مجلة مركز بابل للدراسات الإنسانية ٢٠٢٦ المجلد ١٦/ العدد ١١

الحماية القانونية للمنشأة التجارية الإلكترونية من المخاطر السيبرانية
دراسة تحليلية مقارنة في التشريع العراقي

م.م.علي عبد الرزاق مسلم
جامعة القادسية/كلية الفنون الجميلة

البريد الإلكتروني Email : ali.muslim@qu.edu.iq

الكلمات المفتاحية: المنشأة التجارية الإلكترونية، المتجر الإلكتروني، المخاطر السيبرانية، الاختراق، حماية البيانات، المسؤولية المدنية، التأمين السيبراني، النظام رقم (4)لسنة 2025.

كيفية اقتباس البحث
مسلم ، علي عبد الرزاق ، الحماية القانونية للمنشأة التجارية الإلكترونية من المخاطر السيبرانية دراسة تحليلية مقارنة في التشريع العراقي،مجلة مركز بابل للدراسات الانسانية، تشرين الثاني ٢٠٢٦، المجلد:١٦ ،العدد:١١ .

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

Legal Protection of Electronic Commercial Enterprises against Cybersecurity Risks: A Comparative Analytical Study under Iraqi Legislation

Asst. Lect. Ali Abdulrazzaq Muslim
University of Al-Qadisiyah \ College of Fine Art

Keywords : e-business, online store, cyber risks, intrusion, data protection, civil liability, cyber insurance, Iraqi E-Commerce Regulation No. 4 of 2025.

How To Cite This Article
Muslim, Ali Abdulrazzaq, Legal Protection of Electronic Commercial Enterprises against Cybersecurity Risks: A Comparative Analytical Study under Iraqi Legislation,Journal Of Babylon Center For Humanities Studies, November 2026,Volume:16,Issue 11.

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

A growing number of Iraqi merchants trade with no shop at all. What they own is a web address, a customer list, a platform account, a way to take payments and a reputation built slowly from buyer reviews. We treat this bundle as an electronic commercial establishment: an intangible asset that one intrusion can seriously harm. We ask how far Iraqi law protects it against hacking, data theft, ransomware, website outages, impersonation and payment fraud, looking in turn at prevention, criminal sanctions and civil redress, with Egypt and the UAE as points of comparison. Our finding is that Iraqi protection is patchy and borrowed from rules made for other ends. Criminal provisions dating from 1969 struggle with legality and with a notion of property built around physical objects. The long-awaited cybercrime bill had only a first reading in July 2026. The 2025 e-commerce regulation tells merchants to keep customer data safe, yet names no security benchmark and no reporting deadline. Civil liability under the 1951 Civil Code works in principle, although courts still have to settle what the duty of security requires and whether

an attack can ever excuse the business as an outside cause. We recommend legislation that punishes interference with systems and data, fixes minimum safeguards proportionate to the size of the business, sets up incident reporting and rewards firms that insure against cyber loss.

المستخلص

يبيع كثير من التجار العراقيين اليوم من غير محل يستقبلون فيه أحداً؛ فرأس مالهم الحقيقي اسم نطاق، وسجل بأسماء الزبائن، وحساب على منصة، وقناة دفع، وثقة جمعوها تقييماً بعد تقييم . هذا ما نسميه في البحث المنشأة التجارية الإلكترونية، وهو مال معنوي يكفي اختراق واحد لإهدار جانب كبير منه .ونسأل هنا :ما الذي يقدمه القانون العراقي لهذه المنشأة إذا اخترقت أنظمتها، أو سُرقت بياناتها، أو شُفّرت ملفاتها طلباً للفدية، أو عُطّل موقعها، أو انتحل أحدهم اسمها، أو وقعت ضحية احتيال في الدفع؟ تتبعنا الجواب في الوقاية والعقاب والتعويض، وقابلناه بما في القانونين المصري والإماراتي .والنتيجة أن الحماية العراقية متفرقة في نصوص كُتبت لأغراض أخرى .فقانون العقوبات رقم (111)لسنة 1969يتعثر في الاعتداء المعلوماتي عند مبدأ الشرعية وعند فكرة المال المنقول المادي، ومشروع قانون مكافحة جرائم تقنية المعلومات لم يتجاوز قراءته الأولى .وأوجب نظام تنظيم التجارة الإلكترونية رقم (4)لسنة 2025على التاجر صون بيانات زبائنه، لكنه لم يبين درجة الأمن المطلوبة ولا المهلة التي يُبلَّغ فيها عن الخرق .أما القانون المدني رقم (40)لسنة 1951فقواعده في المسؤولية صالحة في أصلها، وتبقى بحاجة إلى اجتهاد يحدد طبيعة التزام المنشأة بالأمن، ويجيب عن سؤال :متى يكون الهجوم السيبراني سبباً أجنبياً؟ ونقترح تشريعاً يجرّم الاعتداء على الأنظمة والبيانات، ويضع حداً أدنى من تدابير الأمن يتفاوت بتفاوت حجم المنشأة، ويرتب الإبلاغ عن الحوادث، ويحفز على التأمين السيبراني.

المقدمة

أولاً :التعريف بموضوع البحث

حين انتقلت التجارة إلى الشبكة ظهرت منشآت لا تكاد تملك شيئاً مما يُرى ويُلمس .قد يدير صاحبها متجراً إلكترونياً أو تطبيقاً أو صفحة على منصة، فلا يفتح باباً للزبائن، ولا يعرفهم إلا أسماءً مخزنة في جهازه، ولا يقبض ثمن بضاعته إلا عبر بوابة دفع .ومع ذلك فلمنشأته قيمة في السوق، تُحسب بعدد عملائها وحجم الإقبال على موقعها ومقدار ما تحظى به من ثقة، وكل ذلك معلق تقريباً على سلامة نظامها المعلوماتي.

