعقد الذي يبرم عبر شبكة الأنترنت، هو في الأصل عقد عادي لكن يكتسب هذه الصفة من خلال الطريقة التي ينعقد بها، حيث ينشا بوسيلة سمعية بصرية عن بعد، تعتمد هذه العملية على استخدام التقنيات الحديثة للتواصل ،والمعالجة الإلكترونية لتسهيل تبادل السلع ،والخدمات بين البائع ،والمشتري دون الحاجة للتواجد الجغرافي في مكان محدد.

٣. **يتصف عقد التجارة الإلكتروني بالطابع الاستهلاكي**:

محل العقود الإلكترونية دائما بضاعة[٤]،لذلك يطلق عليها عقود التجارة الإلكترونية، وقد جاءت تلك الصفة من الطابع السائد لتلك العقود ،و تستحوذ عقود التجارة الإلكترونية على معظم العقود الإلكترونية، وتلك العقود تتم عن طريق عرض البضاعة على منصات التجارة الإلكترونية، ثم يتسوق المستهلك ويشتري منها.

---

(١) تشير الوسائط الرقمية إلى أكثر من مجرد تنسيق الملفات الرقمية، حيث تمثل مفهومًا واسع النطاق يشمل بعض الأدوات كالصور الرقمية، ومقاطع الفيديو ، ويمكن للعديد من الأجهزة الرقمية تحرير الوسائط الرقمية وتخزينها وعرضها.

(٢) الدكتور / اشرف وفا محمد ،المرجع السابق ذكرة،ص١٢.

(٣) الدكتور / عبد الله نوار شعت ،الأثبات والالتزامات في العقود الإلكترونية ،مكتبة الوفاء القانونية ،السنة٢٠١٧،ص٣٤.

(٤) الدكتور/ رضا عبيد، المرجع السابق ذكرة،ص١١

٤. **عقود التجارة الإلكترونية عقود دولية**: عقود عابرة للحدود، فيمكن لعقود التجارة الإلكترونية الوصول إلى جمهور في مختلف العالم بسهولة، مما يتيح فرصًا للتوسع ،وزيادة العملاء من مختلف أنحاء العالم.

٥. **سهولة عقد التجارة الإلكترونية**: يمكن للمستهلكين، أو العملاء مشاهدة المنتجات [١]،والخدمات ،وشرائها في أي وقت ومن أي مكان بسهولة ، دون الحاجة إلى زيارة المتاجر الفعلية، وذلك يوفر الوقت ،والجهد اللازمين للذهاب إلى المتاجر التقليدية، حيث يمكنهم البحث عن المنتجات ،وشرائها بسرعة ،وسهولة عبر الأنترنت من خلال جهز الكمبيوتر، أو الهاتف المحمول.

(١) الدكتور / مصطفي كمال طة ،الأستاذ / وائل بندق ،المرجع السابق ذكرة ،ص٣٢٥.

الفرع الثانى

فعالية الأمن السيبرانى في صد الهجمات على المتعاقدين في التجارة الإلكترونية

تعتبر الجريمة السيبرانية شكل متطور من الجريمة[١]،فهى مجموعة من الأفعال والأعمال غير المشروعة[٢]،التي تتم عبر الأجهزة إلكترونية أو شبكة الإنترنت وتعرض الجرائم الإلكترونية منصات التجارة الإلكترونية، والمتعاقدين،والمستهلكين، والشركات للخطر[٣]،وتهدد أمانهم[٤]،ومنتجاتهم، وخدماتهم[٥]،من خلال الاستيلاء على البيانات، والمعلومات الخاصة بهم، فيجب على منصات التجارة الإلكترونية[٦]، والمتعاقدين الالتزام بقواعد الأمن السيبرانى ، كمكافحة الفيروسات[٧]،والتشفير، وجدران الحماية، والنسخ الاحتياطي، للوقاية ، ومنع الهجمات ،والتهديدات الإلكترونية ،واكتشافها ،وصدها، لتقليل الأضرار ، والخسائر المحتملة، ويجب عليهم الإبلاغ عن أي هجمات إلكترونية إلى

---

(١) تاريخ الاطلاع ٨/ ٢٠٢٣

https://www.unodc.org/romena/ar/cybercrime.html

(٢) الاستراتيجية الوطنية للأمن السيبراني لدولة الكويت ،الهيئة العامة للاتصالات وتقنية المعلومات ،٢٠١٧-٢٠٢٠،ص٢٩.

(٣) الدكتور / راشد محمد المرى، الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر ، دار النهضة ،٢٠١٨،ص١٢

(٤) الخطر حادث غير محقق الوقوع، الدكتور/ محمود سمير الشرقاوي، الخطر في التامين البحري، الدار القومية للطباعة والنشر القاهرة ،السنة ١٩٦٦،ص٢٣.

(٥) الدكتور / خضر إسماعيل ،أساسيات امن المعلومات والحاسوب، دار الحامد للنشر والتوزيع ،السنة ٢٠١٠،ص٣٤.

(٦) منصات التجارة الإلكترونية مواقع لعرض ،وبيع المنتجات ،والخدمات المختلفة عبر الإنترنت حتى يمكن للمستهلكين إتمام عملية الشراء دون بذل أي وقت وجهد، حيث يتم توصيل المنتجات عبر شركات الشحن.

(٧) الدكتور/ حسام محمود فهمي، الفيروسات والحاسبات كل ئ عنها، دار الحكيم للطباعة القاهرة ،السنة ٢٠٠٤،ص١٦٠

السلطات المختصة، ويجب على منصات التجارة الإلكترونية إخطار عملائها بأي خروقات للبيانات قد تؤثر عليهم.

أولاً: أشكال الهجمات الشائعة على متعاقدين التجارة الإلكترونية:

أ: التصيد الاحتيالي للمتعاقدين في التجارة الإلكترونية (جرائم الاحتيال والاعتداء على بطاقات البنوك):

يتمثل التصيد الاحتيالي في أرسال رسائل احتيالية بالبريد الإلكتروني ،أو الرسائل القصيرة أو الدردشة للمستهلك الإلكتروني[١]، أو العميل لتسويق منتج وهمي ،أو جوائز ،أو مشاريع وهمية، أو يرسل المهاجمون رسائل، كأنها من مصادر مشروعة، مثل البنوك ،أو الشركات ،أو المؤسسات، ويحاولون خداع مستلم الرسالة لفتحها، أو فتح مرفقات ضارة ،لأقناعه بتقديم معلومات سرية، مثل كلمات المرورالسرية ، أو أرقام بطاقات الائتمان ، ويقع ضحية التصيد الاحتيالي كسرقة الهوية الشخصية ،أو الخسارة المالية ،أو الاستيلاء على الحساب.

يرسل أحد المهاجمين بريدًا إلكترونيًا ،أو رسالة إلى صاحب شركة ،أو عملاء ،أو المستهلكين، مدعيًا أنه من البنك الخاص بهم، ويطلب منه التحقق من تفاصيل حسابه، والغرض من ذلك الحصول على رقم بطاقة الائتمان ،أومن خلال فتح رابط يرسله مما يؤدي إلى موقع ويب مزيف ثم يستولى علي حسابة ،وبياناته الشخصية، والهدف من ذلك سرقة المعلومات السرية ،مثل كلمات المرور، والبيانات الحساسة، و المعلومات الشخصية ،أو المصرفية، أو من خلال انتحال شخصية طرف آخر موثوق به، أو معروف[٢]،وتعتبر هجمات التصيد الاحتيالي وسيلة الهجوم المفضلة لدى مجرمي

---

(١) المستهلك الإلكتروني هو الفرد الذين يستخدم الإنترنت ،والتكنولوجيا الرقمية للبحث عن السلع ،والخدمات للتسوق عبر الإنترنت، وهو شخص يفضل القيام بعمليات الشراء ،والتسوق والتفاعل عبر الإنترنت بدلاً من الأساليب التقليدية.

الاطلاع ٨/ ٢٠٢٤

(2)https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity

الإنترنت[١].

ب: أرسال برامج ضارة أو خبيثة للمتعاقدين في التجارة الإلكترونية:

تتضمّن مجموعة من البرامج التي تم إنشاؤها من أجل منح أطراف ثالثة، إمكانية الوصول غير المصرّح به إلى البيانات ،والمعلومات السرية للعملاء ،أو المستهلكين [٢]،و ايضاً تنزيل مرفقات ضارة تثبّت برامج ضارة على أجهزة الشركة، أو العملاء للاستيلاء على المعلومات، و إصابتها برموز خبيثة [٣]، لتعطيل سير العمل العادي للبنية الأساسية للشركة[٤]، ومن الأمثلة الشائعة للبرمجيات الخبيثة أحصنة طروادة، وبرامج التجسس ،والفيروسات، فهى برامج تم تصميمها لتدمير البيانات[٥] ،أو سرقتها[٦]،و تعطيل شبكة الشركة ،أو أجهزة العملاء[٧]،وايضاً الهجوم على الخادم الذي يوفر الموارد ،والبيانات [٨]،وهدفة تعطيل الخدمة ، وهوعبارة عن جهد منسّق لإرباك الخادم ،وإغراقه عن طريق إرسال عدد كبير من الرسائل

---

(1)Types of cybersecutity
https://www.sailpoint.com/identity-library/five-types-of-cybersecurity

مقال منشور تاريخ الاطلاع٩/ ٢٠٢٤

(٢) الدكتور ادريس عطية ،مكانة الأمن السيبرانى في منظومة الأمن الوطني الجزائري، مصداقية، لا يوجد سنة ،ص٥١٥.

(٣) الدكتور / ايمن الحربي، مقدمة في الأمن السيبرانى، معهد البحوث والدراسات ،واحة ام القري.

(٤) لامية، التهديدات والجرائم السيبرانية تأثيرها على الأمن القومي واستراتيجيات مكافحتها ، مجلة الدراسات القانونية والسياسية ،السنة٢٠٢٠،ص٦٥.

(٥) سلام لامية، الجرائم الإلكترونية بعد جديد لمفهوم الأجرام عبر منصات التواصل الاجتماعي ، مجلة الرواق للدراسات الاجتماعية والإنسانية، السنة ٢٠٢٠،ص٤٦٥.

(٦) الدكتور / ذياب البدائية، الأمن وحرب المعلومات ، دار الشروق ،السنة ٢٠٠٦،ص٢٩٢.

(7)https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity

تاريخ الاطلاع ٨/ ٢٠٢٤

(٨) الدكتور/ حيدر فالح سلمان، المرجع السابق ذكرة، ص١٣٧.

جهد منسّق لإرباك الخادم ،وإغراقه عن طريق إرسال عدد كبير من الرسائل المزيفة[١].

تضر الهجمات الإلكترونية شركات، وعملاء التجارة الإلكترونية من خلال وسائل مختلفة، مثل التصيد الاحتيالي ،أو البرامج الضارة، و تسبب تلك الأفعال، عدم رضا العملاء، أو فقدان المبيعات ،أو الإضرار بسمعة الشركة، أو تسريب بيانات شركات التجارة الإلكترونية ،كمعلومات العميل ،أو تفاصيل المنتج ،أو سجلات المعاملات، من خلال الوصول الى قاعدة بيانات العملاء، وسرقة معلوماتهم الشخصية ،والمالية، أو حذف طلباتهم، ولمنع الهجمات، تحتاج منصات ،وأنظمة التجارة الإلكترونية إلى تنفيذ تدابير، وقواعد الأمن السيبرانى، مثل التشفير ،والمصادقة ،والترخيص ،و جدارن الحماية ،ومكافحة الفيروسات ،والنسخ الاحتياطي، وتحديثها بانتظام.

ج: ابتزاز متعاقدين التجارة الإلكترونية :

تعتبر مجموعة واسعة من التقنيات تستخدمها الجهات المسيئة، والمجرمون لابتزاز أموال الشركات ، والعملاء بعد الاستيلاء على بياناتهم ،ومعلوماتهم الشخصية[٢]، وإجبارهم على دفع أموال[٣]،مقابل عدم تسريب تلك المعلومات السرية.

---

(1) https://www.fortinet.com/resources/cyberglossary/what-is-Cybersecurity
تاريخ الاطلاع٨/ ٢٠٢٤

(٢) الاستراتيجية الوطنية للأمن السيبرانى ،وزارة الاتصالات وتكنولوجية المعلومات الأردن ،السنة ٢٠٢١،ص١٨.

