مجلة مركز بابل للدراسات الإنسانية ٢٠٢٦ المجلد ١٦/ العدد ٩

حمايةُ المحلِ التجاري الالكتروني من الهجماتِ السيبرانيَّةِ
(دراسة مقارنة بين القانون العراقي والقانون السعودي والاماراتي)

تقى علي جمعة حسن
قسم القانون الخاص ، كلية الحقوق ، جامعة الموصل
نينوى ، العراق
باشراف
أ.م.د. رواء يونس محمود النجار
قسم القانون الخاص ، كلية الحقوق ، جامعة الموصل
نينوى ، العراق

البريد الإلكتروني Email : Tuqaali499@gmail.com

الكلمات المفتاحية: المحل التجاري الالكتروني ، الهجمات السيبرانية ، الامن السيبراني ، الجرائم الالكترونية، الحماية القانونية.

كيفية اقتباس البحث
حسن، تقى علي جمعة ، رواء يونس محمود النجار ، حمايةُ المحلِ التجاري الالكتروني من الهجماتِ السيبرانيَّةِ (دراسة مقارنة بين القانون العراقي والقانون السعودي والاماراتي)،مجلة مركز بابل للدراسات الانسانية، أيلول ٢٠٢٦، المجلد:١٦ ،العدد:٩ .

هذا البحث من نوع الوصول المفتوح مرخص بموجب رخصة المشاع الإبداعي لحقوق التأليف والنشر (Creative Commons Attribution) تتيح فقط للآخرين تحميل البحث ومشاركته مع الآخرين بشرط نَسب العمل الأصلي للمؤلف، ودون القيام بأي تعديل أو استخدامه لأغراض تجارية.

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

Protecting the e-commerce shop from cyber attacks (A Comparative Study between Iraqi Law and Saudi and Emirati Law)

Tuqaa Ali Gomaa Hassan
Under the supervision of
Assoc. Prof. Dr. Rawa Younis Al-Najjar
Department of Private Law, College of Law, University of Mosul
Nineveh, Iraq

Keywords : Electronic Commercial Establishment; Cyberattacks; Cybersecurity; Electronic Crimes; Legal Protection).

How To Cite This Article
Hassan, Tuqaa Ali Gomaa , Rawa Younis Al-Najjar , Protecting the e-commerce shop from cyber attacks, (A Comparative Study between Iraqi Law and Saudi and Emirati Law) Journal Of Babylon Center For Humanities Studies, September 2026,Volume:16,Issue 9.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Abstract

The rapid development of information and communication technologies has had a profound impact on the modernization of the concept of commercial activity, as such activity is no longer confined to the traditional physical framework. Rather, it has expanded to encompass the digital space, including what is known as the electronic commercial establishment, which has become one of the most prominent components of the contemporary digital economy, given its effectiveness as a means for conducting commercial transactions and exchanging goods and services without being restricted by time or place. However, this development has been accompanied by a number of challenges, most notably cyber risks that threaten the security of this type of commercial activity, particularly those related to data in terms of its integrity, confidentiality, and availability.

With the quantitative and qualitative increase in cyberattacks targeting electronic commercial establishments in their various forms, cybersecurity has emerged as the first line of defense against such threats. It is not merely an organizational option or a precautionary measure, but rather a legal and technical necessity that cannot be dispensed with. Nevertheless, the effectiveness of this role depends on the existence of a sound legislative framework capable of providing protection through the guarantees it offers, embodied in defining obligations and establishing legal liabilities and effective sanctions. This is precisely what national legislation lacks.

Accordingly, this research addresses all the foregoing by defining the electronic commercial establishment, identifying the main types of cyberattacks to which it is exposed, and determining the role of cybersecurity in ensuring its protection, with a view to reaching the most significant findings and recommendations. This is achieved through adopting a comparative analytical approach to demonstrate the legislative deficiency and gap in the Iraqi legal system in this regard.

The rapid development of information and communication technologies has had a profound impact on the modernization of the concept of commercial activity, as such activity is no longer confined to the traditional physical framework. Rather, it has expanded to encompass the digital space, including what is known as the electronic commercial establishment, which has become one of the most prominent components of the contemporary digital economy, given its effectiveness as a means for conducting commercial transactions and exchanging goods and services without being restricted by time or place. However, this development has been accompanied by a number of challenges, most notably cyber risks that threaten the security of this type of commercial activity, particularly those related to data in terms of its integrity, confidentiality, and availability.

With the quantitative and qualitative increase in cyberattacks targeting electronic commercial establishments in their various forms, cybersecurity has emerged as the first line of defense against such threats. It is not merely an organizational option or a precautionary measure, but rather a legal and technical necessity that cannot be dispensed with. Nevertheless, the effectiveness of this role depends on the existence of a sound legislative framework capable of providing protection through the guarantees it offers, embodied in defining obligations and establishing legal liabilities and effective sanctions. This is precisely what national legislation lacks.

Accordingly, this research addresses all the foregoing by defining the electronic commercial establishment, identifying the main types of cyberattacks to which it is exposed, and determining the role of cybersecurity in ensuring its protection, with a view to reaching the most significant findings and recommendations. This is achieved through adopting a comparative analytical approach to demonstrate the legislative deficiency and gap in the Iraqi legal system in this regard.

الملخص

إنَّ التطور المتسارع في تقنيات المعلومات والاتصالات كان له اثره الكبير في الحداثة التي طالت مفهوم النشاط التجاري، إذ لم يعد هذا النشاط مقصورًا على الإطار المادي التقليدي، إلاَّ أنَّه اتسع نطاقه ليشمل الفضاء الرقمي ومنه ما يُعرف بالمحل التجاري الإلكتروني، الذي عد من أبرز مفردات الاقتصاد الرقمي المعاصر بما يمثله من وسيلة ناجعة في إنجاز المعاملات التجارية وتداول السلع والخدمات الذي لا يحده زمان او مكان غير أن هذا التطور جابهته جملة من التحديات ولعل أبرزها المخاطر السيبرانية التي تهدد أمن هذا النوع من النشاط التجاري، خاصة تلك التي تخص البيات من حيث سلامتها وسريتها واستمراريتها.

ومع تزايد الهجمات السيبرانية كماً ونوعاً على المحل التجاري الإلكتروني بمختلف صوره ، برز الأمن السيبراني الذي يعد خط الدفاع الأول في مواجهتها، فهو لا يعني مجرد خيار تنظيمي أو إجراء احترازي فحسب بل ضرورة قانونية وتقنية لا يمكن الاستغناء عنها ، إلا أنه مدى أثر هذا الدور يتوقف على تنظيم تشريعي رصين يحقق حماية من خلال ما يوفره من ضمانات تتجسد بتحديد الالتزامات وإقرار المسؤوليات و الجزاءات القانونية الناجعة، وهو ما يفتقر اليه تشريعنا الوطني، والبحث في كل ما تقدم هو ما تضمنه بحثنا، وذلك بالتعريف بالمحل التجاري الإلكتروني وبيان أبرز أنواع الهجمات السيبرانية التي يتعرض لها المحل التجاري الالكتروني ، فضلاً عن تحديد دور الأمن السيبراني في تأمين الحماية للمحل التجاري الالكتروني لغرض الوقوف على أبرز النتائج والتوصيات، من خلال اعتماد المنهج التحليلي والمقارن لبيان النقص والفراغ التشريعي الذي يعتريه القانون العراقي في هذا الشأن .

المقدمة

أولاً : مدخل تعريفي بموضوع البحث و أهميته

تعد الهجمات السيبرانية خطراً واقعياً متزايداً على المحل التجاري الالكتروني ، لما تسببه من آثار قانونية واخرى اقتصادية تطال بمجملها النشاط التجاري وحقوق المتعاملين معه ،من حيث سلامة

المعاملات وسرية البيانات فضلاً عن الثقة المشروعة للمستهلك، الأمر الذي يتطلب توفير الحماية القانونية الناجمة الناجحة إلى جانب جملة من التدابير التقنية والفنية.

وأن حماية المحل التجاري الالكتروني يتطلب جملة تشريعات متطورة تنظم احكام التجارة الإلكترونية ، واتخاذ تدابير تقنية تحقق أمن المعلومات ،وبذلك سوف تساهم بشكل كبير بتحجيم فرص الاختراق الى جانب ذلك لابد من تطوير الأطر القانونية على الصعيد الوطني لمواكبة التطورات مع تعزيز وإدامة الوعي القانوني والتقني لدى كل من التاجر الالكتروني والمستهلك سواء بسواء ،تحقيقا للأمن القانوني وضماناً لاستدامة النشاط التجاري الإلكتروني في بيئة رقمية آمنة .

ثانياً : مشكلة البحث

تتمثل مشكلة البحث في أن المشرع العراقي لم ينظم أحكاماً كفيلة بتوفير حماية قانونية وتقنية متكاملة للمحل التجاري الالكتروني تتصدى للهجمات السيبرانية التي يتعرض لها ، وبالرغم من إصدار نظام تنظيم التجارة الإلكترونية العراقي لسنة ٢٠٢٥ إلا أنه جاء قاصراً عن توفير الحماية القانونية الكافية للمحل التجاري الالكتروني.

ثالثاً : تساؤلات البحث

تناول البحث الإجابة على العديد من التساؤلات التي نوجز أهمها :

١ـ ما هو المقصود بالمحل التجاري الالكتروني ؟

٢ـ ماذا نعني بـ الهجمات السيبرانية وما مدى خطورتها على المحل التجاري الالكتروني ؟

٣ـ ما هي التدابير التقنية والفنية والقانونية التي يحققها الأمن السيبراني للتصدي لهذه الهجمات ؟

٤ـ ما هو دور التشريعات الوطنية في الحد من الهجمات السيبرانية ؟

٥ـ هل للاتفاقيات الدولية دور في الحد من الجرائم الالكترونية ومنها الهجمات السيبرانية ؟

٦ـ ما هو دور المشرع العراقي في التصدي للهجمات السيبرانية التي تطال المحل التجاري الالكتروني؟

رابعاً : منهجية البحث

جاءت دراسة موضوع حماية المحل التجاري الالكتروني من الهجمات السيبرانية ، وفق المنهج التحليلي والمقارن، بعرض النصوص القانونية ذات الصلة والتعليق عليها ، من خلال تناول موقف مشرعنا العراقي وموقف القوانين محل المقارنة ، القانون الاماراتي والنظام السعودي .

Journal Of Babylon Center For Humanities Studies 2026 Volume :16 Issue : 9
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

خامساً : هيكلية البحث

للإحاطة بموضوع البحث من كافة جوانبه تم اتباع الهيكلية وفقاً للتفصيل الآتي :

المبحث الاول : تعريف المحل التجاري الالكتروني وابرز الهجمات التي تستهدفه.

المطلب الاول : تعريف المحل التجاري الالكتروني .

المطلب الثاني : أنواع الهجمات السيبرانية على المحل التجاري الالكتروني .

المبحث الثاني : الحماية التقنية والتشريعية للمحل التجاري الالكتروني.