ومن هذا التعلق وُلدت مخاطر ما كان التاجر التقليدي يلتفت إليها .أسوأ ما يخشاه صاحب الدكان أن يُسرق أو يحترق .أما صاحب المتجر الإلكتروني فقد يستيقظ ذات صباح ليجد بيانات

زبائنه معروضة للبيع، أو ملفاته مقفلة بتشفير لا يُفك إلا بفدية، أو موقعه عاجزاً تحت سيل من الطلبات المصطنعة، أو موقعاً آخر يحمل اسمه وشعاره ويقبض المال من زبائنه .وقد وصف الفقه الهجمات الإلكترونية بأنها أفعال غير مشروعة يُراد بها الإضرار بالغير عن طريق الوسائل التقنية، ومن صورها الاستيلاء على البيانات واختراق الأنظمة[١].

والمشرع العراقي لم يغب عن المشهد .ففي سنة 2025صدر عن مجلس الوزراء نظام خاص بالتجارة الإلكترونية حمل الرقم (4)، ربط ممارسة هذه التجارة بإجازة، وجعل على التاجر أن يصون ما يجمعه من بيانات زبائنه[٢]. وقبله بعام صدر النظام رقم (2)لسنة 2024الخاص بخدمات الدفع الإلكتروني، وتبعته في العام ذاته ضوابط أصدرها البنك المركزي للصمود السيبراني .على أن هذه النصوص كلها منشغلة بضبط سلوك التاجر وحماية المشتري منه، وقلّما تلتفت إلى المنشأة وهي في موقع المعتدى عليها .أما التجريم الخاص بالعبث بالأنظمة والبيانات فلم يصر قانوناً بعد، وما زال ينتظر دوره في البرلمان.

ثانياً :أهمية البحث

تكمن الأهمية النظرية للموضوع في أن المنشأة التجارية الإلكترونية تقع حيث تلتقي عدة فروع من القانون :التجاري بأحكام المتجر وعناصره، والمدني بقواعد المسؤولية، والجزائي بحمايته للأموال، ثم التشريعات الخاصة بالمعاملات الإلكترونية والدفع والبيانات .ولم نقف على دراسة عراقية نظرت إلى هذه المنشأة من هذه الزاوية كلها معاً، أي بوصفها مالاً معنوياً مستهدفاً؛ فقد ذهب اهتمام الباحثين في الغالب إلى المستهلك في العقد الإلكتروني، أو إلى المسؤولية الجزائية عن الجرائم المعلوماتية على وجه العموم.

وتظهر الأهمية العملية في أن التجارة الإلكترونية تتوسع في العراق أسرع مما يتوسع وعي صغار التجار بأمن المعلومات .فتقع منشآت كثيرة ضحية للاعتداء، ثم يحار أصحابها :أي طريق يسلكون لاسترداد حقهم؟ وكيف يردون مطالبة الزبائن بالتعويض عن تسرب بياناتهم؟ وقد لاحظ بعض الباحثين أن نجاح النظام رقم (4)لسنة 2025رهين بقدرة الجهات المختصة على تطبيقه، وبوجود بنية تقنية وإدارية تكفي لذلك، وأن غياب هذه البنية يُبقي السوق مكشوفة للاحتيال ولخرق بيانات المستهلكين[٣].

ثالثاً :مشكلة البحث

السؤال الذي يدور عليه البحث :إلى أي مدى يحمي القانون العراقي النافذ المنشأة التجارية الإلكترونية من المخاطر السيبرانية، قبل وقوع الاعتداء وبعده؟ وتتولد منه أسئلة أضيق .ما التكييف القانوني لهذه المنشأة، وأي عناصرها يستحق الحماية؟ هل تستطيع نصوص قانون

العقوبات أن تطال الدخول غير المشروع إلى النظام، أو إتلاف البيانات، أو الاستيلاء عليها، من غير أن تخرج على مبدأ الشرعية؟ وماذا سيضيف مشروع قانون مكافحة جرائم تقنية المعلومات إن صدر؟ ثم على أي أساس ترجع المنشأة على من اعتدى عليها، وعلى مزود الخدمة الذي فرّط في التزامه الأمني؟ وأخيراً، ما حالها حين يطالبها زبائنها بالتعويض عن تسرب بياناتهم؟ هل تتمسك بالهجوم بوصفه سبباً أجنبياً، أم يقال لها إنه خطر كان عليها أن تتوقعه وتتحسب له؟

رابعاً :منهجية البحث

سلكنا طريق التحليل :نعرض النص العراقي، ثم نختبره على وقائع الاعتداء كما تحدث في السوق .ولجأنا إلى المقارنة حيث تنفع لا في كل موضع .فمن مصر اخترنا قانون مكافحة جرائم تقنية المعلومات لسنة 2018، وقانون حماية البيانات الشخصية لسنة 2020، وقانون التجارة لسنة 1999. ومن الإمارات اخترنا مرسوم مكافحة الشائعات والجرائم الإلكترونية لسنة 2021، ومرسوم حماية البيانات الشخصية الصادر في السنة ذاتها، وقانون المعاملات التجارية لسنة 2022. لماذا هذان البلدان؟ لأن مصر بنت حمايتها على تشريع جزائي خاص يقترن بواجبات وقائية يتحملها مقدمو الخدمات ومديرو المواقع، ولأن الإمارات أقرت بنص صريح بوجود محل تجاري يمارس نشاطه بالتقنيات الحديثة .الأولى تفيدنا حين نتكلم في العقاب، والثانية حين نتكلم في التكييف.

خامساً :الدراسات السابقة

تعرضت بحوث عراقية حديثة لأطراف من الموضوع دون أن تجمعها .درست مراد والحسناوي الدور الذي تؤديه المسؤولية المدنية في الحد من الهجمات الإلكترونية وأركان هذه المسؤولية،[٤] وتناول جلعوط المسؤولية الجزائية عن الجرائم السيبرانية التي تطال المؤسسات الاقتصادية، ورأى أن قانون العقوبات لا يتسع لها،[٥] وعالجت الحديثي قواعد التأمين من الأخطار الإلكترونية،[٦] وانشغل رعد هاشم أمين بتحديد ماهية المتجر الإلكتروني ومقوماته في ظل النظام رقم (4)لسنة 2025.[٧] أما هذا البحث فيبدأ من المنشأة نفسها، فيعاملها مالاً معنوياً قد يُستهدف، ويتتبع حمايتها وقائياً وجزائياً ومدنياً في سياق واحد .ثم يلتفت إلى الوجه الآخر :حين تُسأل المنشأة أمام زبائنها عن اعتداء كانت هي أول ضحاياه.