(٣) الدكتور/ قاسم محمد حسين، أساسيات في الأمن السيبرانى، كلية الكنوز الجامعية ،قسم الأمن السيبراني،ص١٠.

د: التهديد الداخلي(موظفون شركات التجارة الإلكترونية):

يعتبر التهديد من داخل المؤسسة ،أو الشركة من الموظفين العاملين بها، خطر أمني كبير يهدد المؤسسة، ويسبّبه الأفراد ذوي النوايا السيئة داخل المؤسسة[١]، لما يمتلكه الموظفون من سرعة في الوصول بسرعة إلى الأنظمة ،والبيانات، والمعلومات [٢]، ويمكنهم أن يزعزعوا استقرار أمن البنية الأساسية للمؤسسة من الداخل[٣]،وقد عاقب المشرع المصري بالحبس مدة لا تقل عن ستة أشهر ، وبغرامة لا تقل عن ثلاثين ألف جنيه ، ولا تجاوز خمسين ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من دخل إلى موقع، أو حساب خاص ، أو نظام معلوماتي مستخدماً حقاً مخولاً له[٤].

ثانياً: سبل حماية المتعاقدين في عقود التجارة الإلكترونية بالأمن السيبرانى:

الأمن السيبرانى أساسي ،وجوهري للأطراف في عقود التجارة الإلكترونية، وبدون الأمن الكافي، فإن الشركات، والمتاجر تخاطر بخسارة عملائها، وسمعتها، وإيراداتها، ولذلك يجب على منصات التجارة الإلكترونية ،والمتعاقدين،

---

(١) الدكتور / ماركو إبراهيم ، حماية أنظمة المعلومات، دار الحامد، السنة ٢٠١٣،ص ٣٨.

(2) https://www.comptia.org/content/articles/what-is-Cybersecurity
تاريخ الاطلاع٨/ ٢٠٢٤

(٣) الدكتور/ راشد محمد عبدة ،امن و حماية الوثائق الإلكترونية ،دار الجوهرة ،السنة ٢٠١٥،ص٢٢٢.

(٤) المادة ١٥ من قانون تقنية المعلومات، بالحبس مدة لا تقل عن ستة أشهر ، وبغرامة لا تقل عن ثلاثين ألف جنيه ،ولا تجاوز خمسين ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من دخل إلى موقع ،أو حساب خاص ،أو نظام معلوماتي مستخدماً حقاً مخولاً لها من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة تقنية المعلومات ولائحته التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم ١٦٩٩لسنة ٢٠٢٠.

والمستهلكين الالتزام بمبادئ ،وقواعد الأمن السيبراني كأولوية استراتيجية، وتخصيص ما يكفي من الموارد للاهتمام بها[١]، ويعد الأمن السيبراني عنصر فعال، في إتمام عقود التجارة الإلكترونية، لأنه يحمي كلاً من الشركات، والتجار، والمستهلكين من التهديدات، والهجمات المختلفة عبر الإنترنت، حيث تتعامل شركات التجارة الإلكترونية مع بيانات العملاء الحساسة مثل المعلومات الشخصية ،وتفاصيل بطاقة الائتمان، والتي يمكن الاستيلاء عليها ،واستغلالها من قبل المتسللين ،ومجرمي الإنترنت، ولذلك الالتزام بتدابير الأمن السيبراني ، يحقق فوائد متعددة للشركات ،والتجار، والعملاء في مجال التجارة الإلكترونية.

١: تأمين الأمن السيبرانى للشركات و المتاجر الإلكترونية:

الثقة بين الأفراد عبر الأنترنت أ مر غاية في الصعوبة، ومعظم الأفراد يثقون في الشركات، والمتاجر التى تمتلك سجل حافل[٢]،ومن معايير الأمان تعامل المتعاقدين، أو المستهلكين مع بوابات المتاجر الموثوق بها و التي تعطي الأولوية للأمان الإلكتروني، الذي يعتبر أمر حتمي لعقود التجارة الإلكترونية، لحماية البيانات ،والمعلومات الشخصية ،والسرية، كما تساعد تدابير الأمان القوية على الحد من مخاطر الاحتيال المالي ،وتساعد على بناء الثقة مع عملائك.

يعتبر موقع الويب الخاص بالشركة، دليل، ومرشد العملاء للثقة في التعامل مع الشركة، والمتجر من خلال تمتعه بسمعة طيبة ، و منصات التجارة الإلكترونية الأمنة التي تلتزم بتدابير الأمن السيبرانى كتشفير البيانات ،و الالتزام بأمنها ،وسرية الرسائل

---

(١) تاريخ الاطلاع ٨/ ٢٠٢٤)-https://blog.present.ca/cybersecurity-is-not optional

(٢) الدكتور / عبد الوهاب محمد عبد الوهاب السادة، التنظيم القانوني للأمن السيبراني ،دار المطبوعات الجامعية ،السنة ٢٠٢٥،ص٨.

المُرسلة بين متصفح المستهلك، ومنصة التجارة الإلكترونية، كما عرض الشركة ،أو المتجر لمؤشرات الثقة مثل أيقونات القفل لموقع الويب لغرس الثقة في العملاء[١]،فيجب ان يكون لدي الشركة ،أو المتجر سجل موثوق في مجال الأمن السيبرانى، كالتزامها تماماً بحماية البيانات، والقدرة على إثبات الضمانات التي لديها بشكل مقنع، واستخدام جدران الحماية ،أو أنظمة كشف التطفل ،أو تصفية أي حركة مرور ،أو طلبات غير مرغوب فيها ،أو ضارة من الوصول إلى موقع الويب ،والمنصة .

٢:التزام منصات التجارة الإلكترونية والشركات بقواعد الأمن السيبرانى:

يجب أن تستخدم منصات التجارة الإلكترونية تدابيرالأمن السيبرانى، التي تمكنها اكتشاف الهجمات الإلكترونية ،ومنعها، مثل أنظمة كشف التسلل ،والوقاية منه، وجدران الحماية لتطبيقات الويب[٢]،ويجب على شركات التجارة الإلكترونية تنفيذ آليات قوية، باستخدام كلمات مرور أمنة ، بإنشاء واستخدام كلمات مرور قوية، ومعقدة ،وتجنب استخدام نفس كلمة المرور لحسابات ،أو خدمات متعددة، ، ومن الضروري تقليل مدة تغيير كلمات المرور، وإحداث آليات تمكن من مواجهة الهجمات على كلمات المرور[٣]،ويجب على شركات،ومتاجر التجارة الإلكترونية مراقبة ،وتدقيق نشاط شبكتها ،وموقعها على الويب، مثل التحقق من الطلبات ،أو الاستجابات ،أو الأخطاء أو السجلات، لاكتشاف ،وتحليل أي سلوك مشبوه ، والتحقق من هوية المستخدمين ،أو العملاء ،و الموظفين ،و الشركاء، ومحاربة انتحال الشخصية ،و الاحتيال ،و سوء الاستخدام من قبل المهاجمين.

---

(١) الاطلاع ٨/ ٢٠٢٤ https://www.cloudflare.com/learning/ssl/what-is-ssl/

(٢) الاطلاع ٨/ ٢٠٢٤ https://www.bolddesk.com/blogs/troubleshooting-gui

(٣) الاطلاع ٨/ ٢٠٢٤ https://cypfer.com/what-are-the-6-types-of-cyber-security/

يجب على منصات التجارة الإلكترونية ،ومقدمي الخدمات تقديم ميزات ،وأدوات الأمن السيبرانى لعملائهم، لمساعدتهم على تعزيز أمان متجرهم عبر الإنترنت، كالمصادقة الثنائية ،وتتم من خلال مطالبة المستخدمين بتقديم تحقق إضافي مثل إرسال الرمز المؤقت إلى أجهزتهم المحمولة، مما يقلل من مخاطر الوصول غير المصرح به بشكل كبير [١]، وأيضا حماية كلمة المرور، وجدران الحماية، ومكافحة الفيروسات، ومكافحة البرامج الضارة، والنسخ الاحتياطي، وتطبيقات المصادقة الثنائية تزيد من الأمان إلى حسابات العملاء،

٣: معالجة منصات ومتاجر التجارة الإلكترونية الأعطال بانتظام وبصورة فورية:

يجب على منصات التجارة الإلكترونية تحديث، و أصلاح أعطال أنظمتها ،وبرامجها بانتظام[٢]، كأنظمة التشغيل، أو تطبيقات الويب، أو قواعد البيانات، لإصلاح أي خطأ ،ومعالجة نقاط الضعف ،والثغرات، أو العيوب الأمنية التي قد يستغلها المهاجمون، وتوفير تحديثات ،وتصحيحات منتظمة لبرامجهم ،وأنظمتهم، لإصلاح أي أعطال ،أو أخطاء يمكن أن تهدد أمان الشركات ،والمتاجر عبر الإنترنت، ومواكبة أحدث معايير الأمن السيبرانى ،وأفضل الممارسات، لذلك من المهم أن يكون لدي منصات التجارة الإلكترونية خطة استجابة سريعة للحوادث السيبرانية التي تمكنهم من التعافي من الهجوم السيبراني بفعالية ،وكفاءة ،وذلك بمعرفة فريق أمن

---

(١) تعد المصادقة الثنائية طريقة أمان لإدارة الهوية ،والوصول تتطلب شكلين من أشكال التعريف للوصول إلى المعلومات ،والبيانات، تمنح المصادقة الثنائية الشركات إمكانية المراقبة ،والمساعدة في حماية المعلومات.

(٢) الاطلاع ٨/ ٢٠٢٤١)-https://cypfer.com/what-are-the-6-types-of-cyber-security/

سيبرانى لضمان المراقبة المستمرة ،و تحديثات البرامج ،وتصحيحات الأمان التي تعمل على إصلاح الثغرات الأمنية[١].

تنظم ،وتحدد خطة الاستجابة للحوادث السيبرانية أدوار، ومسؤوليات فريق المعالجة، وقنوات الاتصال ،والبروتوكولات، واستراتيجيات المعالجة ،والتخفيف، وإجراءات الاستعادة، وتدابير التقييم ،والتحسين، والإبلاغ عن نقاط الضعف المعروفة في البنية الأساسية للمؤسسة،و الحالات الشاذة التي قد تشير إلى هجوم إلكتروني محتمل ،أو مستمر، لذلك فإن التحديث ،والإصلاح المنتظم للأنظمة ،والبرمجيات يساعد على الحماية من الهجمات الالكترونية ،ويقوي الأمان العام للمؤسسة، بخطة منظمة تضمن استجابة المنصة ،وتعافيها فوريًا من الحوادث الأمنية المحتملة.

٤: تعليم وتدريب موظفين منصات وشركات التجارية الإلكترونية على ممارسات الأمن السيبرانى:

يعد الخطأ البشري أحد الأسباب الرئيسية للهجمات الإلكترونية، ويمكن منعه من خلال تثقيف ،وتدريب الموظفين على أهمية ،وأفضل ممارسات الأمن السيبراني للتجارة الإلكترونية، ويتعين على الشركات التجارية تدريب على الموظفين على الأمن السيبرانى لتحديث الفريق دائمًا، فالموظف داخل الشركة عامل مؤثر في حماية الأجهزة[٢]،ويجب وضع برنامج تدريبي داخلي متخصص على إدارة الأنظمة التكنولوجية لرفع درجة وعي[٣]،الموظف بالأمن السيبرانى[٤]،وذلك بصفة دورية

---

(1) https://cypfer.com/what-are-the-6-types-of-cyber-security/
مقال منشور تاريخ الاطلاع ٩/ ٢٠٢٤

(٢) الدكتور / عبد الوهاب محمد عبد الوهاب السادة، المرجع السابق ذكرة،ص٢٠.