المطلب الاول : الأمن السيبراني ودوره في حماية المحل التجاري الالكتروني .

المطلب الثاني : الحماية القانونية للمحل التجاري الالكتروني من الهجمات السيبرانية.

المبحث الاول

تعريف المحل التجاري الالكتروني وابرز الهجمات التي تستهدفه.

أن المحل التجاري الالكتروني هو منصة رقمية لبيع المنتجات والخدمات عبر الإنترنت، بالتالي يتعرض لمخاطر الهجمات السيبرانية بشكل متزايد تهدد استقراره وبيانات زبائنه عليه، سنقسم هذا المبحث على مطلبين يتناول المطلب الأول تعريف المحل التجاري الالكتروني و سنخصص المطلب الثاني لأنواع الهجمات السيبرانية على المحل التجاري الالكتروني.

المطلب الاول

تعريف بالمحل التجاري الالكتروني

سوف نتناول في هذا المطلب تعريف المحل التجاري الالكتروني فقهاً وقانوناً وفقاً للتفصيل الآتي :

الفرع الاول

تعريف المحل التجاري الالكتروني فقهاً

يعتبر مصطلح المحل الالكتروني من المصطلحات الحديثة التي ترتبط بالوسائل التقنية الحديثة التي تتسم بالتطور المستمر، وإن عدم وجود تنظيم قانوني للمحل الالكتروني في معظم التشريعات العربية أدى الى صعوبة إيراد تعريف جامع مانع لهذا المصطلح ، وعلى الرغم من ذلك حاول جانب من الفقه القانوني وضع تعاريف تبين المقصود بالمحل التجاري الالكتروني، حيث ينظر كل تعريف من منظور معين وذلك بهدف الوصول الى تحديد معالمه.

فقد عُرف بأنه : " نافذة بيع لمتاجر ومصانع قائمة يتم استخدامه في عرض خدماتها وتسويق منتجاتها عبر شبكة الانترنت، ويكون التسليم مادياً عن طريق وسائل الشحن والتوصيل التقليدية "[١]. يبين لنا التعريف كيفية عرض السلع والخدمات وهو عن طريق شبكة الانترنت، وبين

طريقة التسليم تكون مادية وبالوسائل التقليدية أي التي تصل الى الزبون يدوياً عن طريق مثلاً السيارة أو السفينة أو الطائرة الخ..... مما يعد مأخذاً على هذا التعريف لانه قصر التسليم على التسليم المادي فقط ، إذ انه يوجد نوع آخر من التسليم وهو التسليم المعنوي عن طريق الوسائل التقنية الحديثة مثلاً، إرسال كتاب الكتروني عبر تطبيق الواتس آب بمقابل مادي يدفع الكترونياً.

وعَرفه آخر بأنه : "خدمة الكترونية يتم الدخول إليها عبر شبكة الانترنت ومفتوحة لكل مستخدميها، وتسمح للتجار بعرض بضائعهم أو خدماتهم من خلالها " [٢]. يفهم من هذا التعريف أن المحل الالكتروني هو خدمة تقدم للمستهلكين وتكون مفتوحة فلا تحتاج الى خبرات برمجية للدخول اليها.

وعرفه فقيه آخر بأنه: " كتلة من العناصر تساهم في مجموعها في إنجاز العمل التجاري الالكتروني"[٣]. يلاحظ أن التعريف أبرز أمراً مهماً وهو أن المحل الالكتروني مجموعة من العناصر مجتمعة وليس مجرد عناصر منفردة . ويعاب على هذا التعريف أنه لم يبين هذه العناصر مادية فقط أم معنوية فقط أم انها مادية ومعنوية.

وعُرف أيضاً بأنه: " صفحة من صفحات الانترنت تتضمن جميع شروط التعاقد مع ايقونة القبول والتي توجد في آخر الصفحة، فمن خلال الضغط عليها يعبر المتعاقد عن قبوله بتلك الشروط أو رفضها، مما يعني عدم وجود التفاوض في حالة التعاقد من خلال موقع المحل التجاري الالكتروني " [٤]. ومما يؤخذ على هذا التعريف أنه حصر المحل التجاري الالكتروني في كيفية التعاقد وآليته ، ولم يبين كيفية عرض السلع والخدمات.

ونلاحظ على جميع التعاريف الفقهية السابقة ، التركيز على الجانب الفني التقني بقدر يفوق الجانب القانوني .

ولكل ماتقدم من تعاريف ، نقترح تعريف للمحل التجاري الالكتروني على أنه : " هو موقع أو أي وسيلة من الوسائل التقنية الحديثة على شبكة الانترنت ، من خلاله يقوم التاجر الالكتروني بعرض وبيع المنتجات والخدمات على المستهلكين بصورة غير مادية مع بيان مواصفاتها وأثمانها بصورة دقيقة ".

الفرع الثاني

تعريف المحل التجاري الالكتروني قانوناً

عرف المشرع العراقي المحل التجاري التقليدي في الفقرة (١) من المادة ٦٦ قانون التجارة الملغي رقم (١٤٩) لسنة ١٩٧٠ والتي نصت على أنه: " المتجر مجموعة من الأموال المنقولة تخصص لمزاولة تجارة معينة ".

و لم يتناول تعريفاً للمحل التجاري الالكتروني، و المحل التجاري التقليدي في قانون التجارة العراقي رقم (٣٠) لسنة ١٩٨٤ النافذ ، ولكن المشرع العراقي عرف المحل التجاري الالكتروني في الفقرة (٦) من المادة ١ من نظام تنظيم التجارة الالكترونية رقم (٤) لسنة ٢٠٢٥ والتي نصت على : " المتجر الالكتروني: أي وسيلة إلكترونية يستخدمها التاجر الالكتروني [٥] لعرض منتجاته أو خدماته على الزبون سواء أكانت تطبيقات إلكترونية، أو مواقع إلكترونية ، أو وسائل التواصل الاجتماعي ، أو غيرها من التقنيات الحديثة التي تربط التاجر الالكتروني بالزبون إلكترونياً " . يفهم من التعريف أن المشرع العراقي وسع من مفهوم المحل التجاري الالكتروني حيث نص على (أي وسيلة ، أو غيرها) فلم يذكر الوسيلة عى سبيل الحصر ، بل على سبيل المثال تحسباً للتطورات التقنية التي تزداد مع مرور الوقت ، وذكر الهدف من المحل وهو لعرض المنتجات أو الخدمات من قبل التاجر والتواصل مع الزبون بصورة الكترونية ، وجاء التعريف واسعاً ويشمل التطورات المستقبلية ، وحسناً فعل المشرع العراقي.

وبالرجوع الى النظام السعودي [٦] نجد أن المنظم السعودي عرف المحل التجاري الالكتروني في المادة (١) من نظام التجارة الالكترونية رقم (١٢٦) لسنة ١٤٤٠ النافذ نصت على أنه: " منصة ألكترونية [٧] تتيح لموفر الخدمة [٨]عرض منتج أو بيعه، أو تقديم خدمة، أو الإعلان عنها أو تبادل البيانات الخاصة بها ".

ويؤخذ على التعريف ، تضييقه لمفهوم المحل التجاري الالكتروني وحصره في المنصة الالكترونية فقط ، وبالتالي لا يغطي كل انواع المحلات التجارية الالكترونية المتخذة عبر الوسائل الإلكترونية.

وعُرفَ المحل التجاري الالكتروني في المادة (١) من القانون الاتحادي رقم (١٤) لسنة ٢٠٢٣ في شأن التجارة من خلال وسائل التقنية الحديثة والتي جاء فيها: المتجر الافتراضي: " موقع أو منصة أو غيرها من وسائل التقنية الحديثة [٩] تتيح للتاجر الرقمي[١٠] عرض سلعة أو خدمة أو بيعها أو تقديم خدمة، أو الإعلان عنها أو تبادل البيانات الخاصة بها من خلال تلك المواقع أو المنصات أو أي وسيلة من وسائل التقنية الحديثة الأخرى".

يُلاحظ أن المشرع الاماراتي لم يقتصر في تعريفه للمحل الالكتروني على المنصة فقط ، بل شمل المواقع واي وسيلة تقنية حديثة ، وذلك لان التطور المستمر للوسائل التقنية قد يظهر وسائل جديدة يمارس التاجر أعماله التجارية خلالها.

ومما تقدم نجد أن المشرع العراقي والتشريعات محل المقارنة، السعودي والاماراتي قد جاءت بتعريفات متشابهة من ناحية التركيز على الجانب الفني وإهمال الجانب القانوني، وإغفال

التشريعيين السعودي والاماراتي لذكر الطرف الأساسي في العمليات التجارية التي تتم عبر المحل التجاري الالكتروني وهو الزبون.

وتفوق المشرع الاماراتي والعراقي على المنظم السعودي، من جانب عدم حصر المحل التجاري الالكتروني بمنصة فقط ، بل وسعا من ذلك المفهوم ليشمل كل وسيلة تقنية حديثة يمكن ان تظهر أو موجودة تمكن التاجر من ممارسة أعماله التجارية .

وبالرغم من كل ذلك ، ليس مهمة المشرع إيراد تعريف بل يكون من اختصاص الفقه القانوني، وخاصة لحداثة المحل التجاري الالكتروني وتطوره المستمر وارتباطه بتقنيات التكنلوجيا الحديثة التي تتطلب وقتاً لمجاراتها تشريعياً.

المطلب الثاني

الهجمات السيبرانية على المحل التجاري الالكتروني وانواعها

إن البحث في الهجمات السيبرانية على المحل التجاري الالكتروني ستكون من خلال تعريفها وبيان أنواعها وهذا ما سيتضمنه الفرعين التاليين :

الفرع الاول

تعريف الهجمات السيبرانية

أن معنى كلمة سيبراني (cyber) تطلق على كل ما يتعلق بشبكات الإنترنت والفضاء السيبراني يعني الفضاء الإلكتروني وهو كل ما يتعلق بشبكات الإنترنت الحواسيب والتطبيقات والمواقع المختلفة(١١).

وقد عُرف الهجوم السيبراني فقهاً بأنه : " الهجوم على المواقع الإلكترونية باستخدام وسائل إلكترونية لتعطيلها أو تدميرها والإضرار بها " (١٢). وعرفه آخر بأنه : " برامج الكترونية ، يتم استخدامها بواسطة الانترنت ، من قبل اشخاص او جهات معينة ، بهدف السيطرة والتحكم في مواقع التجارة الالكترونية التابعة لأشخاص آخرين مسببة اضراراً جسيمة في تلك المواقع " (١٣).

أما على صعيد التشريع لم يعرف المشرع العراقي الهجمات السيبرانية ، لأنه لم يتناول في الأصل هذا الموضوع . في حين عرفه المنظم السعودي وذكره على أنه الدخول غير المشروع حيث عرفه بأنه : " دخول شخص بطريقة متعمدة إلى حاسب آلي ، أو موقع الكتروني ، أو نظام معلوماتي أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها " (١٤).