سادساً :خطة البحث

وزعنا البحث بعد هذه المقدمة على ثلاثة مباحث .في الأول نحدد مفهوم المنشأة التجارية الإلكترونية والمخاطر السيبرانية التي تحيط بها .وفي الثاني ننظر في حمايتها الوقائية والجزائية . ونفرد الثالث للحماية المدنية ووسائل جبر الضرر .وفي الخاتمة نعرض النتائج والمقترحات.

المبحث الأول: مفهوم المنشأة التجارية الإلكترونية والمخاطر السيبرانية التي تهددها

لا يُحكم على كفاية الحماية التي يقررها القانون لشيء ما قبل أن نعرف هذا الشيء ونعرف ما يتهدده .فنبدأ في مطلب أول بتحديد المنشأة التجارية الإلكترونية وعناصرها، ثم ننتقل في مطلب ثانٍ إلى المخاطر السيبرانية وما تتركه من أثر في مركزها القانوني.

المطلب الأول :مفهوم المنشأة التجارية الإلكترونية

الفرع الأول :تعريف المنشأة التجارية الإلكترونية

تعبير "المنشأة التجارية الإلكترونية "غائب عن التشريع العراقي .الذي نجده في النظام رقم (4) لسنة 2025هو "المتجر الإلكتروني"، ويراد به الأداة الإلكترونية التي يعرض بها التاجر سلعه أو خدماته على الشبكة[٨]. فالنظام نظر إلى المتجر نظرته إلى وسيلة، لا إلى مال .المتجر عنده هو الموقع أو التطبيق أو الصفحة، لا ما يرصده التاجر من أموال لنشاطه .وهذه النظرة تخدم الغرض التنظيمي للنظام، لكنها قاصرة حين نريد أن نبني عليها حماية؛ لأن المعتدي نادراً ما يقصد الواجهة التي يراها الزبون، وإنما يقصد ما خلفها :البيانات، والبرمجيات، والحسابات، والعملاء.

لهذا آثرنا تعبير "المنشأة التجارية الإلكترونية"، وأردنا به ما يخصصه التاجر من أموال مادية ومعنوية لمباشرة تجارته بالوسائل الإلكترونية كلها أو في جزء جوهري منها .وللتعبير أصل في فكرة المتجر كما عرفها القانون التجاري العراقي؛ فقد وصف قانون التجارة رقم (149)لسنة 1970المتجر بأنه »مجموعة من الأموال المنقولة تخصص لمزاولة تجارة معينة«، وأوجب أن يشتمل على عنصري الاتصال بالعملاء والسمعة التجارية[٩]. وبالمعنى ذاته أخذ قانون التجارة المصري رقم (17)لسنة [١٠].1999

وتقدّم المشرع الإماراتي خطوة حين أصدر قانون المعاملات التجارية سنة 2022؛ إذ جعل المحل التجاري مجموع الأموال المادية والمعنوية المرصودة للعمل التجاري، سواء أُدير هذا العمل بالأساليب المعروفة أم من خلال وسائل التقنية الحديثة[١١]. فلم تعد المنشأة الرقمية هناك حالة تحتاج إلى قياس .هي محل تجاري بنص القانون، يُباع ويُرهن ويُحمى من المنافسة غير المشروعة كغيره.

ولا نرى في سكوت المشرع العراقي عن مثل هذا النص مانعاً من الوصول إلى النتيجة نفسها . فالقانون العراقي لم يربط المتجر بمكان، ولم يجعل الأثاث أو البضاعة ركناً فيه، وإنما علّق وجوده على الاتصال بالعملاء والسمعة التجارية .وهذان حاضران في المنشأة الإلكترونية حضوراً قد يكون أوضح منه في الدكان؛ فعملاؤها مقيدون بأسمائهم وعناوينهم، وسمعتها مقروءة في تقييمات منشورة .وإلى قريب من ذلك ذهب جانب من الفقه العراقي حين قرر أن للمتجر الإلكتروني عناصر مادية ومعنوية تفترق بعض الشيء عن عناصر المتجر التقليدي، وأن هذا الافتراق يقتضي قواعد تلائمه[١٢].

الفرع الثاني :عناصر المنشأة التجارية الإلكترونية

يعرف القانون التجاري للمتجر عناصر مادية كالبضائع والمعدات، وعناصر معنوية كالاسم التجاري والعلامة والاتصال بالعملاء .والمنشأة الإلكترونية تحتفظ بهذه كلها تقريباً، ثم تضيف إليها ما لم يكن في حسبان من كتب قانون التجارة .ونقف عند أهم هذه الإضافات.

اسم النطاق. به يصل الزبون إلى المتجر، فهو في الفضاء الرقمي بمنزلة العنوان التجاري واللافتة في السوق .وقد تنبهت ضوابط وزارة التجارة رقم (3)لسنة 2025لقيمته، فجعلت من شروط تسجيل التاجر الإلكتروني أن يكون اسم تطبيقه أو صفحته داخل النطاق العراقي (IQ).[١٣] ويجري تشغيل هذا النطاق تحت إشراف هيأة الإعلام والاتصالات[١٤].

سجل العملاء. هو الوجه الرقمي لعنصر الاتصال بالعملاء، وهو في الغالب أثمن ما تملكه المنشأة .لكنه عنصر ذو وجهين .فهو مال يدخل في ذمة المنشأة، وهو في الوقت ذاته بيانات شخصية لأصحابها، محمية لمصلحتهم هم .ومن هنا تنشأ المفارقة التي نعود إليها في المبحث الثالث :إذا سُرق هذا السجل صارت المنشأة ضحية ومسؤولة في لحظة واحدة.

البرمجيات والأنظمة. منصة المتجر، ونظام الطلبات، وبرنامج المخزون .قد تملكها المنشأة، وقد تستعملها بترخيص، وقد تكون مستضافة عند مزود خارجي .وليس هذا التفريق ترفاً نظرياً، فعليه يتوقف السؤال عمن يتحمل تبعة الثغرة حين يقع الاختراق.