(٣) على بينة، ودراية منها عارف بها وبأسبابها

(4) https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity
الاطلاع ٨/ ٢٠٢٤

لمواكبة كل جديد في مجال الأمن السيبرانى[١]، ويجب على منصات التجارة الإلكترونية تثقيف، وتدريب موظفيها على ممارسات الأمن السيبراني[٢]، مثل كيفية التعرف على التصيد الاحتيالي، أو البرامج الضارة ،أو الخبيثة ،وصد الهجمات الإلكترونية، وكيفية حماية بيانات الأجهزة، والعملاء، أو كيفية الإبلاغ عن أي حوادث، أو انتهاكات الأنظمة، والتأكد من درايتهم بسياسات ،وإجراءات الأمن السيبراني، كحماية البيانات، أو الاستجابة للحوادث، أو التعافي من الكوارث ، وبرامج الفدية ورفض الخدمة، ويجب توعيتهم بأهمية النسخ الاحتياطي الذاتي لبياناتهم ،للحفاظ عليها ،وبشكل منتظم من أجل مواجهة الخسائر المحتملة في البيانات في أعقاب هجوم سيبراني ،وتُعتبر مشاركة المعلومات مفتاحًا لضمان تدريب الموظفين على أفضل ممارسات الأمن السيبرانى، و حذف الرسائل الإلكترونية المشبوهة ،والامتناع عن توصيل أجهزة غير معروفة كالفلاشات المجهولة، فيقوم الموظف داخل المؤسسة بدورًا مهمًا في ضمان نجاح استراتيجيات الأمن السيبراني.

٥: نشر الوعى بالأمن السيبرانى بين المتعاقدين في عقود التجارة الإلكترونية(الشركات والعملاء أو المستهلكين):

يجب نشر الوعى بالأمن السيبرانى بين العملاء، والمستهلكين ،وكيفية اتباع سياسات ،والإجراءات الأمنية[٣]كاستخدام كلمات مرور قوية ،وتحديث البرامج ،

---

(١))مقال بعنوان التدريب والتوعية بقضايا الامن السيبرانى منشور على(٦ https://www.cbe.org.eg/ar/cybersecurity/cybersecurity-issues-training-and-awarenessتاريخ الاطلاع ٩/ ٢٠٢٤

(٢) الوعي السيبراني: بانه القدرة على تزويد الفرد بالحد الأدنى من المعارف والمهارات والاتجاهات التي تمكنهم التعامل مع الأمن السيبراني والتعامل معها.

(١) مقال بعنوان تدريب الموظفين على الأمن ٢الاطلاع٨/ ٢٠٢٤

والإبلاغ عن الحوادث[١]، وينبغي إعلامهم بالفوائد التي توفرها إجراءات الأمن السيبرانى ،بالإضافة إلى النصائح ،والاحتياطات اللازمة لحماية معلوماتهم الشخصية ،والمالية عبر الإنترنت، حيث يعتبر نقص الوعي ،والتعليم بين المتعاقدين، أو العملاء في مجال التجارة الإلكترونية، من المخاطر التي تهدد المعاملات، وعقود التجارة الإلكترونية[٢]،فقد يهمل العملاء ،والمستهلكون فى تقديرهم للمخاطر ، والعواقب المحتملة للهجمات السيبرانية، فلا يتحققون من مصداقية ،وأمن منصات ،ومواقع التجارة الإلكترونية التي يزورونها، أو قد يستخدمون نفس كلمة المرور لحسابات متعددة، أو قد لا يستخدمون طرق دفع آمنة، أو قد لا يراقبون معاملاتهم ، وبياناتهم عبر الإنترنت، فيتعرضون للمخاطر كسرقة الهوية ،والاحتيال ،و التصيد الاحتيالي ، والجرائم الإلكترونية الأخرى.

يجب على منصات، و شركات التجارة الإلكترونية ، تثقيف عملائهم ، لرفع مستوى الوعي ،والتثقيف بشأن الأمن السيبراني للتجارة الإلكترونية ، لمساعدتهم على فهم أهمية الأمن السيبراني ،وأفضل الممارسات التي يجب اتباعها، ويجب عليهم أيضًا تقديم التوجيه ،والدعم لعملائهم لمساعدتهم في التعامل مع أي مشكلات ،أو حوادث أمنية، لضمان نجاح معاملات ،وعقود التجارة الإلكترونية.

---

employeeslk-for-security-cyber/base-knowledge/org.academyibs//:https

(١) تقرير بعنوان الأمن السيبرانى في مؤسسات منظومة الأمم المتحدة، تقرير وحدة التفتيش المشتركة، الامم المتحدة ،السنة ٢٠٢١.

(٢) الدكتور / محمد سعيد ،التامين الإلكتروني ضد المخاطر السيبرانية ،المجلة الدولية للقانون ،دار نشر قطر ،٢٠٢١ص٩

٦: الالتزام بالقوانين واللوائح التي تحكم عقود التجارة الإلكترونية:

تعمل منصات التجارة الإلكترونية في شبكة معقدة ، ومترابطة من المتعاقدين، مثل الموردين والشركاء، والمنافسين، والعملاء، أو المستهلكين ويجب على المتعاقدين في مجال التجارة الإلكترونية التعاون، والتنسيق مع بعضهم لإنشاء بيئة آمنة ،وجديرة بالثقة عبر الإنترنت ،والحفاظ عليها بالالتزام بالقوانين، واللوائح التي تحكم عقود، ومعاملات التجارة الإلكترونية[١] (،كقوانين حماية البيانات، والخصوصية المختلفة التي تطبق على معاملات، وعقود التجارة الإلكترونية،نظرا لأهمية دور هذه القوانين فى حماية حقوق ،ومصالح العملاء ،والمستهلكين، والشركات عبر الإنترنت، وايضاً مطالبة منصات ،وشركات التجارة الإلكترونية بالحصول على التراخيص اللازمة، واحترام حقوق العملاء .

٧: التزام المتعاقدين في عقود التجارة الإلكترونية بالأمن السيبراني بشكل دائم:

تتطور التهديدات، والهجمات السيبرانية باستمرار، وتصبح أكثر تعقيدًا، ولذلك يجب أن تكون الحلول ،والممارسات الأمنية التي تتبناها منصات ،وشركات التجارة الإلكترونية حديثة ،ومتطورة ،وحديثة، ومواكبة لتطور التهديدات، والهجمات[٢]، ويجب على شركات ،ومنصات التجارة الإلكترونية تحديث أنظمتهم ،وسياساتهم الأمنية بصورة دورية، وإجراء عمليات تدقيق ،وتقييم دورية لتحديد، ومعالجة أي نقاط ضعف ،أو ثغرات تكون هدف للمتسللين، فالأمن السيبراني عملية دائمة ،ومستمرة ،ومتطورة يجب الالتزام بها بصورة دورية، ومنتظمة.

---

(١) تاريخ الاطلاع ٨/ ٢٠٢٤١) https://gca.isa.org/blog/why-collaboration-is-essential-for-cybersecurity-teams

(٢) تاريخ الاطلاع ٨/ ٢٠٢٤٢)

https://www.sciencedirect.com/science/article/pii/S235286482100047X

رابعاً: أثر الأمن السيبرانى على التجارة الإلكترونية:

يعد الأمن السيبرانى للمتعاقدين في التجارة الإلكترونية أمرً حيوي، وضروري ، وتعمل منصات التجارة الإلكترونية ،و الشركات على مواجهة الجرائم الإلكترونية[١]،حيث تتعرض تلك المنصات ،والشركات باستمرار لتهديدات إلكترونية جديدة ،ومتطورة، مثل برامج الفدية ،و التصيد الاحتيالي ،ورفض الخدمة ،وخرق البيانات، ،أو سرقة البيانات ، ويتعين عليهم أن يكونوا استباقين ،ويقظين في الدفاع عن أنظمتهم ،وأصولهم من هذه التهديدات، و حماية أنظمتهم من وصول المخترقين اليها، وذلك بالالتزام بلوائح ،ومعاييرالأمن السيبراني، وتطوير فرق الأمن السيبرانى لديها، مما يحقق لهم العديد من الفوائد كالتالي:

١: الالتزام بالأمن السيبراني يعزز ثقة المتعاقدين في منصات وشركات التجارة الإلكترونية:

تعتبر أهم أهداف الأمن السيبرانى السرية ،والسلامة ،و حماية بيانات المتعاقدين[٢]،وهى اهم عوامل نجاح عقود التجارة الإلكترونية ،فتعتمد العقود التجارية عبر الإنترنت على ثقة عملائها، وولائهم للحفاظ على عملياتها، ويتوقع المتعاقدين أن توفر لهم المنصات ،والشركات عبر الإنترنت تجربة تسوق آمن، وموثوق به، فيتسوق العملاء عبر الإنترنت تسوق أمن عبر منصات التجارة الإلكترونية التي تتمتع بميزات التسوق الإلكتروني الذي يجذب

---

(١) كامل خضر ،سمر المداح، العلاقة بين الاقتصاد الرقمي ،وامن المعلومات ،دراسة تطبيقية ،المجلة العلمية للاقتصاد والتجارة، العدد ٣،السنة ٢٠٢٠،ص١٢.

(٢) الدكتور / حسن الصاوي، الدكتور/ خالد الشلفان ،امن الشبكات والنظم المفاهيم والتقنيات ،لا يوجد دار نشر ،السنة ٢٠١٣،ص٢٤.

المستهلك[١]،فتقوم معاملات التجارة الإلكترونية عبر الإنترنت بجمع ،وتخزين المعلومات، والبيانات الحساسة من عملائها، مثل الأسماء ،والعناوين ،وأرقام بطاقات الائتمان ،وكلمات المرور، والتفضيلات، وتعتبر هذه البيانات ذات قيمة عالية بالنسبة للمتسللين ،ومجرمي الإنترنت الذين يمكنهم استخدامها من الاحتيال ،أو الابتزاز.

يدرك المتعاقدين في عقود التجارة الإلكترونية بشكل متزايد أهمية حماية بياناتهم الشخصية، من خلال التزام المنصات ،والشركات ،والتجار بتدابير بالأمن السيبراني، من خلال تشفير البيانات، واستخدام بروتوكولات آمنة، وتنفيذ آليات مصادقة ،وتفويض قوية ،ويعمل الأمن السيبراني على حماية بيانات المؤسسات، والأفراد من التهديدات الداخلية، والخارجية سواء كانت عرضية ،أو ذات نوايا خبيثة، من الموظفين السابقين ،أو البائعين الخارجيين، ويضمن الأمن السيبراني أيضا إمكانية وصول الموظفين إلى الإنترنت عند الحاجة دون تهديدات بخرق البيانات، مما يساعد الشركات في بناء الثقة مع عملائها ،والعلاقات طويلة الأمد، حيث يساعد تنفيذ تدابير الأمن السيبراني القوية المؤسسات على بناء الثقة مع عملائها ،والمتعاقدين ، فيساعد ألأمن السيبراني على نجاح عقود التجارة الإلكترونية ،وبذلك الالتزام بتدابير بالأمن السيبرانى يؤدي إلى تعزيز رضا المتعاقدين وثقتهم في المنصات ،والمتاجر الإلكترونية، والاحتفاظ بهم، بالإضافة إلى جذب عملاء جدد يقدرون الأمان ، والراحة.

---

(١) الدكتور/ عبد العزيز فتحي العلواني، حماية المستهلك الإلكتروني وفق نظام التجارة الإلكترونية، مجلة الصدي للدراسات القانونية والسياسية ،العدد السابع ،السنة ٢٠٢١،ص٣٠.

٢: الأمن السيبرانى يخفض تكاليف الشركات والمتاجر ويرفع مستوي الإنتاج:

يمكن لشركات التجارة الإلكترونية توفير المال ،والمصاريف، والموارد عن طريق منع ،أو تقليل تأثير الهجمات الإلكترونية، والتي يمكن أن تسبب لها خسائر مالية كبيرة كانتهاكات للبيانات، والإضرار بالسمعة، وذلك من خلال الاستثمار في حلول الأمن السيبراني ،والالتزام بها، وتنفيذها فتستطيع منصات التجارة الإلكترونية،بالأمن السيبراتى تجنب تكاليف التعافي من الحوادث السيبرانية، مثل استعادة البيانات، وتعويض العملاء، ودفع الغرامات، وإصلاح الأنظمة، ،وتساعد تدابير الأمن السيبراني، وتدابير الأمن السيبرانى الشركات على تحسين إنتاجيتها[١]، من خلال حماية أنظمتها من الهجمات، مما يوفر عليها مبالغ كبيرًة[٢]،والاطلاع الدائم بالاتجاهات الحديثة للمخترقين، يوفر علي الشركات وقت التوقف عن العمل.