وقد عرف المشرع الإماراتي كلمة (السيبراني) بأنها " كل ما يتعلق بالشبكات المعلوماتية الحاسوب وشبكة الانترنت والبرامج المعلوماتية المختلفة وكل الخدمات التي تقوم بتنفيذها " (١٥).

وعرف التهديدات السيبرانية هي " المخاطر التي تواجه الأشخاص الطبيعية / الاعتبارية على

الشبكة الالكترونية ، وقد يكون التهديد متعمد ومخطط له بهدف لمحاولة فضح أو تغيير أو تعطيل أو تدمير أو سرقة أو الوصول الغير مصرح به للأصول أو النظم أو البنى التحتية أو الشبكات الإلكترونية أو المعلومات لأغراض شخصية أو سياسية أو اقتصادية أو تخريبية أو مكاسب مالية " [١٦] . مما تقدم نجد ان المشرع الإماراتي كان الأكثر توضيحاً ما المقصود بالهجمات السيبرانية حيث تناوله بشكل مفصل وهو ما لم نجده في التشريع السعودي الذي جاء بشكل مقتضب وفي الوقت الذي لم يعرفه المشرع العراقي وبدورنا ندعو المشرع العراقي لمسايرة التطورات والمشاركة في العالم الرقمي اسوة بالتشريعات الأخرى ومنها التشريعات محل المقارنة ، ولكن لم يكن المشرع الاماراتي موفقاً من حيث الصياغة اذ استخدم كلمة التهديدات بدلاً من الهجوم وهي تهديدات غير مؤكدة الوقوع تسبق الهجوم السيبراني .

الفرع الثاني

أنواع الهجمات التي يتعرض لها المحل التجاري الإلكتروني

تتخذ الهجمات السيبرانية انواعاً وأشكالاً مختلفة بحسب الوسائل التقنية المستخدمة وطبيعة الهدف التي تبغي تحقيقه وهي في تزايد مستمر، عليه سنتناول في هذا الفرع ابرز هذه الهجمات وكما يأتي :

أولاً : استخدام برامج فايروسية

تؤدي هذه البرامج إلى إحداث اضرار بوسائل مادية ملموسة تكون مرتبطة ببرامج إلكترونية ، مثل بطاقات الدفع الإلكتروني التي هي عبارة عن الوسائل المادية مرتبطة ببرامج إلكترونية معينة و قرصنة هذه البرامج يؤدي إلى عدم إمكانية استعمال تلك البطاقة من قبل المستهلك الإلكتروني وحصوله على المنتجات والخدمات[١٧]، فقد يقوم المخترق باختراق الحسابات الشخصية لكبار الزبائن الذين يتعاملون باستمرار مع المحلات التجارية الإلكترونية وذلك عن طريق نظام التحويلات الدولي بين البنوك وسرقة بطاقة الائتمان من مراكز التسوق الدولية الكبيرة وسحب ملايين الدولارات من أصحاب هذه البطاقات [١٨] وعن طريقها يستطيع الوصول إلى عنوان المحل التجاري الإلكتروني ومعلوماته الخاصة لاستخدامها بعد ذلك في إنشاء محل تجاري الكتروني وهمي فيصبح هنالك محلاً وهمي و أصلي يحملان العنوان نفسه فيقوم المخترق بعد ذلك باستعمال جميع المعاملات التجارية والمالية المقدمة من المحل التجاري الإلكتروني الأصلي و المعلومات الخاصة ببطاقات الدفع الإلكتروني واستخدامها بصورة غير مشروعة في المحل وهمي [١٩]، أو أن يقوم المخترق بمراقبة البريد الإلكتروني بين التاجر الإلكتروني والمستهلك فعندما يطلب التاجر من المستهلك تحويل ثمن المنتجات أو الخدمات على رقم حسابه في

المصرف ، فينشئ المخترق بريد إلكتروني مشابه لبريد المحل التجاري الإلكتروني العائد للتاجر، وبعد ذلك يرسل للمستهلك بأنه غير رقم حسابه ويطلب منه إعادة إدخال رقم بطاقته المصرفية لأعمال البيع التي تم الاتفاق عليها وبمجرد إدخال المستهلك رقم يقوم المخترق بسرقة جميع أمواله[٢٠].

ثانياً : استخدام برامج الفدية (البرمجيات الخبيثة)

وهي فيروسات إلكترونية تعمل على حجب الوصول إلى المحلات التجارية الإلكترونية أو تشفير البيانات الموجودة على موقع المحل التجاري وطلب مبلغ مالي كبير مقابل فك تشفير البيانات المسروقة [٢١]، أو قد يكون المقرصن هو منافس للمحل التجاري الإلكتروني فنتيجةً للمنافسة التجارية الكبيرة قد يخترق المحل التجاري الإلكتروني لغرض الاطلاع على معلومات المحل التجاري الإلكتروني المنافس ، لغرض تحقيق ارباح تجارية[٢٢]، أو يقوم المقرصن بحذف أو إنشاء أو إتلاف أو تدمير أو إعادة نشر بيانات أو تغييرها كتغير الأسعار للمنتجات والخدمات المعروضة إما بمضاعفتها أو تخفيضها بشكل مبالغ وفي الحالتين يضر بالمحل التجاري الإلكتروني أو يحذف بعض المنتجات من الكتلوج المعروض فيه هذه المنتجات على أساس أنها غير متوفرة أو يقوم بابتزاز صاحب المحل التجاري بالامتناع عن ممارسة تجارة معينة [٢٣].

ثالثاً : هجمات رفض أداء الخدمة

يقوم المقرصن بغلق المحل التجاري الإلكتروني نهائياً و تعطيله عن العمل وتدميره عن طريق حجب الخدمة أو هجمات رفض أداء الخدمة حيث يرسل رسائل مزيفة إلى موقع المحل التجاري الإلكتروني وبصورة مكثفة جداً ، يؤدي إلى خلل نظام تلقي الرسائل من المستهلكين والتأثير على السعة التخزينية لموقع المحل التجاري الإلكتروني وبالتالي تفجيره وتفتيت البيانات والمعلومات عليه ، ومن ثم منع المستهلكين من الوصول إلى المحل التجاري الإلكتروني [٢٤].

رابعاً : التصيد الاحتيالي للمستهلكين

يكون التصدي الاحتيالي في إرسال رسائل احتيالية عن طريق البريد الإلكتروني أو الرسائل القصيرة، لغرض التسويق لمنتج وهمي أو مشاريع وهمية أو لكسب جائزة من المحل التجاري الإلكتروني الذي يتعامل معه المستهلك عادةً ومحاولة خداع المستهلك ، فينتقل المستهلك إلى الموقع الوهمي ويبدأ بملء بياناته التي تشبه البيانات التي كتبها أثناء الطلب من موقع المحل التجاري الذي يتعامل معه ، أو إرسال روابط بمجرد فتحها يستولي على جهازه والبيانات الشخصية [٢٥] .

خامساً : فايروس طروادة

حيث يستخدمه المخترق ويدخل الأجهزة بدون علم أصحابها وذلك باستخدام كلمة المرور التي يستخدمها صاحب الجهاز، ومن ثم لا يمكن ملاحظة وجوده، إذ ظاهره يبدو برنامج عادي ومفيد، بمجرد دخوله الجهاز المستخدم يصبح نشيطاً ويقوم بوته الضارة ، ويعد من البرامج الخطيرة لأنه لا يمكن كشفه بوسائل كشف البرامج الضارة ، الامر الذي يتطلب حرفية عالية لاكتشافه [٢٦].

من خلال ما تم بحثه في أنواع الهجمات السيبرانية يبدو واضحاً الخطورة والتحدي الكبيرين وما يشكلانه على عمل المحل التجاري الالكتروني فإذا ما طالته فسوف يؤدي الى تعطيل العمل به بالكامل الأمر الذي يتوجب توفر حماية فنية وقانونية للأمن السيبراني لإيقاف تلك الهجمات وهو ما يتم البحث عنه خلال المبحث التالي.

المبحث الثاني

الحماية التقنية والتشريعية للمحل التجاري الالكتروني

لمعرفة الحماية التقنية والتشريعية للمحل التجاري الالكتروني يتطلب ذلك الوقوف على الأمن السيبراني والحلول التشريعية والاتفاقيات الدولية لحماية المحل التجاري الالكتروني عليه ، سنبين ذلك من خلال تقسيم هذا المبحث على مطلبين، سنتطرق في المطلب الأول للأمن السيبراني ودوره في حماية المحل التجاري الالكتروني ،أما المطلب الثاني سيخصص للحماية القانونية للمحل التجاري الالكتروني من الهجمات السيبرانية.

المطلب الاول

الأمن السيبراني ودوره في حماية المحل التجاري الالكتروني

يُعد الأمن السيبراني وسيلة فاعلة وحيوية في تأمين الحماية المحل التجاري الالكتروني فيما يتعرض له من مخاطر الهجمات السيبرانية، وذلك في جملة من التدابير والاجراءات القانونية وأخرى تقنية وتنظيمية والتي تهدف في في عملها سلامة سير العمل في المحل التجاري الالكتروني، وهذا ما سيتضمنه هذا المطلب في فرعين ،الأول بيان المقصود بالأمن السيبراني والثاني البحث في طرق الأمن السيبراني .

الفرع الاول

تعريف الأمن السيبراني

عُرف الأمن السيبراني بأنه : " مجموعة من الأدوات التنظيمية والتقنية والإجرائية ، والممارسات الهادفة إلى حماية الحواسيب والشبكات وما بداخلها من بيانات ومعلومات من الاختراق أو

التلف أو التغيير أو تعطيل الوصول للمعلومات أو الخدمات ، ويعد توجهاً عالمياً سواء كان على مستوى الدول أو المنظمات الحكومية أو الشركات " [٢٧] .

جاء تعريف الأمن السيبراني في اللائحة الإطارية للمنصات والخدمات الرقمية العراقية لسنة ٢٠٢٥ على أنه : " تنفيذ التدابير القانونية والتقنية والتنظيمية لحماية المنصات والمستخدمين من التهديدات السيبرانية " [٢٨].

أما المنظم السعودي فقد عرف الأمن السيبراني بأنه : " حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ، ومكوناتها من أجهزة وبرمجيات ، وما تقدمه من خدمات ، وما تحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع ... " [٢٩]. ولم يضع المشرع الاماراتي تعريفاً للأمن السيبراني في قرار مجلس الوزراء بشأن لجنة مكافحة التهديدات السيبرانية والبرمجيات الخبيثة ولا في قانون مكافحة الشائعات والجرائم الالكترونية.