الحسابات على المنصات. كثير من المنشآت الصغيرة في العراق لا موقع لها أصلاً، وتقوم تجارتها كلها على صفحة في منصة تواصل .صحيح أن المنصة تملك إغلاق الحساب متى شاءت وفق شروطها، لكن هذه الصفحة هي في الواقع مجمع العملاء وسجل السمعة، وضياعها باختراق أو انتحال يساوي إغلاق الدكان.

السمعة الرقمية. سمعة المنشأة على الشبكة لها أرقام :نجوم، وتعليقات، ومتابعون .ويكفي أن يُنشر خبر عن تسريب بيانات الزبائن حتى يتبدد جزء كبير منها .وهذا ضرر يعسر تقديره بالنقود، لكنه قائم، ويندرج تحت ما فات المنشأة من كسب.

ونخلص من ذلك إلى أن العناصر المعنوية في المنشأة الإلكترونية ليست تابعة لغيرها، بل هي قلبها، وأن أكثرها يقوم على بيانات .فحماية المنشأة من المخاطر السيبرانية هي، في حقيقة الأمر، حماية لهذه العناصر.

المطلب الثاني :المخاطر السيبرانية التي تتعرض لها المنشأة التجارية الإلكترونية

الفرع الأول :مفهوم الخطر السيبراني

الخطر السيبراني في معناه الذي نعتمده هو إمكان وقوع حادث ينال من سرية ما تحوزه المنشأة من معلومات، أو من صحتها، أو من قدرة أصحاب الحق على بلوغها .قد يقف وراءه مخترق يتعمد الإيذاء، وقد ينتج عن إهمال عامل في المنشأة، وقد لا يكون أكثر من خلل فني .وتنعكس خصائصه على طريقة معالجته في القانون :فالفاعل كثيراً ما يبقى بلا اسم أو يقيم خارج البلاد، والأذى يتسع ليشمل الزبائن والموردين، والحوادث تتكرر حتى صارت جزءاً معتاداً من العمل على الشبكة، فيصعب أن يقال عن أي منها إنه لم يكن في الحسبان.

وقد عكست ضوابط الصمود السيبراني الصادرة عن البنك المركزي العراقي هذا الفهم، فانتقلت من هدف منع الحادث إلى هدف "الصمود"، أي أن تبقى المؤسسة قادرة على العمل وأن تتعافى بعد وقوعه[١٥]. ولهذا التحول أثر قانوني لا يستهان به .فإذا كان الحادث السيبراني متوقعاً بطبيعته، فلا يُطلب من المنشأة أن تمنعه منعاً مطلقاً، وإنما يُطلب منها ما يفعله التاجر الحريص :أن تقلل احتماله وأن تحد من أثره.

الفرع الثاني :صور المخاطر السيبرانية

صور الخطر التي تواجه المنشأة التجارية الإلكترونية كثيرة، وأبرزها ما يأتي.

الدخول غير المشروع وسرقة البيانات. وهي الصورة الأكثر تكراراً :يتسلل المعتدي إلى نظام المنشأة بلا إذن، ليطلع على بيانات الزبائن أو ينسخها أو يبيعها .وأخطر ما فيها أن المنشأة قد لا تنتبه إليها إلا بعد أشهر.

برمجيات الفدية. يشفّر المعتدي بيانات المنشأة أو أنظمتها، ثم يساومها على مفتاح فك التشفير، وكثيراً ما يهددها بنشر البيانات إن رفضت الدفع .وهذه الصورة تطرح أسئلة لم تُحسم :هل يجوز الدفع أصلاً؟ وهل تلتزم المنشأة بإخبار زبائنها؟

الحرمان من الخدمة. يُغرق الموقع بطلبات كثيفة تصدر عن أجهزة كثيرة، فيعجز عن خدمة الزبائن الحقيقيين وتتوقف المبيعات طوال الهجوم .وقد يلجأ إلى ذلك منافس يريد إقصاء المنشأة في موسم الذروة.

الانتحال والتصيد. يُنشأ موقع أو صفحة تحاكي المنشأة في اسمها وشعارها، ليدفع إليها الزبائن أموالهم أو يدخلوا فيها بياناتهم المصرفية .فتخسر المنشأة عملاءها وتتلطخ سمعتها معاً.

الاحتيال في الدفع. يشتري شخص من المتجر مستعملاً بطاقة ليست له، فتُسلَّم البضاعة، ثم يعترض صاحب البطاقة الحقيقي لدى مصرفه، فيُسحب المبلغ من حساب المنشأة وقد خسرت البضاعة وثمنها معاً .ويلاحظ الفقه أن السطو على البيانات المصرفية يضع مستعملي الدفع الإلكتروني أمام مخاطر متنوعة، استراتيجية وتشغيلية وتقنية، وأن الحلول الفنية لا تكفي لمواجهتها ما لم يسندها التشريع(١٦).

الخطر من الداخل. ليس كل معتدٍ غريباً .قد يكون العامل في المنشأة هو من يبيع قائمة الزبائن لمنافس، أو من يستغل صلاحياته لتحويل مبالغ إلى حسابه، أو من يترك بإهماله الباب مفتوحاً للمخترق .ولهذا أثره حين نبحث مسؤولية المنشأة، فهي تُسأل عما يرتكبه تابعوها.

الفرع الثالث :أثر المخاطر السيبرانية في مركز المنشأة القانوني

يضع الخطر السيبراني المنشأة في مركز مركب .هي من ناحية مجني عليها، لها أن تطلب عقاب المعتدي، وأن تطالبه بما خسرت وما فاتها من كسب، وأن ترجع على مزود الخدمة إن قصّر في واجبه الأمني .وهي من ناحية أخرى مدينة :عليها لزبائنها أن تحفظ بياناتهم، وعليها للجهات الرقابية أن تمتثل لمتطلبات الأمن .فقد تجد نفسها مطالبة بالتعويض بسبب اعتداء وقع عليها هي.