فالمنصات ،والشركات التي تنفذ جميع تدابير الأمن السيبرانى، كاستخدام جدران الحماية ،وبرامج مكافحة الفيروسات ،وبرامج مكافحة البرامج الضارة لحماية موقعها الإلكتروني ،وخوادمها من الهجمات الضارة، وتستخدم أنظمة النسخ الاحتياطي، والاسترداد لاستعادة بياناتها ،ووظائفها في حالة وقوع كارثة، توفر الكثير من الوقت ،ويجعلها تركز على وظائفها الأساسية، لتعزيز قدرتها الإنتاجية[٣]،وتركز

---

(١) تقرير بعنوان الأمن السيبرانى في مؤسسات منظومة الأمم المتحدة، تقرير وحدة التفتيش المشتركة، الامم المتحدة ،السنة ٢٠٢١.

(٢) https://cypfer.com/what-are-the-6-types-of-cyber-security تاريخ الاطلاع ٨/ ٢٠٢٤/

(٣) https://cypfer.com/what-are-the-6-types-of-cyber-security/ تاريخ الاطلاع ٨/ ٢٠٢٤

على المشاريع ،والتوسعات المستقبلية، ويكون لدى الموظفين الوقت الكافي للتركيز على الأعمال الأساسية، وتنمية الابتكار.

٣: الأمن السيبرانى يحمى سمعة منصات وشركات التجارة الإلكترونية:

تستخدم منصات التجارة الإلكترونية ،والشركات تدابير الأمن السيبرانى لتعزيز نظام الأمان الخاص بها ، لتجنب أي هجمات، أو تهديدات غير متوقعة، فيمنع الأمن السيبراني الضرر الذي يلحق بسمعه الشركات نتيجة لانتهاكات البيانات ،والهجوم على الأنظمة، والمعلومات ، والتي يمكن أن تؤدي إلى فقدان ثقة العملاء، والمتعاقدين[١]،من خلال تسريب بياناتهم ،ومعلوماتهم السرية ،والاستيلاء على أموالهم مما يفقد المنصة ،أو الشركة سمعتها التجارية، وانخفاض فرصها في تحقيق الربح، بالأمن السيبراني تحمى المنصات ،والشركات البيانات من الاختراقات ، وبالتالى تحافظ على سمعتها ككيانات موثوقة[٢].

٤: الأمن السيبرانى يشجع على التنافس بين شركات ومتاجر التجارة الإلكترونية:

شركات التجارة الإلكترونية الملتزمة بالأمن السيبراني تكون قادرة على التنافس، من خلال جذب العملاء ،والمتعاقدين بتقديم منتجات آمنة ،وخدمات موثوقة عبر الإنترنت، والحفاظ على بيانات ،ومعلومات المتعاقدين ،مما يمنحهم تجربة تسوق امنه ،والتي تميزها عن الشركات الآخرين في السوق.

---

(١) https://cypfer.com/what-are-the-6-types-of-cyber-security/ تارخ الاطلاع ٨/ ٢٠٢٤

(٢) وليد احمد ،الفرق بين امن المعلومات والأمن السيبرانى ،صحيفة الجزيرة الإلكترونية ،مؤسسة الجزيرة الإلكترونية للصحافة ،السنة ١٤٣١،ص٣٤.

المطلب الثانى
الوسائل القانونية لمكافحة الجرائم الإلكترونية

تمهيد وتقسيم:

من اكثر الصعوبات التي تواجه التعامل الأمني مع الجرائم الإلكترونية بعد وقوعها هي صعوبة اكتشافها من قبل الضحايا، سواء كانوا عملاء أو شركات، والكثير من هذه الجرائم يمر دون ان يتم اكتشافه، و قد يتم محو أثارها، و يتطلب ذلك النوع من الجرائم خبراء ومتخصصين في الأمن السيبرانى للحماية من تلك الجرائم، لقدرتهم على معرفة تقنيات الحاسب الآلي ونظم المعلومات للتحقيق فيها ومقاضاة فاعلها،من خلال تتبع فاعلها والتحقيق فيها وفرض تشريعات تمنع تكراراها،سنقسم هذا المطلب كالتالي:

الفرع الأول: تتبع مرتكبي جرائم الأمن السيبرانى

الفرع الثانى: قواعد الأمم المتحدة الموحدة لتسهيل حركة التجارة الإلكترونية.

الفرع الثالث: القانون الواجب التطبيق على الجرائم الإلكترونية.

الفرع الرابع: المسؤولية عن الجرائم الإلكترونية

الفرع الأول
تتبع مرتكبي جرائم الأمن السيبرانى

أولاً: سبل ضبط وتتبع المتسللين والمخترقين:

أ: تتبع عناوين IP لمرتكبي الجرائم الإلكترونية:

يعد تتبع عناوين IP وهو عنوان فريد يعرّف جهازٌ الكمبيوتر على الإنترنت ، أو شبكة محلية من اهم سبل مكافحة جرائم المعلومات[١]،و بعد ان أصبحت مصدر قلق كبير للعملاء ، والشركات، وباتت تشكل تهديدا كبيرا للأمن السيبراني، فيساعد تتبع عناوين IP في تحديد موقع المخترق عند حدوث جريمة إلكترونية، لإنفاذ القانون ،وتحديد الولاية القضائية على القضية ،ومحاكمة الجاني[٢]،ومعرفة مصدر تهديد الشركات ،أو العملاء.

١ـ يساعد تتبع عناوين IP في تحديد نوع الجهاز المستخدم في الهجوم:

يساعد تتبع عناوين IP أيضاً في تحديد نوع الجهاز المستخدم في الهجوم سواء جهاز كمبيوتر ،أو هاتف محمول[٣] ، و بالتالي تساعد هذه المعلومات في تحديد مستوى تطور المجرم الإلكتروني ،فإذا كان المهاجم يستخدم جهازاً محمولاً، فقد يشير ذلك إلى أن الهجوم تم تنفيذه بواسطة متسلل مبتدئ.

٢ـ يساعد تتبع عناوين IP في منع الهجمات المستقبلية:

يساعد تتبع عناوين IP في منع الهجمات المستقبلية على العملاء ،والشركات من خلال تحديد نقاط الضعف في النظام الشبكى، ومعالجتها ، وتقوية الشبكة التي

---

(1) https://fastercapital.com/arabpreneu

(٢) الدكتور/ حسين سعيد الغافري ،السياسة الجنائية في مواجهة جرائم الأنترنت، دار النهضة العربية، السنة ٢٠٠٩،ص٣٤.

(٣) الدكتور/ خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب ،دار الثقافة والنشر ،السنة ٢٠١١،ص٦٨

تعرضت للهجوم، فتساعد هذه المعلومات في تنفيذ الإجراءات الأمنية المناسبة لمنع وقوع هجمات مماثلة في المستقبل ،فإذا كان المهاجم تمكن من الوصول إلى النظام من خلال ثغرة أمنية في البرنامج، فيمكن تحديث البرنامج ،وإصلاحها لمنع هجمات مماثلة في المستقبل.

٣ـ يساعد تتبع عناوين IP في الدعاوى المدنية:

يساعد تتبع عناوين IP أيضاً في تحديد اختصاص المحاكم من خلال تحديد مصدر التشهير بالشركات والعملاء عبر الإنترنت ،أو انتهاك حقوق الملكية الفكرية، ومتابعة الإجراءات القانونية ضد الجاني وطلب التعويض عن الأضرار.

ب: ضبط من يحاول دخول مبنى الشبكات المعلوماتية الخاصة بالمنصات ،والشركات بغرض سرقة ،أو إتلاف البيانات ،والمعلومات الرقمية، الخاصة بالعملاء وملاحظة أي دخول الى النظام الشبكي ،وتتبع أى شخص متصل بالنظام الشبكى من خارج المؤسسة بواسطة أى نوع من أنواع الاتصال الشبكي من خلال مراقبة كلمات المرور الخاصة، وذلك عن طريق برمجيات متطورة لاكتشاف الخطر ،وتتبع أية نشاطات مشبوهة على الشبكة، والقبض على المخترقين.

ج: يمكن اكتشاف الجريمة الإلكترونية من قبل موظفين الشركات المدربين، من خلال ملاحظة أى تلف البيانات، أو تعديل بعض الملفات، ويمكن أن يتم هذا الاكتشاف من قبل أحد العملاء، أو المستهلكين الذي قد يشتبه في دخول شخص آخر الى جهازه بشكل غير شرعي، ويمكن تتبعه ،وضبطه بمجرد الإبلاغ، وتتبع الرابط الخاص به.

ثانياً: التحقيق الجنائي الرقمي:

هو عمل يقوم بة مأمور الضبط لضبط الجرائم الإلكترونية ،وتقديم المجرم للعدالة [١]،ويعتبر التحقيق الجنائي الرقمي عملية فراسة ،ودراسة[٢]،بالتحقيق في الجريمة المرتكبة باستخدام الأجهزة الإلكترونية، مثل أجهزة الكمبيوتر، والهاتف المحمولة ،وأجهزة الشبكات ،و أجهزة تخزين المعلومات، وهو عبارة عن فحص جهاز المجرم الإلكتروني من قبل المحققين بفحص الحاسوب ،أو الأجهزة المختلفة،ويتم التحقيق الجنائي الرقمي من خبراء لديهم القدرة على فحص الهجمات الإلكترونية،ويتم إجراء التحقيق الجنائي الرقمي بالتحفظ على الأدلة الرقمية ،وتحديدها ،واستخدامها أمام القضاء[٣]

يتم التحقيق الجنائي الرقمي كالتالى:

أ: تدوين التحقيق الإلكتروني [٤]،والتحفظ على كافة الملفات التي تم الاستيلاء عليها من قبل المخترقين بعد استردادها ،والتحفظ على كافة الأدلة المتعلقة بالتحقيق في أكثر من مساحة ،وتخزينها بسرية[٥]،و تقديمها كدليل للقضاء لإدانة المخترق.

---

(١) الدكتور/ مصطفي محمد موسي ،التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة ،السنة ٢٠٠٩،ص١٩.

(٢) الدكتور/ محمد انور عاشور ،المبادئ الأساسية في التحقيق الجنائي العملي، عالم الكتب ،السنة ١٩٨٧،ص٣٤.

(٣) (الدكتور / خالد محمد عجاج ،اصول التحقيق الجنائي ،دار التعليم الجامعي ،السنة٢٠١٨،ص١٠.

(٤) المادة ٢٤ من قانون الإجراءات الجنائية المصري.

(٥) الدكتور/ جميل عبد الباقي الصغير، ادله الأثبات الجنائي والتكنولوجيا الحديثة ،دار النهضة العربية ،السنة ٢٠٠١،ص٥٦.

ب:معرفة الدافع على الجريمة، واكتشاف الركن المادي ،والمعنوي للجريمة[١]، وتحديد هوية الجاني الرئيسية، و علاقته بالضحية لتسهيل القبض علية.

ج: تجهيز مجموعة من التقارير الجنائية ،وتقديم تقرير كامل نهائى عن عملية التحقيق ،وتعرض القضايا بالأدلة الإلكترونية لا ثباتها[٢]،والبحث لتقديمة للقضاء[٣]

(١) الدكتور/ خالد ممدوح إبراهيم ،فن التحقيق الجنائي في الجرائم الإلكترونية ،دار الفكر الجامعي، السنة ٢٠١٨،ص٥٢

(٢) مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ،السنة ٢٠١٥

(٣) (الدكتور/ مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري ،دار النهضة ،السنة ٢٠٠٨،ص٦٣٢.