الفرع الثاني

طرق الامن السيبراني في حماية المحل التجاري الالكتروني

تختلف طرق الامن السيبراني في مواجهة الهجمات السيبرانية لحماية المحل التجاري الإلكتروني، وبالتالي حماية المستهلك المتعامل مع المحل التجاري الإلكتروني ، ويجب أن تستخدم المحلات تدابير وقائية من الأمن السبراني التي تمكنها من اكتشاف الهجمات السيبرانية ، وهذه الطرق هي :

أولاً : جدران الحماية النارية(fire wall)

وهذه الجدران هي برامج توضع من قبل الشركات والمؤسسات المختصة في البرامج الإلكترونية وتوضع في الحواسيب الإلكترونية ويوضع بين شبكة الإنترنت وشبكة الداخلية لمواقع المحلات التجارية الالكتروني ، وذلك لحمايتها من السرقة والاختراق وهذه الجدران يمكن تثبيتها على الأجهزة النقالة أيضاً [٣٠].

ثانياً : التخزين الاحتياطي

هو عملية اجراء نسخ احتياطية من المعلومات والبيانات وحفظها في مكان آمن ، تمكن التاجر من الرجوع إليها في حال تم تدمير محله التجاري الإلكتروني عن طريق تدمير بياناته ، ويعد هذا المكان الآمن لسلامة بيانات المحل التجاري الإلكتروني ، وبالتالي المحافظة على بيانات المستهلكين أيضاً [٣١].

ثالثاً : استخدام برامج مضادة للفيروسات(antivirus)

وهذه البرامج تستخدم الاكتشاف ومحاربة الفيروسات والبرامج المضرة والخبيثة والعمل على محوها كلياً من النظام ومنعها من أحداث الأضرار للبيانات الشخصية للمستهلكين[٣٢].

رابعاً : استخدام أنظمة كشف التسلل (IDS)

تستخدم هذه الأنظمة للكشف عن المحاولات الغير مرغوب بها للدخول والتلاعب بالنظام الإلكتروني للمحل التجاري الإلكتروني فهي " أجهزة استشعار تنبه على وقوع الأحداث، ولوحة تحكم لمراقبة الأحداث والتنبيهات والتحكم بأجهزة الاستشعار، ومحرك يقوم بتسجيل إدخالات الأحداث المتلقاة من خلال أجهزة الأستشعار في قاعدة البيانات" [٣٣].

خامساً : استخدام تقنيات التشفير للبيانات

يلعب التشفير دوراً مهماً في تأمين المعاملات الإلكترونية التي تتم عبر المحل التجاري الإلكتروني لما يحققه من سرية وخصوصية البيانات ، فهو يهدف إلى منع المقرصنين من السيطرة على رسائل البيانات التي قد تتضمن البيانات الخاصة أو أرقام بطاقات الائتمان ، فعند السيطرة عليها من قبل الهجمات السيبرانية يؤدي ذلك إلى الخسارة المادية والمعنوية للطرفين التاجر والمستهلك.[٣٤]

وقد عرف التشفير بأنه : "عملية تحويل النص إلى رموز وإشارات غير مفهومة تبدو غير ذات معنى لمنع الغير من الاطلاع عليها ، إلا الأشخاص المرخص لهم بالإطلاع على النص المشفر وفهمه، مما تتصب عملية التشفير على القيام بتحويل النصوص العامة إلى نصوص مشفرة ، مع إمكانية إعادة النص المشفر إلى نص عادي بدون فك التشفير " [٣٥] .

وللتشفير أنواع تتمثل بما يأتي :

١ ـ التشفير المتماثل

في هذه التقنية يتفق المستهلك مع التاجر على كلمة مرور يتم استخدامها عند البيع والشراء عبر المحل التجاري الإلكتروني ، أي يتم استخدام نفس كلمة المرور بين الطرفين ، فعند استلام الرسالة من قبل أحدهما يقوم باستخدام كلمة المرور المتفق عليها وتقوم برمجيات التشفير بتحويل النص المشفر إلى الشكل الأصلي له ليتم فهمه [٣٦].

٢ ـ التشفير بالمفتاح الخاص والعام

بعد تراجع استخدام التشفير المتماثل وذلك لوجود أهم عيب فيه وهو تبادل المفتاح السري مما أدى إلى عدم الثقة في هذه التقنية ، تم اللجوء إلى تقنية المفتاح العام والخاص ويتجنب هذا

النوع من التقنية تبادل نفس الرمز السري للطرفين ، بل يستخدم في التشفير مفتاحان ، أحدهما خاص والآخر عام [٣٧].

والمفتاح الخاص هو مجموعة من الأرقام والرموز التي تخزن على بطاقة إلكترونية ، ويكون هذا المفتاح معروفاً لطرف واحد فقط ويستعمل لفك تشفير الرسالة التي شُفرت بواسطة المفتاح العام للطرف الآخر وسمي بالمفتاح العام ، لانه عام للجميع عبر شبكة الإنترنت فعندما يقوم المستهلك بالشراء عبر المحل التجاري الإلكتروني يأخذ مفتاحه العام الموجود في الشهادة الرقمية [٣٨] ويتم التأمين من خلال(SSL) وبعد ذلك يستخدمه المستهلك لتشفير بيانات الدفع وإرساله إلى المحل الإلكتروني الذي يفك التشفير بمفتاحه الخاص به فقط [٣٩].

ولنجاح التشفير لابد من استخدام تقنيات خاصة إجرائية توفر الحماية التي تحتاجها المعاملات الإلكترونية المختلفة التي تتم عبر المحل التجاري الإلكتروني ومن بين هذه البرامج :

١ ـ تقنية (SSL)

تكون قوة التشفير في هذا البرنامج قوية ومن الصعوبة فكها وهو برنامج تم تخصيصه لتشفير المعلومات والبيانات ونقلها بين جهاز المستهلك وبين المحل التجاري الإلكتروني بطريقة آمنة لا يستطيع أحد الاطلاع عليها. ويتميز هذا البرنامج عن باقي برامج التشفير في عدم الطلب من المستهلك بالقيام بأي خطوات لتشفير معلوماته أو بيانات التي يريد حمايتها، والمطلوب منه فقط التأكد من أنه يريد استخدام هذا البرنامج (SSL) للتشفير [٤٠]

حيث يقوم المستهلك الذي يرغب بالشراء من المحل التجاري الإلكتروني الدخول إلى الطريق الآمن وفقا لنظام التشفير(SSL)، وبمجرد موافقة المحل التجاري الإلكتروني على ذلك ينتقل المستهلك إلى نظام (SSL) ويقوم المتصفح بالارتباط بالخادم الخاص بالموقع المحل التجاري الإلكتروني وطلب الشهادة الرقمية وتاريخ انتهاء الصلاحية ومن ثم يتم تشفير جميع المعلومات والبيانات وقنوات الإرسال والاتصال بين الطرفين التاجر المستهلك ، و باستطاعة المستهلك التأكد من إكمال عملية التشفير من خلال ملاحظة القفل المفتوح من الشاشة قد اقفل[٤١].

ويمكن تلخيص الخطوات العملية لاستخدام تقنية (SSL) بتقدم المحل التجاري الإلكتروني بطلب لأحد الجهات المخصصة لإصدار الشهادة الرقمية ، ومن خلالها يحصل على شهادة (SSL) ، وتتم الموافقة على طلب المحل التجاري الإلكتروني بعد اتخاذ إجراءات معينة ومنها التأكد من نشاط المحل التجاري الإلكتروني وفحص البيانات المقدمة ، وتتضمن هذه الشهادة اسم المحل التجاري الإلكتروني ، وتاريخ إنشائه وإصدار المفتاح العام والخاص بالمحل التجاري

والذي يكون مزودا ببرنامج التشفير (SSL) ، وبعد ذلك يتم تخزينه في موقع المحل التجاري الإلكتروني [٤٢].

٢ ـ تقنية (SET)

بالإضافة لتقنية التشفير لمستوى التصفح (SSL) ،أصبحت المعاملات المالية الإلكترونية يتم تشفيرها عبر المحل التجاري الإلكتروني بتقنية التشفير (SET) وتمثل هذه التقنية خطوة أساسية ومهمة على تأمين كافة عمليات الدفع الإلكتروني ، بالإضافة للمعاملات الإلكترونية ككل التي تتم عبر المحل التجاري الالكتروني تضمن هذه التقنية للتاجر التحقق من شخصية المستهلك الحقيقية أي أنه هو من يستخدم بطاقته الائتمانية للدفع ، وأنه يقبل العمل بتقنية تشفير (SET) [٤٣] .

وتتطلب هذه التقنية اشتراك كل من التاجر والمستهلك لدى أحد البنوك التي تعمل بنظام (SET) وبعد التأكد من هوية التاجر المستهلك عن طريق تبادل الشهادات المسلمة من قبل البنك للتاجر والمستهلك الدالة على شخصية كل منهما ، بحيث لا يتمكن أحد من الاطلاع على المعلومات سوى المستهلك والتاجر ، وذلك لكونها مشفرة [٤٤].

وبعد ذلك تأتي مرحلة الدفع والسداد للمنتج أو الخدمة المتعاقد عليها ، ويقوم المستهلك بتغيير رقم بطاقته الائتمانية ولا يمكن فكها إلا من قبل البنك الضامن لكل من التاجر والمستهلك ، وبعد تأكد التاجر من الطلب المرسل من المستهلك وتأكيده ، يرسل التاجر طلب الشراء إلى البنك لتوثيقه، وبعد التوثيق والتأكد من حساب المشتري أنه كافي لعملية الشراء من قبل البنك والتأكد من هوية التاجر، يتم بعد ذلك إرسال المنتج من المحل التجاري الالكتروني إلى المشتري ويتم التسليم إلكترونياً او مادياً إذا كان المنتج يتطلب التسليم المادي [٤٥].

المطلب الثاني

الحماية القانونية للمحل التجاري الالكتروني من الهجمات السيبرانية

إن لجسامة الأضرار التي تكبدها الهجمات السيبرانية للمحل التجاري الالكتروني وقد تكلمنا عن الحماية التقنية والفنية التي تحققها إجراءات الأمن السيبراني فإن للتشريع دوره في إضفاء الحماية القانونية للأمن السيبراني من تلك الهجمات على الصعيدين الداخلي والدولي وهو ما سيتم بحثه في هذا المطلب بفرعين وكما يلي :

الفرع الأول

دور التشريعات الوطنية في مكافحة الهجمات السيبرانية

لقد الزم المشرع العراقي التاجر الإلكتروني وذلك من خلال النص على انه: " إتباع أفضل الممارسات والمعايير الدولية في مجال الأمن السيبراني لحماية متجر الالكتروني من الهجمات الإلكترونية " [٤٦]. يلاحظ أن موقف المشرع العراقي جاء بصورة عامة وواسعة ولم يضع جهة مسؤولة عن الرقابة على اتباع إجراءات الأمن السيبراني من قبل التاجر ولم يحدد جزاءات الإخلال بالأمن السيبراني، بالرجوع إلى القواعد العامة في قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل الذي وضع أسس القواعد العامة لتجريم الأفعال التي تتسبب في الاعتداء على الأموال أو إساءة استعمال الوسائل التقنية حيث نص على أنه : " يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد على ١٠٠ دينار أو بإحدى هاتين العقوبتين من نشر بإحدى طرق العلانية اخباراً أو صوراً أو تعليقات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة إذا كان من شأن نشرها الإساءة إليهم" [٤٧]. ومع غياب النصوص القانونية المباشرة في تحقيق الأمن السيبراني في القانون العراقي تبرز الحاجة الملحة لإقرار مشروع قانون مكافحة الجرائم الالكترونية لسنة ٢٠١٩ والذي جاء فيه : " يعاقب بالحبس مدة لا تقل عن سنة واحدة ولا تزيد على سنتين وبغرامة لا تقل عن (١٠٠٠٠٠٠) مليون دينار إلى عراقي ولا تزيد على (٣٠٠٠٠٠٠) ثلاثة ملايين دينار عراقي كل من تنصت لأي رسائل عن طريق شبكة المعلوماتية وأجهزة الحاسوب أو مافي حكمها او التقطها او اعترضها دون تصريح بذلك من الجهة المختصة أو الجهة المالكة "[٤٨].