وقد فرّق الفقه في المسؤولية المدنية عن الهجمات الإلكترونية بين حالتين :مسؤولية عقدية تنشأ حين يخل أحد المتعاقدين بما التزم به من حماية البيانات والأنظمة، ومسؤولية تقصيرية تقوم على الواجب العام بعدم الإضرار بالغير ولو لم يجمع الطرفين عقد(١٧). والتفريق نفسه يصدق على المنشأة في وجهيها؛ فعلاقتها بالمعتدي تقصيرية، وعلاقتها بمزود الخدمة وبالزبون عقدية في الأغلب .ولن تكتمل الحماية ما لم يُعالج الوجهان كلاهما، وهذا ما نحاوله في المبحثين التاليين.

المبحث الثاني: الحماية الوقائية والجزائية للمنشأة التجارية الإلكترونية

تبدأ حماية المنشأة قبل أن يقع الاعتداء، بما يفرضه القانون عليها وعلى من يتعامل معها من تدابير أمن، ولا تنتهي بعد وقوعه إلا بعقاب المعتدي .وعلى هذا نعالج الحماية الوقائية في مطلب أول، والحماية الجزائية في مطلب ثانٍ.

المطلب الأول :الحماية الوقائية للمنشأة التجارية الإلكترونية

الفرع الأول :التزامات الأمن في التشريع العراقي

الحماية الوقائية هي تلك القواعد التي تفرض تدابير تخفض احتمال وقوع الحادث السيبراني أو تحصر أثره .وأول ما يلفت النظر أن العراق لا يملك قانوناً عاماً للأمن السيبراني يحدد ما يجب على المنشآت في حده الأدنى، وأن هذه الواجبات موزعة على نصوص قطاعية لا يجمعها رابط. ففي التجارة الإلكترونية أوجب النظام رقم (4)لسنة 2025على التاجر أن يعتمد أنظمة آمنة لصون البيانات الشخصية لزبائنه، وألا يجمع منها إلا ما تدعو إليه الحاجة، وأن يحصل على موافقة صريحة قبل أن يستعملها أو يشاركها، وأن يبادر إلى إخطار الزبائن المتضررين والجهات المختصة إذا تعرضت البيانات للخرق[١٨]. وهذا يُحمد للنظام، فهو أول نص عراقي يُلزم التاجر صراحة بالإبلاغ عن الخرق .لكن العبارات جاءت فضفاضة .فما الأنظمة الآمنة؟ وبأي معيار نحكم بأن التدابير كافية؟ وخلال كم يوماً يجب الإبلاغ؟ وإلى من بالتحديد؟ لا جواب في النص . وقد سجّل بعض الباحثين غياب المعايير الأمنية الواضحة ومواعيد الإخطار عن الخرق في النظام[١٩].

وفي الدفع الإلكتروني، أخضع نظام خدمات الدفع الإلكتروني للأموال رقم (2)لسنة 2024 مقدمي خدمات الدفع لترخيص البنك المركزي ورقابته،[٢٠] ثم جاءت ضوابط الصمود السيبراني لتخاطب المؤسسات المالية والمصرفية .تنتفع المنشأة التجارية من هذه الضوابط بصورة غير مباشرة، لأن بوابة الدفع التي تستعملها ملزمة بها .أما هي نفسها فلا تخاطبها الضوابط بشيء.

ثم دخلت هيأة الإعلام والاتصالات على الخط، فأصدرت في شباط 2025إطاراً تنظيمياً للخدمات والمنصات الرقمية، عدّت فيه منصات التجارة الإلكترونية صراحة من المخاطبين بأحكامه، وألزمت مقدمي هذه الخدمات بالأخذ بالمعايير الدولية المعتمدة في أمن المعلومات وحماية البيانات[٢١]. ويطرح هذا أمرين لم يُحسما .الأول سند الهيأة في تكليف منشآت تجارية لا تشغّل شبكات اتصال .والثاني العلاقة بين ما تفرضه الهيأة وما تفرضه وزارة التجارة، وهي الجهة التي أناط بها النظام رقم (4)لسنة 2025منح الإجازة والرقابة.

الحصيلة أن على المنشأة واجبات أمنية تأتيها من أكثر من جهة، دون أن يدلها أي نص على ما يجب عليها أن تفعله بالضبط .وهذا الغموض يصيبها مرتين .فهي لا تعرف الحد الذي إن

بلغته أمنت المساءلة .والقاضي الذي ينظر دعوى زبون متضرر لن يجد مقياساً يزن به سلوكها، فيعود إلى معيار الشخص المعتاد بكل ما فيه من اتساع.

الفرع الثاني :حماية الاسم التجاري واسم النطاق

الاسم التجاري المسجل محمي في القانون العراقي، فلا يجوز لغير صاحبه أن يتخذه في النشاط ذاته، غير أن الحماية لا تتجاوز حدود المحافظة أو المحافظات التي سُجل فيها[٢٢]. قيد كهذا كان له ما يبرره يوم كانت المتاجر لا تبيع إلا لأهل مدينتها .أما اليوم فمتجر مسجل في الحلة قد يوصل بضاعته إلى البصرة وأربيل في اليوم نفسه، ومن يسرق اسمه قد يدير صفحته من محافظة أخرى أو من بلد آخر، ثم يقول إن الحماية لا تشمله.

لذلك تظل العلامة التجارية المسجلة أوسع مدى من الاسم التجاري، لأن حمايتها تشمل العراق كله، ويمكن الاستناد إليها في وجه من يسجل اسم نطاق يطابقها أو يشبهها ليضلل الجمهور . وأما منازعات أسماء النطاق نفسها، فتُحل في النطاقات العامة وفق السياسة الموحدة لتسوية منازعات أسماء النطاق، ويُترك النطاق العراقي لما تضعه جهة تشغيل السجل من سياسات، مع بقاء القضاء مفتوحاً للمتنازعين[٢٣]. وفي رأينا أن الضوابط رقم (3)لسنة 2025حين اشترطت التسجيل داخل النطاق العراقي فقد أوجبت ضمناً أن يُنظم تسجيل هذه الأسماء والفصل في منازعاتها بقواعد واضحة؛ فاسم النطاق صار شرطاً لمزاولة النشاط، والاعتداء عليه صار اعتداءً على وجود المنشأة ذاته.