الفرع الثانى
قواعد الأمم المتحدة الموحدة لتسهيل حركة التجارة الإلكترونية

اولاً: اتفاقية الأمم المتحدة بشأن استخدام الخطابات الإلكترونية في العقود الدولية نيويورك ٢٠٠٥

تعرف الاتفاقية الدولية على أنها اتفاق مكتوب يتم بين أشخاص القانون الدولي الخاص بقصد ترتيب آثار قانونية معينة في القانون الدولي الخاص . تحكم معاملات التجارة الدولية[١]،وتعتبر اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية (نيويورك ٢٠٠٥)، تعتبر أول معاهدة تكفل اليقين القانوني للتعاقد الإلكتروني في التجارة الدولية، لتيسير استخدام الأشكال الإلكترونية من المستندات ،والصكوك القابلة للتحويل، مثل سندات الشحن ،والكمبيالات ، والشيكات ،وإيصالات المستودعات، وتهدف اتفاقية الخطابات الإلكترونية إلى تسهيل استخدام الخطابات الإلكترونية في التجارة الدولية عن طريق التأكّد من أن العقود المبرمة ،وغيرها من الخطابات المتبادلة إلكترونيا صحيحةٌ ،وموثوق بها ، وقابلةٌ للتنفيذ كالعقود ،والخطابات الورقية التقليدية[٢].

أهمية الاتفاقية:

لها دوراً بارزاً في إزالة العقبات التي تعرقل استخدام الخطابات الإلكترونية في العقود الدولية، وخاصة فى التشكيك بالقيمة القانونية للخطابات الإلكترونية لذا سعت هذه الاتفاقية الى تذليل تلك العقبات من خلال إرساء قواعد دولية لتحقيق التكافؤ بين الخطابات الإلكترونية ،و الورقية، وتنطبق هذه الاتفاقية عند استخدام الخطابات

---

(١) الدكتور/ طارق عبد العال حماد ،التجارة الإلكترونية (الأبعاد التكنولوجية والمالية)،الدار الجامعية ،السنة ٢٠٠٨، ص٢٣٤.

(٢) اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية (نيويورك ٢٠٠٥).

الإلكترونية في تكوين ،او تنفيذ عقد ، تم بين اطراف تقع مقار أعمالهم في دول مختلفة ، مع الإشارة الى انه يكفي لتطبيقها ان تكون احدى الدولتين هي دولة متعاقدة في هذه الاتفاقية بما يؤدي بالنتيجة الى تطبيق قانون دولة متعاقدة، وتهدف الى تذليل العقبات الرسمية من خلال تحقيق التكافؤ بين شكلي الخطابات الإلكتروني ، والمكتوب، وتسهيل حركة التجارة الإلكترونية ،لتنطبق الاتفاقية على جميع الخطابات الإلكترونية المتبادلة بين طرفين يقع مقرا عملهما في دولتين مختلفتين، على أن يكون مقر عمل أحدهما على الأقل موجودا في دولة متعاقدة، لبث الثقة بين متعاقدين التجارة الإلكترونية في الخطابات، والمراسلات الإلكترونية ،و تُستبعد من نطاق انطباق الاتفاقية العقود المبرمة لأغراض شخصية ،أو عائلية، أو منزلية، كالمتعلق منها بقانون الأسرة، و تحدّد الاتفاقية معايير تحقّق التكافؤ الوظيفي بين الخطابات الإلكترونية ،والمستندات الورقية، وكذلك بين طرائق التوثيق الإلكترونية والتوقيعات الخطية.

ثانياً: قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية ١٩٩٦

يهدف القانون النموذجي بشأن التجارة الإلكترونية إلى مزاولة التجارة من خلال الوسائل الإلكترونية ،وتسهيل حركة الأنشطة التجارية من خلال تزويد الدول بمجموعة قواعد مقبولة دوليا تهدف إلى تذليل العقبات القانونية ،وتعزيز القدرة على التنبّؤ بالتطورات القانونية في مجال التجارة الإلكترونية، والهدف منة التغلّب على العقبات الناجمة عن الأحكام القانونية التي قد لا تكون متنوّعة تعاقديا عن طريق معاملة المعلومات الورقية ،والإلكترونية معاملة متساوية، وهذه المساواة في المعاملة مقوّم أساسي للتمكّن من استخدام الخطابات الإلكترونية ، مما يسهل التجارة الدولية[1]

(١) قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية ١٩٩٦

أهميته:

هو أول نص تشريعي يعتمد المبادئ الأساسية لعدم التمييز ،والحياد ،والتكافؤ الوظيفي التي تعتبر أسس قانون التجارة الإلكترونية، ويكفل مبدأ عدم التمييز فلا يُنكر الأثر القانوني لأي وثيقة ،أو ينفى صحتها ،أو قابليتها للإنفاذ لمجرّد كونها إلكترونيه، وفي ضوء التقدم التكنولوجي السريع، ويهدف إلى استيعاب ما يطرأ من تطوّرات في المستقبل دون الاضطلاع بمزيد من الأعمال التشريعية، ويحدّد مبدأ التكافؤ الوظيفي معايير يمكن بموجبها اعتبار الخطابات الإلكترونية مكافئة للخطابات الورقية، والقانون النموذجي مرفق بدليل اشتراع يقدم معلومات أساسية ،وإيضاحية لمساعدة الدول في إعداد ما يلزمها من أحكام تشريعية[١] .

(١) المرجع السابق ذكرة.

الفرع الثالث
القانون الواجب التطبيق على الجرائم الإلكترونية

يعتبر توفير بيئة قانونية امنه أمرحيوي لتسهيل حركة التجارة الإلكترونية [١]، ولذلك يجب تطبيق عقوبات رادعة على كل من يعتدي علي بيانات ،ومعلومات الغير ،من الشركات ،والعملاء كقواعد قانون العقوبات التي تخضع في تطبيقها من حيث المكان لمبدأ مستقر ،ومعروف ، ألا وهو مبدأ الإقليمية ، والذي يعني خضوع الجرائم التي تقع في إقليم الدولة معينة لقانونها الجنائي ، بحيث يصبح قضائها هو المختص بنظر الجرائم المرتكبة في إقليمها ، ولا تخضع من حيث الأصل لسلطان أي قانون أجنبي، وفي المقابل لا يمتد سريان قانون الدولة الجنائي خارج نطاقها الإقليمي وفقاً لحدودها المعترف بها في القانون الدولي إلاّ في أحوال استثنائية اقتضتها حماية المصالح الجوهرية للدولة، أو متطلبات التعاون، وكما هو معلوم ، فإن الجرائم الإلكترونية لا تستأثر بها دولة بعينها ،فهي بطبيعتها باعتبارها موزعة في كافة أنحاء العالم ،وكل دولة تمارس سيادتها على إقليمها بتطبيق قوانينها داخل حدودها ، بصرف النظر عن جنسية المجرم.

---

(١) الدكتور/ عبد المطلب عبد الحميد، اقتصاديات التجارة الإلكترونية، الدار الجامعية ،السنة ٢٠١٤،ص٢٢٨.

نستعرض القانون المصرى :

أصدر المشرع المصرى القانون رقم ١٧٥ لسنة ٢٠١٨بشأن جرائم تقنية المعلومات ولا ئحتة التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم١٦٩٩لسنة ٢٠٢٠.

تعاريف فى تطبيق أحكام هذا القانون يقص بالألفاظ والعبارات الأتية المعنى لمبين قرين كل منهما[١]:

١ـ **البيانات والمعلومات الإلكترونية** : كل ما يمكن إنشاؤه ،أو تخزينه، أو معالجته، أو تخليقه، أو نقله، أو مشاركته، أو نسخه بواسطة تقنية المعلومات ؛ كالأرقام ،و الأكواد والشفرات ، وما فى حكمها.

٢ـ **بيانات شخصية**: أى بيانات متعلقة بشخص طبيعى محدد ، بشكل مباشر ،أو غير مباشر عن طريق الربط بينها ،وبين بيانات أخرى.

٣ ـ **تقنية المعلومات** : أى وسيلة ،أو مجموعة وسائل مترابطة ،أو غير مترابطة تستخدم لتخزين، واسترجاع، وترتيب، وتنظيم، ومعالجة، وتطوير، وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة ،أو الوسائل المستخدمة سلكياً .

٤ـ **مقدم الخدمة** : أى شخص طبيعى ،أو اعتبارى يزود المستخدمين بخدمات تقنيات المعلومات ،والاتصالات، ويشمل ذلك من يقوم بمعالجة ،أو تخزين المعلومات بذاته ،أومن ينوب عنه فى أى من تلك الخدمات.

٥ـ **المستخدم** : كل شخص طبيعى أو اعتبارى، يستعمل خدمات تقنية المعلومات ، أو يستفيد منها بأى صورة كانت.

---

(١) القانون رقم ١٧٥ لسنة ٢٠١٨بشأن جرائم تقنية المعلومات ولا ئحتة التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم١٦٩٩لسنة ٢٠٢٠.

المحافظة على سرية البيانات التى تم حفظها وتخزينها، وعدم افشائها أو الافصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة ، ويشمل ذلك البيانات الشخصية لأى من مستخدمى خدمته ،أو أى بيانات أو معلومات متعلقه بالمواقع ،والحسابات الخاصة التى يدخل عليها هؤلاء المستخدمون، أو الأشخاص ،والجهات التى يتواصلون معها، تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اعتراضها ،أو اختراقها ،أو تلفها[١].

نطاق تطبيق القانون من حيث المكان[٢]:مع عدم الإخلال بالباب الأول من الكتاب الأول من قانون العقوبات، تسرى أحكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها من هذا القانون، متى كان الفعل معاقبا عليه فى الدولة التى وقع فيها تحت أى وصف قانونى، وذلك فى أى من الأحوال الاتية :

إذا ارتكبت الجريمة على متن أيه وسيله من وسائل النقل الجوى أو البرى أو المائى وكانت مسجله لدى جمهورية مصر العربية أو تحمل علمها.

١. إذا كان المجنى عليهم أو أحدهم مصرياً.

٢. إذا تم الأعداد للجريمة أو التخطيط أو التوجيه أو الأشراف عليها أو تمويلها فى جمهورية مصر العربية.

٣. إذا ارتكبت الجريمة بواسطة جماعة إجرامية تمارس أنشطة إجرامية فى أكثر من دولة من بينها جمهورية مصر العربية

---

(١) القانون رقم ١٧٥ لسنة ٢٠١٨بشأن جرائم تقنية المعلومات ولا ئحتة التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم١٦٩٩لسنة ٢٠٢٠.

(٢) المادة ٣ القانون رقم ١٧٥ لسنة ٢٠١٨بشأن جرائم تقنية المعلومات ولا ئحتة التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم١٦٩٩لسنة ٢٠٢٠.

٤. إذا كان من شأن الجريمة إلحاق ضرر بأى من موطنى جمهورية مصر العربية أو المقيمين فيها، أو بأمنها أو بأى من مصالحها فى الداخل أو الخارج.

٥. إذا وُجد مرتكب جريمة فى جمهورية مصر العربية بعد ارتكابها ولم يتم تسليمة[١].

مجال التعاون الدولى لمكافحة جرائم تقنية المعلومات: تعمل السلطات المصرية المختصة على تيسير التعاون بالبلاد الأجنبية فى إطار الاتفاقيات الدولية ،والإقليمية ،والثنائية المصادق عليها، أو تطبيق مبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادى ارتكاب جرائم تقنيه المعلومات. على أن يكون المركز الفنى للاستعداد لطوارئ الحاسب ،والشبكات بالجهاز هو المنقطة الفنية المعتمدة فى هذا الشأن[٢].

---

(١) المادة ٣ القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن جرائم تقنية المعلومات ولا ئحتة التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم١٦٩٩لسنة ٢٠٢٠.

(٢) المادة ٤ القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن جرائم تقنية المعلومات ولا ئحتة التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم١٦٩٩لسنة ٢٠٢٠.

الفرع الرابع
المسؤولية عن الجرائم الإلكترونية

المسئولية العقدية والمسئولية التقصيرية:

تنقسم المسئولية المدنية الى عقدية ،أو غير عقدية (تقصيرية)، يترتب الأولى على عدم تنفيذ الالتزام الناشئ عن العقد على الوجه المتفق عليه ؛ أما المسئولية التقصيرية فهى تقوم على التزام قانونى مصدره نص القانون يقع على عاتق المسئول يكون الشخص مسئولا عن أعماله غير المشروعة متى صدرت منة وهو مميز [١]،بتعويض المضرور دون علاقة عقدية بينهما بما فى ذلك مثلا مسئولية قائد المركبة عن إصابة أحد المارة .

المسؤولية العقدية: طرفان فى دعوى المسئولية هما المدعى ،والمدعى عليه ، والأول هو المضرور سواء اما المدعى عليه فهو المسئول.