ونص أيضاً على أنه : " يعاقب بالحبس مدة لا تقل على عن ثلاث سنوات ولا تزيد على خمس سنوات وبغرامة لا تقل عن) خمس ملايين دينار عراقي ولا تزيد على (١٠٠٠٠٠٠٠) ملايين دينار عراقي كل من يستخدم شبكة المعلومات أو احد اجهزة الحاسوب أو مافي حكمها بقصد تهديد أو ابتزاز شخص آخر لحمله على القيام بفعل أو الامتناع عنه ولو كان هذا الفعل أو الامتناع مشروعاً " [٤٩].

فضلاً عن أنه عاقب على الجرائم الواقعة على البطاقات الإلكترونية حيث نص على أنه: " يعاقب بالحبس مدة لا تقل عن ثلاث سنوات ولا تزيد على خمس سنوات وبغرامة لا تقل عن (١٠٠٠٠٠٠٠) ملايين دينار عراقي ولا تزيد على (١٥٠٠٠٠٠٠) خمسة عشر مليون دينار عراقي كل من استخدم شبكة المعلومات أو أحد أجهزة الحاسوب وما في حكمها للوصول الى

أرقام وبيانات البطاقات الإلكترونية أو ما في حكمها بقصد استخدامها في الحصول على بيانات الغير أو أمواله أو ما تتيحه تلك البيانات او الارقام من خدمات " [٥٠].

أما المنظم السعودي فقد أولى جهة تتمتع بالشخصية المعنوية والاستقلال الإداري والمالي [٥١] متخصصة في الأمن السيبراني وتدعى بالهيئة الوطنية لشؤون الأمن السيبراني فهي تعد المرجع الوطني ولا تخلو اي جهة عامة او خاصة أو غيرها من مسؤوليتها تجاه أمنها السيبراني [٥٢]، وتقوم هذه الهيئة بوضع المعايير والسياسات الوطنية للتشفير ومتابعة تحديثها والالتزام بها وتنظيم مشاركة البيانات والمعلومات التي تكون مرتبطة بالأمن السيبراني بين الجهات والقطاعات المختلفة في المملكة والإشراف عليها وتقوم بتطوير مؤشرات قياس الأداء الخاصة بالأمن السيبراني وإعداد التقارير الدورية حول حالة الأمن السيبراني على المستويين الوطني والقطاعي وتقوم بتنظيم الحملات والبرامج التوعوية والمسابقات وإصدار المجلات والدوريات والكتب والكتيبات والأدلة الإرشادية والنشرات في مجال اختصاصاتها[٥٣] . وقد عد المنظم السعودي الهجمات السيبرانية على أنها جريمة الكترونية حيث جاء في نظامه بأنه : " يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على (٥٠٠,٠٠٠) ريال او باحدى هاتين العقوبتين كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية: الدخول غير المشروع الى موقع إلكتروني أو الدخول الى موقع إلكتروني لتغيير تصاميم هذا الموقع ، أو إتلافه ، أو تعديله ، أو شغل عنوانه " [٥٤].

وجاء فيه أيضاً يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال ، أو بإحدى هاتين العقوبتين ، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية : " الوصول دون مسوغ نظامي صحيح إلى بيانات بنكية أو ائتمانية .... " [٥٥]. ونص أيضاًعلى أنه : " يعاقب بالسجن مدة لا تزيد على اربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال ، او باحدى هاتين العقوبتين ، كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية : ٢ـ إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها او تدمير او مسح البرامج أو البيانات الموجودة أو المستخدمة فيها او حذفها أو تسريبها أو إتلافها أو تعديلها. ٣ـ إعاقة الوصول إلى الخدمة، أو تشويشها ، أو تعطيلها، بأي وسيلة كانت"[٥٦].

في حين انشأ المشرع الاماراتي لجنة لمكافحة التهديدات السيبرانية والبرمجيات الخبيثة حيث نظم أحكام هذه اللجنة بقانون كامل، يبين كيفية عمل اللجنة وصلاحياتها و تكون مختصة بمكافحة التهديدات السيبرانية والبرامج الخبيثة بكافة أنواعها وهي تشبه عمل الهيئة في المملكة العربية السعودية [٥٧] . والمشرع الاماراتي نص على أنه : " يعاقب بالسجن المؤقت مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن (٥٠٠,٠٠٠) درهم ولا تزيد على ثلاثة ملايين درهم من

حصل او استحوذ او عدل او اتلف او افشى أو سرب أو الغى أو حذف أو غير أو نسخ أو نشر أو أعاد نشر بغير تصريح معلومات أو بيانات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية بإستخدام تقنية المعلومات أو وسيلة تقنية معلومات " [٥٨] ونص على أنه : " يعاقب بالحبس والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم ولا تزيد على (٢٠٠٠,٠٠٠) مليوني درهم، أو بإحدى هاتين العقوبتين، كل من زور أو قلد أو نسخ بطاقة ائتمانية أو بطاقة مدينه أو أي وسيلة من وسائل الدفع الإلكتروني أو استولى على بياناتها أو معلوماتها، وذلك باستخدام وسائل تقنية المعلومات، أو نظام معلوماتي"[٥٩]. بالإضافة الى أنه نص على " يعاقب بالحبس والغرامة التي لا تقل عن (١٠٠,٠٠٠) مائة الف درهم ولا تزيد على (٣٠٠,٠٠٠) ثلاثمائة الف درهم أو باحدى هاتين العقوبتين كل من اخترق موقع الكتروني أو شبكة معلومات أو وسيلة تقنية معلومات " [٦٠].

الفرع الثاني

دور الاتفاقيات الدولية في مكافحة الجرائم الالكترونية

إن للأتفاقيات الدولية دور واضح في مكافحة الجرائم الالكترونية ومنها الهجمات السيبرانية ووفقاً للتفصيل الآتي :

أولاً : الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

تبنى مجلس وزراء الداخلية والعدل العرب في ٢٠١٠/١٢/٢٣ الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لمكافحة الجرائم التقنية ، هدفت هذه الاتفاقية إلى تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم المعلومات والتقنيات التي تتم عبر شبكات الانترنت ومنها الاعتداء على المحلات التجارية الالكترونية والحفاظ على مصالح الدول العربية و أمن مجتمعاتها [٦١]، ومن بين النصوص التي حمت بها هذه الاتفاقية المحلات التجارية الالكترونية من الهجمات السيبرانية ، تجريم الدخول غير المشروع الى المحلات التجارية الالكترونية ومحو او تعديل او تشويه او نسخ او نقل او تدمير البيانات المحفوظة في الاجهزة والانظمة الالكترونية وإلحاق الضرر بالمستخدمين والمستفيدين [٦٢]، وايضاً الاعتداء على سلامة البيانات أو محوها أو إعاقة الوصول إليها [٦٣]. وايضا تجريم الاستخدام غير المشروع لادوات الدفع الالكترونية [٦٤]. وقد صادق العراق عليها في تاريخ ٢٠١٠/١٢/٢١ وحسناً فعل وصادقت عليها السعودية والامارات العربية المتحدة [٦٥].

ثانياً : اتفاقية بودابست لمكافحة جرائم المعلوماتية الدولية

تعد هذه الاتفاقية أول اتفاقية دولية لتجريم الجرائم الإلكترونية الواقعة على المحلات التجارية الالكترونية والمواقع بشكل عام . تم التوقيع عليها بتاريخ ٢٠٠١/١١/٢٣ ، وتضم مجموعة دول من الاتحاد الأوروبي حيث ركزت على وضع الأساليب التي تسهل الملاحقة الجنائية لمرتكبي الجرائم الإلكترونية بين الدول الموقعة، وذلك لأن الهجمات السيبرانية قد تتجاوز حدود الدول الوطنية بالاضافة الى قيامها بتسهيل تبادل المجرمين بين الدول الموقعة على هذه الاتفاقية[٦٦]، حيث جاء فيها : " يقدم الطرفان لبعضهما البعض المساعدة المتبادلة على أوسع نطاق من ممكن لأغراض التحقيقات والإجراءات المتعلقة بالجرائم الجنائية المتعلقة بأنظمة الكمبيوتر والبيانات ....." [٦٧]. والجدير بالذكر ان العراق لم يصادق على هذه الاتفاقية .

نستخلص من كل ما سبق ، أن المحلات التجارية الالكترونية بحاجة إلى تدابير تقنية وفنية تواجه هذه الهجمات و إلزام التجار الإلكترونيين باتخاذ كافة وسائل الوقاية التقنية التي تحمي المحلات التجارية ومنها الجدران النارية و التشفير والنسخ الاحتياطي وغيرها، عليه نتمنى على المشرع العراقي و إنشاء لجنة مكافحة التهديدات السيبرانية التي تكون مسؤولة عن الأمن السيبراني في كل قطاعات الدولة بشكل عام وفي المحلات التجارية الالكترونية بشكل خاص ، والتي تقوم بتنظيم الحملات التوعوية والأدلة الإرشادية لمساعدة المستهلكين في معرفة نوع الهجمات والوقاية منها.

الخاتمة

بعد أن أنتهينا من كتابة بحثنا المتواضع توصلنا الى جملة من الأستنتاجات والتوصيات نلخصها بما يلي:

أولاً : النتائج

١ـ تشكل الهجمات الالكترونية تهديداً كبيراً مباشراً على على استقرار المعاملات التجارية الالكترونية وتؤثر على ثقة المستهلكين بالمحل التجاري الالكتروني وذلك لانتهاك خصوصيتهم ، وتؤثر على التاجر أيضاً إذ تؤدي إلى خسارته المالية الكبيرة وإضعاف سمعته التجارية.

٢ـ يتضح من خلال التشريعات محل المقارنة أنها قد نظّمت بصورة شاملة ما يتعلق بإجراءات الأمن السيبراني، من خلال وضع أطر تنظيمية وهيئات مختصة وتدابير وقائية ملزمة، في حين أن المشرع العراقي لم يتناول تنظيم الأمن السيبراني تنظيماً مستقلاً ومتكاملاً، مكتفياً بنصوص متفرقة لاتحقق الحماية الوقائية المنشودة.