الفرع الثالث :الحماية الوقائية في التشريعين المصري والإماراتي

اعتمد المشرع المصري في باب الوقاية على قانونين يكمل أحدهما الآخر .ففي قانون جرائم تقنية المعلومات لسنة 2018فرض على مقدم الخدمة أن يحتفظ بسجلات نظامه نصف عام تقريباً، وأن يحفظ البيانات ويؤمّنها من التسرب[٢٤]. وذهب أبعد من ذلك، فجعل مدير الموقع أو الحساب أو النظام مسؤولاً جزائياً إذا قصّر في احتياطات التأمين فانكشف نظامه لجريمة من الجرائم التي نص عليها،[٢٥] وجعل من يدير الشخص الاعتباري فعلياً مسؤولاً إذا سكت عن جريمة وقعت على نظام منشأته ولم يُعلم بها السلطات[٢٦]. ثم جاء قانون البيانات الشخصية لسنة 2020فطلب من المتحكم أن يأخذ بالوسائل الفنية والتنظيمية التي تكفل أمن البيانات،[٢٧] وحدد له مهلة ثلاثة أيام لإعلام مركز حماية البيانات بأي خرق، تليها ثلاثة أيام عمل لإعلام صاحب البيانات[٢٨].

والتجربة الإماراتية قريبة من المصرية في هذا الباب .فقانون البيانات الشخصية الإماراتي لسنة 2021يطلب ممن يتحكم في البيانات أو يعالجها أن يتخذ من الوسائل الفنية والإدارية ما

يتناسب مع جسامة الخطر، كالتشفير، والمحافظة على سرية الأنظمة واستمرار تشغيلها، وتهيئة القدرة على استعادة البيانات بعد الأعطال[٢٩]. ويلزم المتحكم بأن يُعلم الجهة المختصة بكل اختراق، ويشرح لها ماهيته وأسبابه وعواقبه المحتملة وما قام به لاحتوائه، وأن يُعلم صاحب البيانات متى كان الاختراق يمس خصوصيته[٣٠]. وجاء قانون التجارة عبر التقنيات الحديثة لسنة 2023فأعاد التأكيد على مسؤولية التاجر الرقمي عن حفظ بيانات من يتعامل معه من المستهلكين[٣١].

ما الذي تكشفه هذه المقارنة؟ أن التشريع العراقي لا يفتقر إلى مبدأ الالتزام بالأمن، فالنظام رقم (4)لسنة 2025قرره، وإنما يفتقر إلى ما يجعله قابلاً للتطبيق :معيار للتدابير يتدرج بحجم المنشأة ونوع البيانات، ومهلة محددة للإبلاغ، وجهة معروفة يُبلَّغ إليها، وجزاء عند المخالفة . ويستوقفنا في التجربة المصرية أنها ألزمت المنشأة الضحية نفسها بالإبلاغ .والحكمة من ذلك ظاهرة؛ فالهجوم على منشأة واحدة كثيراً ما يكون حلقة في حملة أوسع، وسكوت الضحية حرصاً على سمعتها يحجب عن السلطات معلومات كان يمكن أن تحمي بها منشآت أخرى.

المطلب الثاني :الحماية الجزائية للمنشأة التجارية الإلكترونية

الفرع الأول :مدى كفاية قانون العقوبات العراقي

لا جريمة ولا عقوبة إلا بنص، ولا قياس في التجريم[٣٢]. وهذه القاعدة هي أول ما يعترض حماية المنشأة الإلكترونية بنصوص كُتبت سنة 1969لحماية أموال تُرى وتُلمس .ويتضح ذلك إذا مررنا على أبرز صور الاعتداء.

سرقة البيانات. نص القانون العراقي على أن السرقة »اختلاس مال منقول مملوك لغير الجاني عمداً[٣٣].« ولو أردنا أن نطبق هذا على من ينسخ قاعدة بيانات المنشأة لاصطدمنا بعقبتين . أولاهما أن البيانات لا تدخل بسهولة في فكرة المال المنقول كما تصورها المشرع، أي الشيء المادي الذي يُنقل من مكان إلى آخر .والثانية أن الاختلاس معناه انتزاع الشيء من حيازة مالكه، والناسخ لا ينتزع شيئاً؛ فالقاعدة تبقى في أجهزة المنشأة كاملة .والنتيجة مفارقة :من يسرق من المتجر صندوقاً من البضاعة سارق، ومن يستنسخ بيانات آلاف الزبائن ويبيعها قد لا يكون كذلك.

الاحتيال بالوسائل الإلكترونية. يعاقب القانون العراقي من يتوصل إلى تسلم مال منقول مملوك للغير أو نقل حيازته، مستعملاً طرقاً احتيالية أو متخذاً اسماً كاذباً أو صفة غير صحيحة[٣٤]. هذا أقرب النصوص التقليدية إلى ما يقع على المنشأة الإلكترونية .فمن ينتحل اسم المتجر ويجعل زبائنه يدفعون إليه قد اتخذ صفة غير صحيحة وتسلم بها المال .إلا أن النص يفترض

إنساناً مخدوعاً يسلّم ماله بإرادة معيبة .فماذا لو لم يُخدع أحد، وإنما عبث الجاني ببيانات الدفع حتى قبل النظام الآلي عملية لم يأذن بها صاحب الحساب؟ هنا يدخل الشك.

إتلاف البيانات وتعطيل الأنظمة. يعاقب القانون العراقي على إتلاف أموال الغير المنقولة،[٣٥] لكن محو البيانات، أو تشفيرها ببرمجية فدية، أو إسقاط الموقع بهجوم حرمان من الخدمة، لا يُتلف شيئاً مادياً .الأجهزة سليمة، والبيانات قد تعود، والموقع يرجع إلى العمل حين يتوقف الهجوم .وإدخال هذه الأفعال في الإتلاف يحتاج إلى توسع في التفسير لا يسمح به مبدأ الشرعية.

تسريب الأسرار من الداخل. يعاقب القانون العراقي من علم بسر بحكم وظيفته أو صناعته أو فنه أو طبيعة عمله فأفشاه في غير الأحوال التي يجيزها القانون[٣٦]. وهذا نص يصلح للموظف الذي يسرّب قاعدة البيانات أو الأسرار التجارية للمنشأة، وهو من المواضع القليلة التي يسعف فيها القانون القديم دون تأويل.