المسؤلية الجنائية :تقوم كجزاء الإضرار بمصالح المجتمع [٢]،وفيها يتعين توقيع عقوبة على المسئول زجرا له ،وردعا لغيره، وتتحرك فيها الدعوى الجنائية عن طريق النيابة العامة بوصفها ممثلة المجتمع فى الدعوى العمومية .

المسئولية المدنية:

فهى جزاء على الإضرار بالمصالح الخاصة التى يكفى لحمايتها التزام المسئول بتعويض الضرر[٣] ،بناء على طلب صاحب المضرور الذى يحق له التنازل عنه ،أو التصالح بشأنه، وفى المسؤولية المدنية لم يحدد المشرع أفعالا بذاتها تنعقد لمرتكبها المسؤلية المدنية.

---

(١) المادة ١٦٤ من القانون المدني المصري.

(٢) الدكتور / السيد عمران ،الأسس العامة في القانون ،منشورات الحلبي الحقوقية ،السنة ٢٠٠٢،ص٢٦٧.

(٣) المادة ١٧٠ من القانون المدنى المصري.

الضرر المادي:الضرر المادي أخلال بحق للمضرور لة قيمة مالية ،او بمصلحة لة ذات قيمة مالية ،فهو ضرر مادي يترتب علية خسارة مالية للمضرور[1]،يتمثل في نفقات العلاج وكسب فائت يتمثل في العجز في القدرة علي العمل واظهر صور الضرر المادي يتمثل في الاعتداء علي حق مالي ايا كان نوعة أي سواء كان حقا عينيا تبعيا، او علي حق شخصي وقد يتمثل الضرر المادي في المساس بمجرد مصلحة.

الضرر الادبي :

الضرر الأدبي لا يمس أموال المضرور(العميل ،او المستهلك) ،و انما يصيب مصلحة غير مالية، يصيب المضرور في عاطفته وشعورة وتدخل الي قلبة الغم والحزن .

عناصر الضرر الموجب للتعويض:

اولاً: الأخلال بمصلحة المضرور :

يكفي ان يمس بمجرد مصلحة العميل ،أو الشركة ،وتفسير ذلك انه لا صعوبة اذا كان الفعل الضار قد اخل للمضرور كحق الأنسان في حياته في سلامة جسمه ، او حق الملكية .

ثانياً : ان تكون المصلحة مشروعة :

لا يقوم الضرر ألا اذا ترتب علي الأخلال بمصلحة مشروعة للعملاء ،والشركات فان كانت المصلحة التي تم المساس بها غير مشروعة أي مخالفة للنظام العام، و الآداب لم يقم عنصر الضرر قانونا

ثالثا : ان يكون الضرر محقق الوقوع :

لا يكون الضرر مستوجبا التعويض عنة الا اذا كان محقق الوقوع، وهو يكون كذلك اذا وقع فعلا على العملاء ،والشركات.

---

(١) الدكتور / السيد عمران،المرجع السابق ذكرة،ص٢٥٤.

التعـويض: يقـدر القـاضي قيمـة التعـويض وفقـا لظـروف الـدعوي[١]،عـن الأضرار النا جمة عـن الـسلوك غـير القـانو ني، فتتنـوع أنـواع الأضرار التـي يمكـن اللجـوء إلى المـسؤولية المدنيـة للتعـويض عنهـا، مثـل الأضرار الماديـة والأضرار النا جمـة عـن الاعتداء على البيانات الشخصية للعمـلاء ومحاولـة ابتـزازهم وعنـدما يـتم تحديـد المسؤولية المدنية لجريمة إلكترونية، يتم تحديد الجانـب الـذي يتحمـل المـسؤولية ،والأضرار التي يتعين عليه تعويـضها، ويمكـن أن تكـون المـسؤولية المدنيـة متعـددة الأطراف، للشركات المتعاقدة معه، وللمـوردين والمـصنعين، ولمـزودي الخـدمات الإلكترونية، وعند التحقـق مـن المـسؤولية المدنيـة للجـرائم الإلكترونيـة، يـتم تقـدير التعويض لتغطية الأضرار التي تعرض لها المتضرر(العميل أو المستهلك)، ويمكن تحديد هذا القيمة بتحديد الأضرار المادية والنفسية والخسائر المالية، التي أصابت المستهلك ،وقد يتم تحديـد القيمـة الإجماليـة للتعـويض بنـاءً عـلى حجـم الخـسائر الناتجة عن الجريمة الإلكترونية.

(١) المادة ١٧١ من القانون المدنر المصري.

خاتمة

يعد الأمن السيبراني عامل أساسي في نجاح عقود التجارة الإلكترونية، لأنه يحمي الشركات عبر الإنترنت ،وعملائها من التهديدات السيبرانية المختلفة، و تلعب منصات التجارة الإلكترونية ومقدمو الخدمات دورًا مهمًا في ضمان تنفيذ تدابير الأمن السيبراني، حيث إنهم مسؤولون عن تأمين الشركات، و المتاجر ،،والمستهلكين في معاملات التجارة الإلكترونية، بالتزامهم بتدابير، وإجراءات الأمن السيبراني كحماية البيانات، والمعلومات الشخصية ،و الأنظمة بعناية ،مما يساعد فى الحفاظ على سمعة تلك المنصات ،والشركات ،ويجذب ثقة المتعاقدين في التعامل ،وإبرام عقود التجارة الإلكترونية مع تلك الشركات ،والمتاجر، ويتم ذلك من خلال منع ،أو تقليل مخاطر انتهاكات البيانات ،أو الهجمات الإلكترونية ،على العملاء، أو المستهلكين، أو التوقف عن العمل، ومن المهم أن يكون هناك شفافية في عرض طريقة جمع بيانات العملاء ،وتخزينها ،واستخدامها ،و توخي الحذر ،واستخدام أكبر عدد ممكن إجراءات الأمن السيبرانى لحماية المتعاقدين.

وبالاستثمار في تطوير تقنيات ،واستراتيجيات الأمن السيبرانى لمواكبة التهديدات المتطورة، لتأمين سياسات الخصوصية الواضحة ، اصبح الأمن السيبراني عاملاً حاسماً لنجاح عقود التجارية الإلكترونية، لدورة الفعال في تأمين الجوانب الفنية لعقود التجارة الإلكترونية ، كحماية البيانات ،والخصوصية ،ودعم الثقة، فيجب أن تكون كل الشركات متيقظة، ومجهزة باتخاذ كافة التدابير الاحترازية بأتباع وسائل الأمن السيبراني؛ لاكتساب ميزة تنافسية ،وتعزيز قاعدة عملاء مميزين، فالأمن السيبراني هو مفتاح نجاح التجارة الإلكترونية،والأمن السيبراني ليس مجرد مسؤولية

الخبراء التقنيين فحسب، بل هو مسؤولية كل متعاقد في عقود التجارة الإلكترونية ، و أصبح من معايير قياس أمان منصات التجارة الإلكترونية.

النتائج:

أولاً: يهدف الأمن السيبراني الى مقاومة التهديدات، ومنع الهجمات على متعاقدين التجارة الإلكترونية .

ثانياً: الأمن السيبراني وسيلة الدفاع في الحروب الجديدة وهي الحروب الإلكترونية.

ثالثا: يعتبر الأمن السيبراني وسيلة إتمام عقود التجارة الإلكترونية.

رابعاً: يعتبر الأمن السيبرانى وسيلة لمنع أي انقطاع لمعاملات التجارة الإلكترونية بسبب الأنشطة الغير مرغوب فيها، عبر منصات التجارة الإلكترونية.

خامساً: يهدف الأمن السيبرانى ألي حماية المعاملات الإلكترونية بكافة أشكالها.

سادساً: الأمن السيبرانى عنصرأساسي لحماية أطراف في عقود التجارة الإلكترونية، وبدونة، فإن منصات ،وشركات التجارة الإلكترونية تخاطر بخسارة عملائها، وسمعتها، وإيراداتها، وحتى وجودها.

سابعاً: الأمن السيبراني يعزز ثقة متعاقدين التجارة الالكترونية في منصات ،وشركات التجارة الإلكترونية.

ثامناً: الأمن السيبرانى يخفض تكاليف الشركة ،ويرفع مستوي الإنتاجية، ويوفر الوقت ،ويساعد على التركيز على العمل في الشركات التي تنفذ جميع تدابير الأمن السيبرانى.

تاسعاً: شركات التجارة الإلكترونية الملتزمة بالأمن السيبراني تكون قادرة على التنافس من خلال تقديم خدمات ،ومنتجات آمنة تجذب المتعاقدين.

عاشراً: الأمن السيبرانى يحمي سمعة المنصات ،والشركات التي تلتزم به.

التوصيات:

أولاً: ضرورة إقامة دورات مكثفة للتثقيف حول الأمن السيبراني.

ثانيا: ضرورة استخدام الأمن السيبراني والتعامل به في كافة عقود التجارة الإلكترونية .

ثالثاً: يجب أن نكون مستعدين لتبني نهج أكثر شمولية للأمن السيبراني في كافة المجالات.

رابعاً: تزويد الأفراد ،والمؤسسات بأدوات، وإجراءات الأمن السيبرانى لحماية أنفسهم من التهديدات، والهجمات السيبرانية من خلال منصات التجارة الإلكترونية.

خامسا: يجب أن تلتزم منصات التجارة الإلكترونية بالأمن السيبرانى والرقابة عليها من الجهات المختصة.

سادسا: يجب على منصات ،وشركات التجارة الإلكترونية تثقيف، وتدريب موظفيها ،وعملائها، لرفع مستوى الوعي ،والتثقيف بشأن الأمن السيبراني ،وتوضيح دورة فى أتمام عقود التجارة الإلكترونية.

سابعاً: يجب على شركات ،ومنصات التجارة الإلكترونية الالتزام بالأمن السيبرانى، ومتابعة ، ومراقبة ، وتحديث أنظمتهم ،وسياساتهم الأمنية بصورة دورية، وإجراء عمليات تدقيق ،وتقييم دورية لتحديد، ومعالجة أي نقاط ضعف ،أو أى ثغرات تكون هدف للمتسللين.

ثامناً: يجب على منصات التجارة الإلكترونية ، تقديم ميزات ،وسبل الأمن السيبرانى لمتعاقدين التجارة الإلكترونية ،لمساعدتهم على تعزيز أمان متجرهم ،عبر الإنترنت، وتقديم التوجيه ،والدعم لعملائهم لمساعدتهم في التعامل مع أي مشكلات ،أو حوادث أمنية، لضمان نجاح معاملات ،وعقود التجارة الإلكترونية.

قائمة المراجع :

الكتب:

١. الدكتور/ محمود سمير الشرقاوي، الخطر في التامين البحري، الدار القومية للطباعة والنشر القاهرة ،السنة ١٩٦٦.

٢. الدكتور / مصطفي كمال طة ،الأستاذ / وائل بندق ،الأوراق التجارية ووسائل الدفع الإلكتروني، دار الفكر الجامعي ،السنة ٢٠٠٥.

٣. الدكتور/ احمد عبد الكريم سلامة، نظرية العقد الدولي الطليق ، دار النهضة العربية ، ج٢، ١٩٨٩.

٤. الدكتور / عبد الوهاب محمد عبد الوهاب السادة، التنظيم القانوني للأمن السيبراني ، دار المطبوعات الجامعية ،السنة ٢٠٢٥.

٥. الدكتور/ حيدر فالح سلمان، مقدمة في الأمن السيبرانى ،الذاكرة للنشر والتوزيع ،لا يوجد سنة نشر.

٦. الدكتور / راشد المري ،الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر، دار النهضة ،السنة ٢٠١٨.

٧. الدكتور / علي القهوجي ،الحماية الجنائية لبرامج الحاسب ،دار الجامعة ،السنة١٩٩٧.

٨. الدكتور/ جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية ،السنة ٢٠٠١.

٩. الدكتور خالد حسن لطفي، الدليل الرقمي ودورة في أثبات الجريمة المعلوماتية ، دار الفكر الجامعي ،السنة ٢٠٢٠.

١٠. الدكتور/ خالد ممدوح إبراهيم ،الجرائم المعلوماتية ،دار الفكر الجامعي، السنة ٢٠١٩.