٣ ــ في الوقت الذي يشهد فيه المحل التجاري الألكتروني تطوراً متسارعاً واتساع في نطاق التعامل به، تتزايد الهجمات السيبرانية التي تواجهه في ظل قصور تشريعي وطني يوفر حماية وضمانات قانونية للمحل التجاري الالكتروني ، وقد كان آخرها مشروع قانون الجرائم الالكترونية (الذي لم يتم اقراره كقانون لحين اعداد هذا البحث) إذ أغفل تنظيم لأحكام عقابية تجرم هذه الهجمات الواقعة على التجارة الالكترونية بشكل عام والمحل التجاري الالكتروني بشكل خاص.

ثانياً : التوصيات

١ــ بالرغم من من إصدار المشرع العراقي لنظام تنظيم التجارة الإلكترونية وتنظيم المحل التجاري الالكتروني إلى أنه لا يخلو من القصور وعليه ، ندعو المشرع العراقي الى اصدار قانون خاص متكامل ينظم كل مايتعلق بالمحل التجاري الالكتروني .

٢ ــ دعوة المشرع العراقي الى تضمين مشروع قانون الجرائم الألكترونية لأحكام قانونية تجرم الهجمات السيبرانية الواقعة على التجارة الالكترونية بشكل عام والمحل التجاري الالكتروني بشكل خاص ، لتجسد ما نص عليه مشروع القانون في مادته الثانية (أهداف هذا القانون) و التي تنص على حماية الافراد والمجتمع من الجرائم الالكترونية، كما نتمنى عليه الاسراع في اقراره كقانون لسد فراغاً تشريعياً واضحاً في هذا المجال .

٣ ــ نتمنى على المشرع العراقي تشريع قانون خاص بالأمن السيبراني ، ويُعنى بتشكيل هيئة وطنية للامن السيبراني تقوم بوضع الضوابط والارشادات الفنية إلزامية للمحلات التجارية الالكترونية ، وذلك لحماية أنظمة وبيانات المحل التجاري الالكتروني والمستهلكين من الاختراق والتسريب ، أسوةً بما جاء في تنظيم الهيئة الوطنية للأمن السيبراني السعودي ولجنة مكافحة التهديدات السيبرانية والبرمجيات الخبيثة الاماراتي.

الهوامش

(١) د. خالد ممدوح إبراهيم ، إبرام العقد الالكتروني دراسة مقارنة ، ط ١، دار الفكر الجامعي ، الإسكندرية ، ٢٠٠٦ ، ص٣٩.

(٢) د. أسامة أبو الحسن مجاهد ، التعاقد عبر الانترنت ، دار الكتب القانونية ، مصر، ٢٠٠٥، ص ١٣.

(٣) حنان مليكة ، المتجر الالكتروني ، بحث منشور في مجلة جامعة البعث للعلوم الإنسانية ، جامعة البعث ، سوريا ، المجلد ٤٠ ، العدد ٥٥ ، ٢٠١٨، ص ١٤.

(٤) د. سامح عبد الواحد التهامي ، التعاقد عبر الانترنت ـ دراسة مقارنة ، دار الكتب القانونية ، المحلة الكبرى، مصر ، ٢٠٠٨ ، ص ١٣٤.

(٥) التاجر الالكتروني : كل شخص طبيعي أو معنوي ، سواء أكان عراقياً أم أجنبياً يمارس التجارة الالكترونية على سبيل الاحتراف . المادة (١) من نظام تنظيم التجارة الالكترونية العراقي.

[٦] في المملكة العربية السعودية استخدم مصطلح النظام بدلاً من القانون ، وذلك لخلفية شرعية لأنهم يستمدون نصوصهم القانونية من الكتاب والسنة ، وأن مصطلح قانون هو قادم من الدول الأوروبية و بينها كثير من النصوص المخالفة للشريعة الإسلامية ، مما دفع الكثير من علماء الشريعة في المملكة العربية السعودية إلى الاستغناء عن مصطلح قانون واستبداله بمصطلح نظام وهو ما يصدر من الجهات التشريعية والتنفيذية. للمزيد من المعلومات ينظر في : زياد بن عبد العزيز الطرباق ، قوانين أم أنظمة ، مقال منشور على الموقع الالكتروني الآتي : https://www.aleqt.com تاريخ أخر زيارة : ٦/١٨ / ٢٠٢٥.

[٨] موفر الخدمة : هو التاجر أو الممارس ، والممارس هو الشخص غير المقيد بالسجل التجاري الذي يزاول التجارة الالكترونية. ينظر: الدليل الارشادي للمتاجر الالكترونية السعودي لسنة ٢٠٢٣، ص ٦.

[٩] وسائل التقنية الحديثة : هي أي وسيلة تقنية تستخدم بشأن التجارة من خلال وسائل التقنية الحديثة سواء كانت الكترونية أو رقمية أو بيومترية أو تقنية الذكاء الاصطناعي وتقنيات سلسلة الكتل" البلوك تشين" أو في الأوساط التقنية سواء من خلال الدخول على مواقع الكترونية أو من خلال التطبيقات الذكية . ينظر: في قانون رقم ١٤ لسنة ٢٠٢٣في شأن التجارة من خلال الوسائل التقنية الحديثة الاماراتي ، ص ١.

[١٠] التاجر الرقمي : هو الشخص الطبيعي أو الاعتباري الذي يقوم ببيع السلع أو الخدمات من خلال وسائل التقنية الحديثة. ينظر في ذلك، المصدر السابق ، ص ٢. ولايختلف مصطلح التاجر الرقمي عن الالكتروني ، وذلك من خلال التعريفات المذكورة لهما ، لذلك سنعتمد مصطلح التاجر الالكتروني وفقاً لما ذكر مشرعنا العراقي.

[١١] منى عبد الله السمحان ، متطلبات تحقيق الأمن السيبراني ، بحث منشور في مجلة كلية التربية ، جامعة المنصورة ، مصر، المجلد ١١١، العدد١ ، ٢٠٢٠، ص ٩.

[١٢] د. أحمد عبيس نعمة الفتلاوي ، الهجمات السيبرانية ـ دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط ١ ، منشورات زين الحقوقية ، بيروت ، ٢٠١٨، ص ١٢.

[١٣] م.م أحمد عطا حسين ، وسائل حماية التجارة الإلكترونية من مخاطر الهجمات السيبرانية ، بحث منشور في مجلة واسط للعلوم الانسانية ، جامعة واسط ، المجلد ١٨، العدد ٣، ٢٠٢٢، ص ٦٦٩.

[١٤] الفقرة (٧) من المادة (١) من نظام مكافحة جرائم المعلوماتية السعودي.

[١٥] المادة (١) من قانون مكافحة الشائعات والجرائم الالكترونية الاماراتي .

[١٦] المادة (١) من قرار مجلس الوزراء رقم (١٣) لسنة ٢٠٢٣ بشأن لجنة مكافحة التهديدات السيبرانية والبرمجيات الخبيثة.

[١٧] م.م أحمد عطا حسين ، مصدر سابق ص ٦٧١.

(١٨) د. ريمة مشطوب ود. نورة لخويدر، دور الأمن السيبراني في علاج الإرهاب التجاري ، بحث منشور في مجلة رؤى للدراسات المعرفية والحضارية الجزائر، المجلد ٤ ، العدد١ ، ٢٠١٨، ص ١٤٧ .

(١٩) د. نسرين محسن نعمة الحسيني ود. محمد حسن مرعي ، الجرائم الإلكترونية الواقعة على الأموال، المكتب الجامعي الحديث ، الإسكندرية ، ٢٠٢٠، ص ١٣٣ ـ ١٣٤.

(٢٠) د. عبد الرحمن خليفة الرواس ، أثر التشريعات المتعلقة بحماية البيانات الشخصية على فعالية التجارة الإلكترونية ، ط ١ ، منشورات زين الحقوقية، بيروت ، ٢٠١٩، ص ١٢١ ـ ١٢٢ .

(٢١) هيلين عبد الغني رمضان ، العمليات السيبرانية في ضوء القانون الدولي العام ، دروب المعرفة للنشر والتوزيع ، الإسكندرية ، ٢٠٢٥، ص ٨١.

(٢٢) د. زيد محمد اسماعيل ود. صلاح مهدي هادي الشمري ، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقي ، بحث منشور في مجلة قضايا سياسية ، كلية العلوم السياسية ، جامعة النهرين العدد ٦٢ ، ٢٠٢٠، ص ٢٨٠.

(٢٣) د. علي عبد الخضر محمد المعموري ، آليات الأمن السيبراني ودورها في الحد من الهجمات الإلكترونية على المستوى الدولي، بحث منشور في مجلة ضياء الفكر للبحوث والدراسات ، بيروت ، عدد خاص بمؤتمر بيروت الدولي الثاني ٣٠/ ٤/ ٢٠٢٤ ،ص ٣٤٠ .

(٢٤) د. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة ، ط ١، منشورات زين الحقوقية ، ٢٠١٣، من ص ٥٥٧ الى ٥٦٠.

(٢٥) د. دحان حزام القريطي ، الأمن السيبراني وحماية أمن المعلومات ، ط ١، دار الفكر الجامعي ، الإسكندرية ،٢٠٢١، ص ٦٣.

(٢٦) د. علي جعفر، مصدر سابق ، ص ٥٥٤.

(٢٧) د. حان حزام ناصر، مصدر سابق ، ص ١٤

(٢٨) اللائحة الإطارية للمنصات والخدمات الرقمية العراقية لسنة ٢٠٢٥ ، ص ٦.

(٢٩) المادة (١) من تنظيم الهيئة الوطنية للأمن السيبراني رقم (٦٨٠١) لسنة ١٤٣٩ هـ السعودي .

(٣٠) د. خالد حسن أحمد ، جرائم الإنترنت بين القرصنة الالكترونية وجرائم الابتزاز الالكتروني ـ دراسة مقارنة دار الفكر الجامعي ، الإسكندرية ، ٢٠١٩، ص ٨٨.

(٣١) د. عادل موسى عوض جاب الله ، وسائل حماية الأمن السيبراني ، بحث منشور في مجلة كلية الشريعة والقانون ، جامعة الأزهر، مصر، العدد ٣٤، ٢٠٢٢، ص ٢٢٦٢.

(٣٢) د. فيلالي اسماء ود. شليل عبد اللطيف ، تهديدات أمن المعلومات وسبل التصدي لها، بحث منشور في مجلة البشائر الاقتصادية ، كلية العلوم الاقتصادية والتجارية ، جامعة طاهري محمد ، الجزائر، المجلد٤ ، العدد٣ ، ٢٠١٩ ، ص ١٧٠.

(٣٣) صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني ـ دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير قدمت إلى كلية الآداب والعلوم ، جامعة الشرق الاوسط ، الاردن، ٢٠٢١ ، ص ٦١.

(٣٤) د. محمد فواز المطالقة الوجيز في عقود التجارة الإلكترونية ط ٣ ، دار الثقافة للنشر والتوزيع ، الاردن ،٢٠١١، ص ١٦١.