الحاصل أن حماية المنشأة في قانون العقوبات حماية عرجاء .تستقيم إذا جاء الاعتداء في هيئة مألوفة للمشرع القديم، كالاحتيال أو كشف السر، وتتعثر إذا قصد المعتدي النظام نفسه أو ما فيه من بيانات .ولم يبتعد جلعوط عن هذا، إذ قرر قصور النصوص القائمة عن ملاحقة الجرائم السيبرانية التي تصيب المؤسسات الاقتصادية، ونبّه إلى ما يصاحبها من عسر في الإثبات، وغموض في شخص الفاعل، وتزاحم في الاختصاص[٣٧]. وفي إقليم كوردستان صدر سنة 2008قانون يمنع إساءة استعمال أجهزة الاتصالات، لكنه محصور بحدود الإقليم، ومعظم أحكامه موجه إلى التهديد والإساءة عبر الهاتف والشبكة، لا إلى اقتحام الأنظمة والعبث بالبيانات.

وقد يقال إن العراق ملزم بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي أُبرمت في القاهرة سنة 2010، وإنها توجب على أطرافها تجريم النفاذ غير المشروع والمساس بسلامة البيانات والاحتيال عبر التقنية[٣٨]. وهذا صحيح، لكنه لا يحل المشكلة .الاتفاقية تخاطب الدولة وتطلب منها أن تشرّع، ولا تحدد عقوبة يمكن أن يحكم بها القاضي، ومبدأ الشرعية يأبى أن يُدان شخص من غير نص وطني يسمي الفعل ويقدّر جزاءه.

الفرع الثاني :مشروع قانون مكافحة جرائم تقنية المعلومات

أكثر من عشر سنين ومشروع قانون الجرائم المعلوماتية يدخل مجلس النواب ويخرج منه، يُسحب كل مرة تحت وطأة الانتقادات الموجهة إلى نصوصه الماسة بحرية التعبير .وفي 6/7/2026 أنجز المجلس القراءة الأولى لمشروع قانون مكافحة جرائم تقنية المعلومات، وسط اعتراض

منظمات مدنية رأت فيه صياغات مبهمة وعقوبات مغلظة قد تطال حرية التعبير والصحافة الاستقصائية[٣٩].

هذا الجدل مشروع، لكنه غطى على حاجة لا يكاد يختلف فيها أحد :تجريم الاعتداء على سلامة الأنظمة والبيانات .المنشأة التي اختُرق نظامها أو شُفّرت ملفاتها لا يعنيها ما في المشروع من أحكام النشر والإساءة .ما يعنيها نصوص محددة تعاقب على الدخول غير المشروع، واعتراض البيانات، وإتلافها أو تعديلها، وتعطيل الأنظمة، والاحتيال المعلوماتي، والاستيلاء على بيانات وسائل الدفع .هذه هي النواة المشتركة في التشريعات المقارنة وفي الاتفاقيات الدولية، ومنها اتفاقية بودابست بشأن الجرائم الإلكترونية[٤٠]. لذلك نقترح، إذا تعذر الاتفاق على المشروع كله، أن تُستل منه نصوص حماية الأنظمة والبيانات وتُشرّع مستقلة وأولاً، فكل تأخير فيها يترك المنشآت الاقتصادية بلا غطاء جزائي حقيقي.

الفرع الثالث :الحماية الجزائية في التشريعين المصري والإماراتي

يحوي القانون المصري لسنة 2018عدداً من النصوص التي تصيب ما يقع على المنشأة التجارية الإلكترونية .فهناك تجريم للنفاذ إلى موقع أو حساب أو نظام بغير حق، سواء أكان الدخول مقصوداً من البداية أم جاء عرضاً ثم استمر صاحبه فيه، مع عقوبة أشد إذا ترتب على ذلك محو شيء من البيانات أو تبديله أو نسخه[٤١]. وهناك عقاب لمن يتعدى الصلاحية الممنوحة له في الدخول،[٤٢] ولمن يلتقط البيانات أثناء انتقالها في الشبكة،[٤٣] ولمن يعبث بالبيانات أو الأنظمة فيعطلها أو يغير مسارها أو يمحوها[٤٤]. ويعاقب القانون من يعتدي على بريد إلكتروني أو موقع أو حساب، ويرفع العقوبة إذا كان صاحبه شخصاً اعتبارياً من أشخاص القانون الخاص،[٤٥] ومن يوقف الشبكة المعلوماتية عن العمل،[٤٦] ومن يصل بلا حق إلى أرقام بطاقات المصارف ووسائل الدفع أو يستعملها[٤٧]. ويُسأل الشخص الاعتباري نفسه إذا وقعت الجريمة لحسابه أو باسمه[٤٨].

أما المرسوم بقانون الإماراتي رقم (34)لسنة 2021فأقرب إلى حاجات المنشأة التجارية .فإلى جانب تجريم الاختراق،[٤٩] والإضرار بالمواقع والأنظمة المعلوماتية أو تعطيلها،[٥٠] أفرد نصاً مستقلاً للحصول على البيانات والمعلومات السرية للمنشآت المالية أو التجارية أو الاقتصادية أو تعديلها أو إفشائها،[٥١] وجرّم الحصول بلا تصريح على الرموز السرية وكلمات المرور،[٥٢] واصطناع المواقع والحسابات الزائفة المنسوبة زوراً إلى غير أصحابها،[٥٣] والاستيلاء على بيانات وسائل الدفع الإلكتروني،[٥٤] والاحتيال الإلكتروني للاستيلاء على مال الغير[٥٥].

نستنتج من هذا أن التشريعين لم يكتفيا بحماية الفرد في بياناته، بل حميا المنشأة ذاتها في نظامها وأسرارها وحساباتها .فالقانون المصري رفع العقوبة حين يكون الموقع أو الحساب المعتدى عليه لشركة أو منشأة خاصة، والقانون الإماراتي أفرد لأسرار المنشآت التجارية نصاً، وعاقب على اصطناع المواقع المزيفة صراحة، فأغنى القاضي عن تطويع نصوص الاحتيال القديمة .وأمام المشرع العراقي نماذج جاهزة يستطيع أن يفيد منها، على أن يراعي تناسب العقوبة مع الفعل، وأن يضبط العبارة حتى لا تتسع لملاحقة الرأي.