١١. الدكتور/خالد ممدوح ابراهيم، إبرام العقد الإلكتروني، دار الفكر الجامعي، السنة ٢٠٠٦.

١٢. الدكتور/ علاء حسين الحمامي ،الدكتور / سعد عبد العزيز ،تكنولوجيا امن المعلومات وأنظمة الحماية، دار وائل للنشر ،السنة ٢٠٠٧.

١٣. الدكتور / صالح المنزلاوي، القانون الواجب التطبيق على عقود التجارة الإلكترونية ،دار النهضة ،السنة ٢٠٠٥.

١٤. الدكتور/ احمد محمد ابراهيم ،القانون المدني معلقا علي نصوصه بالأعمال التحضيرية وأحكام القضاء ،دار المعارف ،السنة ١٩٦٤.

١٥. الدكتور/ رضا عبيد، القانون التجاري، لا يوجد دار نشر، السنة ١٩٨٣.

١٦. الدكتور / ماركو إبراهيم ، حماية أنظمة المعلومات، دار الحامد، السنة ٢٠١٣.

١٧. الدكتور / عبد الوهاب محمد عبد الوهاب السادة، التنظيم القانوني للأمن السيبراني ،دار المطبوعات الجامعية ،السنة ٢٠٢٥.

١٨. الدكتور/ راشد محمد عبدة ،امن وحماية الوثائق الإلكترونية ،دار الجوهرة ،السنة ٢٠١٥.

١٩. الدكتور / حسن الصاوي، الدكتور/ خالد الشلفان ،امن الشبكات والنظم المفاهيم والتقنيات ،لا يوجد دار نشر ،السنة ٢٠١٣.

٢٠. الدكتور / راشد محمد المرى، الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر ، دار النهضة ،٢٠١٨،

٢١. الدكتور / خضر إسماعيل ،أساسيات امن المعلومات والحاسوب، دار الحامد للنشر والتوزيع ،السنة ٢٠١٠.

٢٢. الدكتور/ حسام محمود فهمي، الفيروسات والحاسبات كل ئ عنها، دار الحكيم للطباعة القاهرة ،السنة ٢٠٠٤.

٢٣. الدكتور / ذياب البدائية، الأمن وحرب المعلومات ، دار الشروق ،السنة ٢٠٠٦.

المقالات:

١. الدكتور / خالد عبد الله المطيري، مقال بعنوان دور التشريعات الجزائية في حماية الأمن السيبرانى مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية،السنة١٤٤٣.

٢. الدكتورة / أماني قرني ،مقال بعنوان دور مواقع الأعلام الرقمي في حماية الأمن السيبرانى، المجلة المصرية لبحوث الأعلام ،السنة ٢٠٢٢.

٣. الدكتور / محمد سعيد ،مقال بعنوان التامين الإلكتروني ضد المخاطر السيبرانية ،المجلة الدولية للقانون ، دار نشر قطر ،٢٠٢١.

٤. هربرت لين ،مقال بعنوان النزاع السيبرانى والقانون الدولي الإنساني، المجلة الدولية للصليب الأحمر ،السنة ٢٠١٢

٥. حسن طاهر داود، مقال بعنوان الحاسب وامن المعلومات ،مركز البحوث، السنة ٢٠٠٠.

٦. الدكتورة / مني عبد الله السمحان ،مقال بعنوان متطلبات تحقيق الأمن السيبرانى لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية جامعة المنصورة، يوليو ٢٠٢٠ .

٧. حسين بن راشد الطيار، الأمن السيبرانى في منظور مقاصد الشرع ،دراسة تأصيلية، المملكة العربية السعودية جامعة الطائف، مجلة الطائف للعلوم الإنسانية، السنة ٢٠٢٠.

٨. الدكتور/ عدنان مصطفي البار، مقال بعنوان أمن المعلومات والأمن السيبرانى، كلية الحاسبات وتقنية المعلومات ،جامعة الملك عبد العزيز.

٩. الدكتور / عادل راضي ،مقال بعنوان الوقاية من المخاطر السيبرانية ،جامعة تبوك ، السنة ٢٠٠٦.

١٠. نهى مجدي السيد ،مقال بعنوان الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر ٢٠٣٠،المجلة العلمية لبحوث الأعلام، السنة٢٠٢١.

١١. الدكتور / حسام الأهوانى ،مقال بعنوان أثبات عقود التجارة الإلكترونية ،مؤتمر القانون وتحديات المستقبل ،كلية الحقوق جامعة الكويت ،١٩٩٧.

١٢. الدكتور / اشرف وفا محمد ،مقال بعنوان عقود التجارة الإلكترونية في القانون الدولي الخاص ،المجلة المصرية للقانون الدولي ،العدد ٥٧،السنة ٢٠٠١.

١٣. الدكتور ادريس عطية ،مقال بعنوان مكانة الأمن السيبرانى في منظومة الأمن الوطني الجزائري، مصداقية، لا يوجد سنة .

١٤. الدكتور / ايمن الحربي، مقال بعنوان مقدمة في الأمن السيبرانى، معهد البحوث والدراسات ،واحة ام القري.

١٥. لامية، مقال بعنوان التهديدات والجرائم السيبرانية تأثيرها علي الأمن القومي واستراتيجيات مكافحتها ، مجلة الدراسات القانونية والسياسية ،السنة٢٠٢٠.

١٦. سلام لامية، مقال بعنوان الجرائم الإلكترونية بعد جديد لمفهوم الأجرام عبر منصات التواصل الاجتماعي ، مجلة الرواق للدراسات الاجتماعية والإنسانية، السنة ٢٠٢٠.

١٧. الدكتور/ قاسم محمد حسين، مقال بعنوان أساسيات في الأمن السيبرانى، كلية الكنوز الجامعية ،قسم الأمن السيبراني.

١٨. الدكتور / محمد سعيد ،مقال بعنوان التامين الإلكتروني ضد المخاطر السيبرانية ،المجلة الدولية للقانون ،دار نشر قطر ،٢٠٢١.

١٩. وليد احمد ،مقال بعنوان الفرق بين امن المعلومات والأمن السيبرانى ،صحيفة الجزيرة الإلكترونية ،مؤسسة الجزيرة الإلكترونية للصحافة ،السنة ١٤٣١.

٢٠. كامل خضر ،سمر المداح، مقال بعنوان العلاقة بين الاقتصاد الرقمي ،وامن المعلومات ،دراسة تطبيقية ،المجلة العلمية للاقتصاد والتجارة، العدد ٣،السنة ٢٠٢٠.

٢١. الدكتور/ عبد العزيز فتحي العلواني، مقال بعنوان حماية المستهلك الإلكتروني وفق نظام التجارة الإلكترونية، مجلة الصدي للدراسات القانونية والسياسية ،العدد السابع ،السنة ٢٠٢١.

٢٢. الدكتور/ حسين سعيد الغافري ،السياسة الجنائية في مواجهة جرائم الأنترنت، دار النهضة العربية، السنة ٢٠٠٩

٢٣. الدكتور/ خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب ،دار الثقافة والنشر ،السنة ٢٠١١.

٢٤. الدكتور/ مصطفي محمد موسي ،التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة ،السنة ٢٠٠٩.

٢٥. الدكتور/ محمد انور عاشور ،المبادئ الأساسية في التحقيق الجنائي العملي، عالم الكتب ،السنة ١٩٨٧،ص٣٤.

٢٦. الدكتور / خالد محمد عجاج ،اصول التحقيق الجنائي ،دار التعليم الجامعي ،السنة٢٠١٨.

٢٧. الدكتور/ جميل عبد الباقي الصغير، ادله الأثبات الجنائي والتكنولوجيا الحديثة ،دار النهضة العربية ،السنة ٢٠٠١.

٢٨. الدكتور/ خالد ممدوح إبراهيم ،فن التحقيق الجنائي في الجرائم الإلكترونية ،دار الفكر الجامعي، السنة ٢٠١٨.

٢٩. الدكتور/ مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري ،دار النهضة ،السنة ٢٠٠٨

٣٠. الدكتور/ طارق عبد العال حماد ،التجارة الإلكترونية (الأبعاد التكنولوجية والمالية)،الدار الجامعية ،السنة ٢٠٠٨.

٣١. الدكتور/ عبد المطلب عبد الحميد، اقتصاديات التجارة الإلكترونية، الدار الجامعية ،السنة ٢٠١٤

٣٢. الدكتور / السيد عمران ،الأسس العامة في القانون ،منشورات الحلبي الحقوقية ،السنة ٢٠٠٢

قوانين وتشريعات:

١. القانون المدنى المصري رقم ١٣١لسنة ١٩٤٨.

٢. القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة تقنية المعلومات ولائحته التنفيذية الصادرة بقرار رئيس مجلس الوزراء رقم ١٦٩٩لسنة ٢٠٢٠.

٣. قانون حماية المستهلك ،القانون رقم ١٨١لسنة ٢٠١٨ ولائحة التنفيذية الصادرة بقرار مجلس الوزراء رقم لسنة ٢٠١٩.

٤. قانون الإجراءات الجنائية المصري.

٥. قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية ١٩٩٦

تقارير:

١. تقرير بعنوان الأمن السيبرانى في مؤسسات منظومة الأمم المتحدة، تقرير وحدة التفتيش المشتركة، الأمم المتحدة ،السنة ٢٠٢١.

٢. الاستراتيجية الوطنية للأمن السيبراني لدولة الكويت ،الهيئة العامة للاتصالات وتقنية المعلومات ،٢٠١٧-٢٠٢٠.

٣. الاستراتيجية الوطنية للأمن السيبرانى ،وزارة الاتصالات وتكنولوجية المعلومات الأردن ،السنة ٢٠٢١.

٤. تقرير الأمين العام ،المبادئ التوجيهية لاستعمال البرنامج العالمي للأمن السيبراني ،جنيف الوثيقة ٦٥-Aالسنة ٢٠٢٠

٥. مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ،السنة ٢٠١٥

رسائل علمية:

الدكتور/ مهند عزمي مسعود ،القانون الواجب التطبيق علي العقد الدولي ،رسالة دكتوراه ،حقوق عين شمس ،السنة ٢٠٠٥.

اتفاقيات:

اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الإلكترونية في العقود الدولية (نيويورك ٢٠٠٥).

مراجع اجنبية:

1)Travaux de l institute de sciences criminelles de poitiers ,informatiqe et adroit paneled cujas ,1983.

2) Olivier mean ,L internet et Le droit. Aspects juridiques du commerce electronique ed eyrolles ,Paris 1996.

مواقع الأنترنت :

https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security

https://www.sailpoint.com/identity-library/five-types-of-cybersecurity

https://www.comptia.org/content/articles/what-is-cybersecurity

https://www.fortinet.com/resources/cyberglossary/operational-security

https://www.comptia.org/content/articles/what-is-cybersecurity

https://www.geeksforgeeks.org/cyber-security-types-and-importance/

https://www.sailpoint.com/identity-library/five-types-of-cybersecurity

https://online.eou.edu/resources/article/main-types-of-cyber-security

https://www.comptia.org/content/articles/what-is-cybersecurity

https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity

https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security
https://www.comptia.org/content/articles/what-is-cybersecurity
https://cypfer.com/what-are-the-6-types-of-cyber-security
https://preyproject.com/blog/how-to-educate-employees-about-cybersecurity https://blog.qit.company/
https://www.institutedata.com/blog/what-are-the-7-types-of-cyber-security /
https://www.unodc.org/romena/ar/cybercrime.html2
https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity
https://www.sailpoint.com/identity-library/five-types-of-cybersecurity https://www.comptia.org/content/articles/what-is-cybersecurity
https://blog.present.ca/cybersecurity-is-not-optional
https://www.cloudflare.com/learning/ssl/what-is-ssl/
https://www.bolddesk.com/blogs/troubleshooting-gui
https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity
[https://www.cbe.org.eg/ar/cybersecurity/cybersecurity-issues-training-and-awareness
https://ibsacademy.org/knowledge-base/cyber-security-for-employeeslk
https://gca.isa.org/blog/why-collaboration-is-essential-for-cybersecurity-teams
https://www.sciencedirect.com/science/article/pii/S235286482100047X
https://fastercapital.com/arabpreneu

References:

alkutub:

• alduktur/mahmud samir alsharqawi, alkhatar fi altaamin albahrii, aldaar alqawmiat liltibaeat walnashr alqahirat ,alsanat 1966.