(٣٥) د. مدحت عبد الحليم رمضان ، الحماية الجنائية للتجارة الالكترونية ، دار النهضة العربية ، القاهرة ،٢٠٠١، ص ٢٢.

(٣٦) د. حسين محمد الغول ، جرائم شبكة الانترنت والمسؤولية الجنائية الناشئة عنها ـ دراسة مقارنة ، مكتبة بدران الحقوقية ، لبنان، ط ١ ، ٢٠١٧، ص ٩٣ .

(٣٧) د. لورنس محمد عبيدات ، إثبات المحرر الإلكتروني ، ط ١ ، دار ثقافة للنشر والتوزيع ، الأردن ، ٢٠٠٩، ص ١٤١.

(٣٨) وتسمى أيضاً بشهادات التوثيق وهي ملفات مشفرة تخزن داخل جهاز خدمة الويب الذي يستخدمه االفرد وتسجل عادة بواسطة طرف ثالث. حيث تتشاور هذه الملفات مع برنامج التصفح الذي يستخدمه المستهلك للتأكد من أن الموقع الذي دخله هو الموقع الصحيح وتستخدم هذه التقنية للتأكد من هوية مستخدمي شبكة الانترنت وتصدرها جهة مرخصة يستخدمها الفرد في تعاملاته الإلكترونية حيث يستوثق من خلالها عن هوية الطرف الأخر وبالتالي تستخدم في ضمان أمن المعاملات الفردية والتجارية .

(٣٩) د. نايف احمد ضاحي الشمري ود.عبد الباسط جاسم محمد ، المفيد في التعاقد والاثبات بالوسائل الالكترونية المعاصرة ، ط١ ، منشورات الحلبي الحقوقية ، بيروت ، ٢٠١٩، ص ٢٤١.

(٤٠) أ. مصطفى يوسف كافي ، التجارة الإلكترونية ، دار رسلان للطباعة والنشر والتوزيع ، دمشق ، ٢٠٠٩، ص ١٦٤ .

(٤١) د. عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والاجنبية ، دار الجامعة الجديدة ، الإسكندرية ، ٢٠٠٩، ص ٦٠.

(٤٢) أ. مصطفى يوسف كافي ، مصدر سابق ، ص ١٦٥.

(٤٣) د. ناصر وسام خليل ، التجارة والتسويق الالكتروني ، ط ١ ، دار أسامة للنشر والتوزيع ، عمان ، الأردن ، ٢٠٠٨، ص ٢٤٤.

(٤٤) أمير فرج يوسف ، الجرائم التجارية الالكترونية وأساليب مكافحتها ، ط ١، مكتبة الوفاء القانونية ، الاسكندرية ، ٢٠١٣، ص ١٥٢ ـ ١٥٣.

(٤٥) امير فرج يوسف ، المصدر نفسه ، ص ١٥٢ـ ١٥٣.

(٤٦) الفقرة (٤) من المادة (٧) من نظام تنظيم التجارة الالكترونية العراقي .

(٤٧) الفقرة (١) من المادة ٤٣٨ من قانون العقوبات العراقي .

(٤٨) المادة (٥) من مشروع قانون مكافحة الجرائم الالكترونية لسنة ٢٠١٩.

(٤٩) المادة (٦) من مشروع قانون مكافحة الجرائم الالكترونية لسنة ٢٠١٩.

(٥٠) المادة (٧) من مشروع قانون مكافحة الجرائم الالكترونية لسنة ٢٠١٩.

(٥١) ينظر في : الفقرة (٢) من المادة (٢) من تنظيم الهيئة الوطنية للأمن السيبراني .

(٥٢) ينظر في : المادة (٣) من تنظيم الهيئة الوطنية للأمن السيبراني.

(٥٣) ينظر في المادة (٤) من تنظيم الهيئة الوطنية للأمن السيبراني.

(٥٤) الفقرة (٣،٥) من المادة (٣) من نظام مكافحة جرائم المعلوماتية السعودي .

(٥٥) الفقرة (٢) من المادة (٤) من نظام مكافحة جرائم المعلوماتية السعودي.

(٥٦) المادة (٥) من نظام مكافحة جرائم المعلوماتية السعودي.

(٥٧) ينظر في الفقرة (١) من المادة (٢) من قرار مجلس الوزراء بشأن لجنة مكافحة التهديدات السيبرانية والبرمجيات الخبيثة.

(٥٨) المادة (٨) من قانون مكافحة الشائعات والجرائم الالكترونية الاماراتي .

(٥٩) المادة (١٥) من قانون مكافحة الشائعات والجرائم الالكترونية الاماراتي.

(٦٠) المادة (٢) من قانون مكافحة الشائعات والجرائم الالكترونية الاماراتي .

(٦١) المادة (١) من الاتفاقية العربية لمكافحة جرئم تقنية المعلومات .

(٦٢) المادة (٦) من الاتفاقية العربية لمكافحة جرئم تقنية المعلومات.

(٦٣) المادة (٨) من الاتفاقية العربية لمكافحة جرئم تقنية المعلومات.

(٦٤) المادة (١٨) من الاتفاقية العربية لمكافحة جرئم تقنية المعلومات.

(٦٥) من الاتفاقية العربية لمكافحة جرئم تقنية المعلومات، ص ١٧.

(٦٦) د. خالد ظاهرعبدالله جابر، مواجهة الجرائم المعلوماتية في ضوء التشريعات الجنائية المعاصرة والاتفاقيات الدولية ، بحث منشور في مجلة البحوث القانونية والاقتصادية ، كلية الحقوق ، جامعة بني سويف ، مصر ، المجلد ٣١، العدد ٢ ، ٢٠١٩، ص ٤٥.

(٦٧) الفقرة (١) من المادة ٢٥ من اتفاقية بودابست.

المصادر

أولاً : الكتب القانونية

١ــ د. أحمد عبيس نعمة الفتلاوي ، الهجمات السيبرانية ــ دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط ١ ، منشورات زين الحقوقية ، بيروت ، ٢٠١٨ .

٢ــ د. أسامة أبو الحسن مجاهد ، التعاقد عبر الانترنت ، دار الكتب القانونية ، مصر، ٢٠٠٥.

٣ــ أمير فرج يوسف ، الجرائم التجارية الالكترونية وأساليب مكافحتها ، ط ١، مكتبة الوفاء القانونية ، الاسكندرية ، ٢٠١٣.

٤ــ د. حسين محمد الغول ، جرائم شبكة الانترنت والمسؤولية الجنائية الناشئة عنها ـ دراسة مقارنة ، مكتبة بدران الحقوقية ، لبنان، ط ١ ، ٢٠١٧ .

٥ــ د. خالد حسن أحمد ، جرائم الإنترنت بين القرصنة الالكترونية وجرائم الابتزاز الالكتروني ـ دراسة مقارنة دار الفكر الجامعي ، الإسكندرية، ٢٠١٩ .

٦ــ د. خالد ممدوح إبراهيم ، إبرام العقد الالكتروني دراسة مقارنة ، ط ١، دار الفكر الجامعي ، الإسكندرية ، ٢٠٠٦.

٧ــ د. دحان حزام القريطي ، الأمن السيبراني وحماية أمن المعلومات ، ط ١، دار الفكر الجامعي ، الإسكندرية ، ٢٠٢١ .

٨ــ د. سامح عبد الواحد التهامي ، التعاقد عبر الانترنت ـ دراسة مقارنة ، دار الكتب القانونية ، المحلة الكبرى، مصر ، ٢٠٠٨.

٩ــ د. عبد الرحمن خليفة الرواس ، أثر التشريعات المتعلقة بحماية البيانات الشخصية على فعالية التجارة الإلكترونية ، ط ١ ، منشورات زين الحقوقية، بيروت ، ٢٠١٩ .

١٠ــ د. عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والاجنبية ، دار الجامعة الجديدة ، الإسكندرية ، ٢٠٠٩ .

١١ــ د. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة ، ط ١، منشورات زين الحقوقية ، ٢٠١٣.

١٢ــ د. لورنس محمد عبيدات ، إثبات المحرر الإلكتروني ، ط ١ ، دار ثقافة للنشر والتوزيع ، الأردن ، ٢٠٠٩.

١٣ــ د. محمد فواز المطالقة الوجيز في عقود التجارة الإلكترونية ط ٣ ، دار الثقافة للنشر والتوزيع ، الأردن ، ٢٠١١ .

١٤ــ د. مدحت عبد الحليم رمضان ، الحماية الجنائية للتجارة الالكترونية ، دار النهضة العربية ، القاهرة ، ٢٠٠١ .

١٥ــ أ. مصطفى يوسف كافي ، التجارة الإلكترونية ، دار رسلان للطباعة والنشر والتوزيع ، دمشق ، ٢٠٠٩.

١٦ــ د. ناصر وسام خليل ، التجارة والتسويق الالكتروني ، ط ١ ، دار أسامة للنشر والتوزيع ، عمان ، الأردن ، ٢٠٠٨.

١٧ــ د. نايف احمد ضاحي الشمري ود.عبد الباسط جاسم محمد ، المفيد في التعاقد والاثبات بالوسائل الالكترونية المعاصرة ، ط١، منشورات الحلبي الحقوقية ، بيروت ، ٢٠١٩ .

١٨ــ د. نسرين محسن نعمة الحسيني ود. محمد حسن مرعي ، الجرائم الإلكترونية الواقعة على الأموال، المكتب الجامعي الحديث ، الإسكندرية ، ٢٠٢٠ .

١٩ــ هيلين عبد الغني رمضان ، العمليات السيبرانية في ضوء القانون الدولي العام ، دروب المعرفة للنشر والتوزيع ، الإسكندرية ، ٢٠٢٥.

ثانياً : الرسائل الجامعية

١ــ صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني ـ دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير قدمت إلى كلية الآداب والعلوم ، جامعة الشرق الاوسط ، الاردن ، ٢٠٢١.

ثالثاً : البحوث القانونية

١ــ م . م أحمد عطا حسين ، وسائل حماية التجارة الإلكترونية من مخاطر الهجمات السيبرانية ، بحث منشور في مجلة واسط للعلوم الانسانية ، جامعة واسط ، المجلد ١٨، العدد ٣، ٢٠٢٢ .

٢ــ حنان مليكة ، المتجر الالكتروني ، بحث منشور في مجلة جامعة البعث للعلوم الإنسانية ، جامعة البعث ، سوريا ، المجلد ٤٠ ، العدد ٥٥ ، ٢٠١٨.

٣ــ د. ريمة مشطوب ود. نورة لخويدر، دور الأمن السيبراني في علاج الإرهاب التجاري ، بحث منشور في مجلة رؤى للدراسات المعرفية والحضارية الجزائر، المجلد ٤ ، العدد ١ ، ٢٠١٨ .