• alduktur /mustafi kamal tat ,al'ustadh / wayil bunduq ,al'awraq altijariat wawasayil aldafe al'iilikturunii, dar alfikr aljamieii ,alsanat 2005.

• alduktur/ ahmad eabd alkarim salamat, nazariat aleaqd aldawlii altaliq , dar alnahdat alearabiat , ji2, 1989.

• alduktur /eabd alwahaab muhamad eabd alwahaab alsaadati, altanzim alqanuniu lil'amn alsaybiranii , dar almatbueat aljamieiat ,alsanat 2025.

• alduktur/hidar falih salman, muqadimat fi al'amn alsiybirania ,aldhaakirat lilnashr waltawzie ,la yujad sanat nashra.

• alduktur / rashid almirii ,aljarayim al'iiliktiruniat fi zili alfikr aljinayiyi almueasiri, dar alnahdat ,alsanat 2018.

• alduktur /eali alqahwaji ,alhimayat aljinayiyat libaramij alhasib ,dar aljamieat ,alsanat1997.

• alduktur/jamil eabd albaqi alsaghir, aljawanib al'iijrayiyat liljarayim almutaealiqat bial'antirinta, dar alnahdat alearabiat ,alsanat 2001.

• alduktur khalid hasan litafi, aldalil alraqamii wadawrat fi 'athabat aljarimat almaelumatiat , dar alfikr aljamieii ,alsanat 2020.

• alduktur/ khalid mamduh 'iibrahim ,aljarayim almaelumatiat ,dar alfikr aljamieii, alsanat 2019.

• alduktur/khalid mamduh abrahim, 'iibram aleuqd al'iilikturunii, dar alfikr aljamieii, alsanat 2006.

• alduktur/eala' husayn alhamaami ,alduktur /saed eabd aleaziz ,tiknulujia amin almaelumat wa'anzimat alhimayati, dar wayil lilnashr ,alsanat 2007.

• alduktur /salih almanzilawi, alqanun alwajib altatbiq ealaa euqud altijarat al'iiliktruniat ,dar alnahdat ,alsanat 2005.

• alduktur/ aihmad muhamad abrahim ,alqanun almadaniu muealiqan eali nususah bial'aemal altahdiriat wa'ahkam alqada' ,dar almaearif ,alsanat 1964.

• alduktur/rida eubaydi, alqanun altijari, la yujad dar nashra, alsanat 1983.

• alduktur /marku 'iibrahim ,himayat 'anzimat almaelumati, dar alhamidi, alsanat 2013.
• alduktur /eabd alwahaab muhamad eabd alwahaab alsaadati, altanzim alqanuniu lil'amn alsiybiranii ,dar almatbueat aljamieiat ,alsanat 2025.
• alduktur/rashid muhamad eabdat ,amin wahimayat alwathayiq al'iiliktruniat ,dar aljawharat ,alsanat 2015.
• alduktur / hasan alsaawi, alduktur/khalid alshalfan ,amin alshabakat walnuzum almafahim waltiqniaat ,la yujad dar nashr ,alsanat 2013.
• alduktur /rashid muhamad almaraa, aljarayim al'iiliktiruniat fi zili alfikr aljinayiyi almueasir , dar alnahdat ,2018,
• alduktur /khadar 'iismaeil ,'asasiaat amin almaelumat walhasuba, dar alhamid lilnashr waltawzie ,alsanat 2010.
• alduktur/husam mahmud fahmi, alfayrusat walhasibat kulun y eanha, dar alhakim liltibaeat alqahirat ,alsanat 2004.
• alduktur / dhiab albidayiyati, al'amn waharb almaelumat , dar alshuruq ,alsanat 2006.

almaqalat:

• alduktur /khalid eabd allah almutayri, maqal bieunwan dawr altashrieat aljazayiyat fi himayat al'amn alsiybirania majlis altaeawun alkhaliji, majalat albuhuth alfiqhiat walqanuniati,alsanatu1443.
• aldukturat /'amani qarniun ,maqal bieunwan dawr mawaqie al'aelam alraqamii fi himayat al'amn alsiybiranaa, almajalat almisriat libuhuth al'aelam ,alsanat 2022.
• alduktur /muhamad saeid ,maqal bieunwan altaamin al'iiliktruniu dida almakhatir alsiybiraniat ,almajalat aldawliat lilqanun , dar nashr qatar ,2021.
• hirbirt lin ,maqal bieunwan alnizae alsiybiranaa walqanun alduwliu al'iinsaniu, almajalat aldawliat lilsalib al'ahmar ,alsanat 2012
• hasan tahir dawud, maqal bieunwan alhasib wamin almaelumat ,markaz albuhuthi, alsanat 2000.
• aldukturat / miniy eabd allah alsamhan ,maqal bieunwan mutatalabat tahqiq al'amn alsiybiranaa li'anzimat almaelumat al'iidariat bijamieat almalik saeud, majalat kuliyat altarbiat jamieat almansurati, yuliu 2020 .

• husin bin rashid alttyaar, al'amn alsiybirania fi manzur maqasid alsharae ,dirasat tasiliati, almamlakat alearabiat alsaeudiat jamieat altaayif, majalat altaayif lileulum al'iinsaniati, alsanat 2020.
• alduktur/eadnan mustafi albari, maqal bieunwan 'amn almaelumat wal'amn alsaybiranaa, kuliyat alhasibat watiqniat almaelumat ,jamieat almalik eabd aleaziza.
• alduktur /eadil radi ,maqal bieunwan alwiqayat min almakhatir alsiybiraniat ,jamieat tabuk , alsanat 2006.
• nahaa majdi alsayid ,maqal bieunwan al'amn alsaybiraniu waealaqatuh bialmadmun al'iielamii fi zili ruyat misr 2030,almajalat aleilmiat libuhuth al'aelami, alsinati2021.
• alduktur /husam al'ahwanaa ,maqal bieunwan 'athabat euqud altijarat al'iiliktruniat ,mutamar alqanun watahadiyat almustaqbal ,kuliyat alhuquq jamieat alkuayt ,1997.
• alduktur / ashraf wafa muhamad ,maqal bieunwan euqud altijarat al'iiliktruniat fi alqanun alduwalii alkhasi ,almajalat almisriat lilqanun alduwalii ,aleadad 57,alsanat 2001.
• alduktur adris eatiat ,maqal bieunwan makanat al'amn alsiybirania fi manzumat al'amn alwatanii aljazayirii, misdaqiatun, la yujad sanatan .
• alduktur /aymin alharbi, maqal bieunwan muqadimat fi al'amn alsiybirania, maehad albuhuth waldirasat ,wahat am alqari.
• lamiat, maqal bieunwan altahdidat waljarayim alsaybaraniat tathiruha eali al'amn alqawmiu wastiratijiaat mukafahatiha ,majalat aldirasat alqanuniat walsiyasiat ,alsanat2020.
• salam lamiatun, maqal bieunwan aljarayim al'iilikturuniat baed jadid limafhum al'ajram eabr minasaat altawasul alaijtimaeii ,majalat alrawaq lildirasat aliajtimaeiat wal'iinsaniati, alsanat 2020.
• alduktur/qasim muhamad husayn, maqal bieunwan 'asasiaat fi al'amn alsiybirania, kuliyat alkunuz aljamieiat ,qism al'amn alsiybirani.
• alduktur /muhamad saeid ,maqal bieunwan altaamin al'iiliktruniu dida almakhatir alsiybiraniat ,almajalat alduwaliat lilqanun ,dar nashr qatar ,2021.
• wlid aihmad ,maqal bieunwan alfarq bayn amin almaelumat wal'amn alsiybirania ,sahifat aljazirat al'iiliktruniat ,muasasat aljazirat al'iiliktruniat lilsahafat ,alsanat 1431.

• kamil khadir ,smar almadahi, maqal bieunwan alealaqat bayn alaiqtisad alraqmii ,wamin almaelumat ,dirasat tatbiqiat ,almajalat aleilmiat lilaiqtisad waltijarati, aleadad 3,alsanat 2020.
• alduktur/eabd aleaziz fathi aleulwani, maqal bieunwan himayat almustahlik al'iiliktrunii wifq nizam altijarat al'iiliktruniati, majalat alsidi lildirasat alqanuniat walsiyasiat ,aleadad alsaabie ,alsanat 2021.
• alduktur/hsin saeid alghafiri ,alsiyasat aljinayiyat fi muajahat jarayim al'antirinti, dar alnahdat alearabiati, alsanat 2009
• alduktur/khalid eayaad alhalbi, ajara'at altahariy waltahqiq fi jarayim alhasub ,dar althaqafat walnashr ,alsanat 2011.
• alduktur/mustafi muhamad musi ,altahqiq aljinayiyu fi aljarayim al'iiliktruniati, matabie alshurtat ,alsanat 2009.
• alduktur/muhamad anur eashur ,almabadi al'asasiat fi altahqiq aljinayiyi aleamaliu, ealam alkutub ,alsanat 1987,s34.
• alduktur /khalid muhamad eajaaj ,asul altahqiq aljinayiyi ,dar altaelim aljamieii ,alsanat2018.
• alduktur/ jamil eabd albaqi alsaghir, adalah al'athabat aljinayiyu waltiknulujia alhadithat ,dar alnahdat alearabiat ,alsanat 2001.
• alduktur/khalid mamduh 'iibrahim ,fan altahqiq aljinayiyu fi aljarayim al'iilikturuniat ,dar alfikr aljamieii, alsanat 2018.
• alduktur/mamun muhamad salamat, al'iijra'at aljinayiyat fi altashrie almisrii ,dar alnahdat ,alsanat 2008
• alduktur/tariq eabd aleal hamaad ,altijarat al'iiliktrunia (al'abead altiknulujiat walmaliatu),aldaar aljamieiat ,alsanat 2008.
• alduktur/eabd almutalib eabd alhamidi, aqtisadiaat altijarat al'iilikturuniati, aldaar aljamieiat ,alsanat 2014
• alduktur / alsayid eimran ,al'usus aleamat fi alqanun ,manshurat alhalabii alhuquqiat ,alsanat 2002

qawanin watashrieat:

• alqanun almudnaa almisrii raqm 131lsanat 1948.
• alqanun raqm 175 lisanat 2018 bishan mukafahat taqniat almaelumat walayihatih altanfidhiat alsaadirat biqarar rayiys majlis alwuzara' raqm 1699lsanat 2020.
• qanun himayat almustahlik ,alqanun raqm 181lsanat 2018 walayihatat altanfidhiat alsaadirat biqarar majlis alwuzara' raqm lisanat 2019.
• qanun al'iijra'at aljinayiyat almisriu.

• qanun al'uwnsitral alnamudhajiu bishan altijarat al'iilikturuniat 1996

tiqarir:

• taqrir bieunwan al'amn alsiybirania fi muasasat manzumat al'umam almutahidati, taqrir wahdat altaftish almushtarakati, al'umam almutahidat ,alsanat 2021.

• alastiratijiat alwataniat lil'amn alsiybiranii lidawlat alkuayt ,alhayyat aleamat lilaitisalat watiqniat almaelumat ,2017-2020.

• alastiratijiat alwataniat lil'amn alsiybirania ,wizarat alaitisalat watiknulujiat almaelumat al'urdun ,alsanat 2021.

• taqrir al'amin aleami ,almabadi altawjihiat liaistiemal albarnamaj alealamii lil'amn alsiybiranii ,jinif alwathiqat 65-Aalsanatu2020

• mutamar al'atraf fi aitifaqiat al'umam almutahidat limukafahat aljarimat almunazamat eabr alwataniat ,alsanat 2015

rasayil eilmia:

• alduktur/mhand eazmi maseud ,alqanun alwajib altatbiq eali aleaqd alduwaliu ,risalat dukturah ,huquq eayn shams ,alsanat 2005.

• itifaqiaat:

• atifaqiat al'umam almutahidat almutaealiqat biaistikhdam alkhitabat al'iilikturuniat fi aleuqud alduwalia (niuyurk 2005).

فهـــــرس الموضوعـــــات