٤ــ د. زيد محمد اسماعيل ود. صلاح مهدي هادي الشمري ، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقي ، بحث منشور في مجلة قضايا سياسية ، كلية العلوم السياسية ، جامعة النهرين العدد ٦٢ ، ٢٠٢٠، ص ٢٨٠.

٦ــ د. عادل موسى عوض جاب الله ، وسائل حماية الأمن السيبراني ، بحث منشور في مجلة كلية الشريعة والقانون ، جامعة الأزهر، مصر، العدد ٣٤، ٢٠٢٢ .

٧ــ د.علي عبد الخضر محمد المعموري ، آليات الأمن السيبراني ودورها في الحد من الهجمات الإلكترونية على المستوى الدولي، بحث منشور في مجلة ضياء الفكر للبحوث والدراسات ، بيروت ، عدد خاص بمؤتمر بيروت الدولي الثاني ٣٠/ ٤/ ٢٠٢٤ .

٨ــ د. فيلالي اسماء ود. شليل عبد اللطيف ، تهديدات أمن المعلومات وسبل التصدي لها، بحث منشور في مجلة البشائر الاقتصادية ، كلية العلوم الاقتصادية والتجارية ، جامعة طاهري محمد ، الجزائر، المجلد ٤ ، العدد ٣ ، ٢٠١٩ .

٩ــ منى عبد الله السمحان ، متطلبات تحقيق الأمن السيبراني ، بحث منشور في مجلة كلية التربية ، جامعة المنصورة ، مصر، المجلد ١١١، العدد١ ، ٢٠٢٠ .

رابعاً : القوانين والأنظمة واللوائح

أ ــ القوانين العراقية

١ ـ قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩.

٢ ـ قانون التجارة العراقي الملغي رقم ١٤٩ لسنة ١٩٧٠.
٣ ـ قانون التجارة العراقي النافذ رقم ٣٠ لسنة ١٩٨٤.
٤ـ مشروع قانون مكافحة الجرائم الالكترونية لسنة ٢٠١٩.
٥ـ نظام تنظيم التجارة الالكترونية رقم ٤ لسنة ٢٠٢٥ .
٦ـ اللائحة الإطارية للمنصات والخدمات الرقمية العراقية لسنة ٢٠٢٥.

ب ــ القوانين السعودية

١ ـ نظام مكافحة جرائم المعلوماتية السعودي رقم ١٧ لسنة ١٤٢٨هـ
٢ ـ نظام التجارة الإلكترونية السعودي رقم ١٢٦ لسنة ١٤٤٠هـ ـ ٢٠١٩م .
٣ ـ الهيئة الوطنية للأمن السيبراني السعودي رقم(٦ ٨ ٠ ١) لسنة ١٤٣٩هـ
٤ ـ الدليل الإرشادي السعودي لسنة ٢٠٢٣.

ج ــ القوانين الإماراتية

١ ـ قانون مكافحة الشائعات والجرائم الإلكترونية الاماراتي رقم ٣٤ لسنة ٢٠٢١
٢ ـ قانون التجارة من خلال وسائل التقنية الحديثة الاماراتي رقم ١٤ سنه ٢٠٢٣
٣ ـ قانون لجنة مكافحة التهديدات السيبرانية والبرمجيات الخبيثة رقم ١٣ لسنة ٢٠٢٣

خامساً : الاتفاقيات الدولية

١ ـ اتفاقية بودابست لمكافحة جرائم المعلوماتية الدولية لسنة ٢٠٠١
٢ ـ الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٠

سادساً : المقالات المنشورة على الانترنت

١ ــ زياد بن عبد العزيز الطرباق ، قوانين أم أنظمة ، مقال منشور على الموقع الالكتروني الآتي : https://www.aleqt.com تاريخ أخر زيارة : ٦/١٨ / ٢٠٢٥.

Sources

First: Legal Books

-١Dr. Ahmed Abis Naama Al-Fatlawi, Cyber Attacks: An Analytical Legal Study on the Challenges of Their Contemporary Regulation, 1st ed., Zain Legal Publications, Beirut, 2018.

-٢Dr. Osama Abu Al-Hassan Mujahid, Online Contracting, Dar Al-Kutub Al-Qanuniyya, Egypt, 2005.

-٣Amir Faraj Youssef, Electronic Commercial Crimes and Methods of Combating Them, 1st ed., Al-Wafaa Legal Library, Alexandria, 2013.

-٤Dr. Hussein Muhammad Al-Ghul, Internet Crimes and the Arising Criminal Liability: A Comparative Study, Badran Legal Library, Lebanon, 1st ed., 2017.

-٥Dr. Khaled Hassan Ahmed, Internet Crimes Between Electronic Piracy and Electronic Extortion: A Comparative Study, Dar Al-Fikr Al-Jami'i, Alexandria, 2019.

-٦Dr. Khaled Mamdouh Ibrahim, Concluding Electronic Contracts: A Comparative Study, 1st ed., Dar Al-Fikr Al-Jami'i, Alexandria, 2006.

.٧Dr. Dahan Hazam Al-Quraiti, Cybersecurity and Information Security Protection, 1st ed., Dar Al-Fikr Al-Jami'i, Alexandria, 2021.

.٨Dr. Sameh Abdel-Wahed Al-Tohamy, Online Contracting: A Comparative Study, Dar Al-Kutub Al-Qanuniyya, Al-Mahalla Al-Kubra, Egypt, 2008.
.٩Dr. Abdel-Rahman Khalifa Al-Rawas, The Impact of Legislation Related to the Protection of Personal Data on the Effectiveness of E-Commerce, 1st ed., Zain Legal Publications, Beirut, 2019.
.١٠Dr. Essam Abdel-Fattah Matar, E-Commerce in Arab and Foreign Legislations, Dar Al-Jami'a Al-Jadeeda, Alexandria, 2009.
.١١Dr. Ali Jaafar, Modern Information Technology Crimes Against Individuals and the Government, 1st ed., Zain Legal Publications, 2013.
.١٢Dr. Lawrence Muhammad Ubaidat, Proof of Electronic Documents, 1st ed., Dar Thaqafa for Publishing and Distribution, Jordan, 2009.
.١٣Dr. Muhammad Fawaz Al-Mutalqa, A Concise Guide to Electronic Commerce Contracts, 3rd ed., Dar Thaqafa for Publishing and Distribution, Jordan, 2011.
.١٤Dr. Medhat Abdel Halim Ramadan, Criminal Protection of Electronic Commerce, Dar Al-Nahda Al-Arabiya, Cairo, 2001.
.١٥Mr. Mustafa Youssef Kafi, Electronic Commerce, Dar Raslan for Printing, Publishing and Distribution, Damascus, 2009.
.١٦Dr. Nasser Wissam Khalil, Electronic Commerce and Marketing, 1st ed., Dar Osama for Publishing and Distribution, Amman, Jordan, 2008.
.١٧Dr. Nayef Ahmed Dhahi Al-Shammari and Dr. Abdul Basit Jassim Muhammad, Useful Guide to Contracting and Proof Using Contemporary Electronic Means, 1st ed., Al-Halabi Legal Publications, Beirut, 2019.
.١٨Dr. Nasreen Mohsen Neama Al-Husseini and Dr. Mohamed Hassan Marai, Cybercrimes Against Funds, Modern University Office, Alexandria, 2020.
.١٩Helen Abdel-Ghani Ramadan, Cyber Operations in Light of Public International Law, Daroub Al-Maarefa for Publishing and Distribution, Alexandria, 2025.

Second: University Theses

.١Salah Haider Abdel-Wahid, Cyber Warfare: A Study of its Concept, Characteristics, and Methods of Confrontation, Master's Thesis submitted to the Faculty of Arts and Sciences, Middle East University, Jordan, 2021.

Third: Legal Research

.١M.M. Ahmed Atta Hussein, Means of Protecting E-Commerce from the Dangers of Cyber Attacks, Research published in Wasit Journal of Human Sciences, Wasit University, Volume 18, Issue 3, 2022. 2. Hanan Malika, "The E-commerce Store," research published in the Al-Baath University Journal of Humanities, Al-Baath University, Syria, Volume 40, Issue 55, 2018.
.٣Dr. Rima Mashtoub and Dr. Noura Lakhwaider, "The Role of Cybersecurity in Combating Commercial Terrorism," research published in the Algerian Journal of Visions for Cognitive and Civilizational Studies, Volume 4, Issue 1, 2018.
.٤Dr. Zaid Muhammad Ismail and Dr. Salah Mahdi Hadi Al-Shammari, "Cybersecurity as a New Pillar in Iraqi Strategy," research published in the Journal of Political Issues, College of Political Science, Al-Nahrain University, Issue 62, 2020, p. 280.
.٦Dr. Adel Moussa Awad Jaballah, "Means of Cybersecurity Protection," research published in the Journal of the Faculty of Sharia and Law, Al-Azhar University, Egypt, Issue 34, 2022. 7. Dr. Ali Abdul Khader Mohammed Al-Maamouri, "Cybersecurity Mechanisms and Their Role in Reducing Cyberattacks at the

International Level," a research paper published in the Diaa Al-Fikr Journal for Research and Studies, Beirut, special issue for the Second Beirut International Conference, April 30, 2024.
.٨Dr. Filali Asma and Dr. Shleel Abdul Latif, "Information Security Threats and Ways to Counter Them," a research paper published in Al-Bashair Economic Journal, Faculty of Economic and Commercial Sciences, Tahri Mohamed University, Algeria, Volume 4, Issue 3, 2019.
.٩Mona Abdullah Al-Samhan, "Requirements for Achieving Cybersecurity," a research paper published in the Journal of the Faculty of Education, Mansoura University, Egypt, Volume 111, Issue 1, 2020.

Fourth: Laws, Regulations, and Bylaws

A. Iraqi Laws
.١Iraqi Penal Code No. (111) of 1969.
.٢The repealed Iraqi Commercial Law No. 149 of 1970.
.٣The current Iraqi Commercial Law No. 30 of 1984.
.٤The draft Cybercrime Law of 2019.
.٥The Electronic Commerce Regulation No. 4 of 2025.
.٦The Framework Regulation for Iraqi Digital Platforms and Services of 2025.

B. Saudi Laws
.١The Saudi Anti-Cybercrime Law No. 17 of 1428 AH (2007/2008(
.٢The Saudi Electronic Commerce Law No. 126 of 1440 AH (2019 CE). 3. Saudi National Cybersecurity Authority No. (6801) of 1439 AH
.٤Saudi Guidance Manual of 2023

C. UAE Laws
.١UAE Anti-Rumors and Cybercrime Law No. 34 of 2021
.٢UAE Trade Through Modern Technology Law No. 14 of 2023
.٣Cyber Threats and Malware Committee Law No. 13 of 2023

Fifth: International Agreements
.١Budapest Convention on Cybercrime of 2001
.٢Arab Convention on Combating Information Technology Crimes of 2010

Sixth: Online Articles
.١Ziyad bin Abdul Aziz Al-Tarbaq, "Laws or Regulations," an article published on the following website: https://www.aleqt.com, last accessed: June 18, 2025.