المبحث الثالث: الحماية المدنية للمنشأة التجارية الإلكترونية وآليات جبر الضرر السيبراني

عقاب المعتدي لا يعيد إلى المنشأة ما خسرته .ما يهمها في الغالب أن يُجبر ضررها، وأن تعود إلى العمل، وأن تدفع عنها مطالبات الآخرين .ولهذا نقسم المبحث على ثلاثة مطالب :رجوع المنشأة على المسؤولين عن الضرر، ثم مسؤوليتها هي أمام زبائنها، ثم التأمين من المخاطر السيبرانية.

المطلب الأول :رجوع المنشأة على المسؤولين عن الضرر السيبراني

الفرع الأول :مسؤولية المعتدي

يُسأل من اعتدى على نظام المنشأة أو بياناتها مسؤولية تقصيرية، فالقانون المدني العراقي يقرر أن »كل تعدٍّ يصيب الغير بأي ضرر آخر غير ما ذكر في المواد السابقة يستوجب التعويض[٥٦].« وسعة هذه القاعدة هي مصدر قوتها .فهي لا تشترط أن يكون الفعل جريمة، ولا تخضع لمبدأ الشرعية الجزائية .ومؤدى ذلك أن من ينسخ قاعدة البيانات، فيفلت من العقاب لعدم وجود نص يطاله، يبقى مسؤولاً مدنياً ما دام فعله قد وقع بغير حق وأضر بالمنشأة .وفي هذا تتقدم الحماية المدنية على الجزائية في ظل التشريع العراقي كما هو اليوم.

ويغطي التعويض ما خسرته المنشأة وما فاتها من كسب، بشرط أن يكون ذلك نتيجة طبيعية للفعل غير المشروع[٥٧]. فمن الخسارة نفقات فحص النظام واسترجاع البيانات وسد الثغرات وتعويض الزبائن .ومن الكسب الفائت ما ضاع من مبيعات مدة التوقف، وما انصرف من عملاء بعد الحادث .ويدخل في التعويض أيضاً الضرر الأدبي،[٥٨] وهو متصور في المساس بسمعة المنشأة .وإذا تعدد المعتدون، فاخترق أحدهم النظام، وباع الثاني البيانات، واشتراها منافس يعلم مصدرها، كانوا جميعاً متضامنين في التعويض[٥٩].

ولا تقوم هذه المسؤولية إلا بأركانها المعروفة :الخطأ أو التعدي، والضرر، وعلاقة السببية بينهما. وقد بيّن الفقه أن الضرر في الهجمات الإلكترونية يجب أن يكون محققاً، وأن الخطأ فيها درجات بين العمد والإهمال، وأن السببية يجب أن تكون مباشرة[٦٠]. على أن العقدة الحقيقية ليست في

التكييف، بل في معرفة من فعل .المعتدي يخفي نفسه، ويعمل في الغالب من وراء الحدود، فتبقى الدعوى عليه حقاً على الورق في حالات كثيرة .ومن هنا تبحث المنشأة عن مدين آخر يمكن الوصول إليه، أو عن طريق يجبر الضرر دون حاجة إلى معرفة الفاعل، كالتأمين.

الفرع الثاني :مسؤولية مزودي الخدمات المتعاقدين مع المنشأة

لا تعمل المنشأة الإلكترونية وحدها .هناك مزود استضافة يحفظ موقعها وبياناتها، ومزود منصة يقوم عليها متجرها، ومقدم خدمة دفع يعالج مدفوعات زبائنها، وربما شركة متخصصة في الأمن . فإذا جاء الاختراق من ثغرة في نظام أحد هؤلاء، رجعت عليه المنشأة بالمسؤولية العقدية.

والمدين في العقد إذا لم يعد التنفيذ العيني ممكناً حُكم عليه بالتعويض، إلا أن يثبت أن السبب في ذلك أمر خارج عنه لا يد له فيه[٦١]. ويتوقف نطاق مسؤولية المزود على نوع ما التزم به في شأن الأمن .فإذا كان التزامه وسيلة يبذل فيها جهده، فيكفيه أن يبذل ما يبذله الشخص المعتاد،[٦٢] ويقع على المنشأة إثبات أنه لم يفعل .وإذا تعهد بنتيجة محددة، كأن يضمن بقاء الموقع يعمل في أغلب ساعات الشهر، قامت مسؤوليته بمجرد ألا تتحقق هذه النتيجة .ونرجح أن حفظ البيانات في عقود الخدمات التقنية من قبيل الالتزام بالوسيلة، على أن يُقاس جهد المزود بجهد المختص في مهنته، لأن المنشأة ما تعاقدت معه إلا لأنه يعرف ما لا تعرف.

والعقبة العملية أن عقود المزودين تُكتب سلفاً، وتتضمن عادة بنوداً تحصر التعويض في رسوم شهر واحد، أو تستبعد الخسائر غير المباشرة والأرباح الضائعة .والقانون المدني العراقي يسمح بالاتفاق على إعفاء المدين من تبعة إخلاله بالعقد، لكنه يستثني الغش والخطأ الجسيم[٦٣]. فالبنود صحيحة ما لم تثبت المنشأة أن الاختراق يعود إلى خطأ جسيم من المزود، كأن يُهمل سد ثغرة شاع أمرها ونُبّه إليها، أو يخزن كلمات المرور كما هي دون تشفير .ويبقى للمنشأة كذلك أن تحتج بقواعد عقد الإذعان إن لم يُترك لها مجال لمناقشة تلك البنود[٦٤].

وتُسأل المنشأة كذلك عن تابعيها .فالقانون المدني العراقي يجعل من يستغل مؤسسة تجارية مسؤولاً عن الضرر الذي يحدثه مستخدموه أثناء قيامهم بخدماتهم، ويسمح له بالتخلص من المسؤولية إذا أثبت أنه بذل ما ينبغي من العناية لمنع الضرر[٦٥]. ولهذا النص وجهان في موضوعنا .فالمنشأة مسؤولة أمام الغير إذا سرّب موظفها بيانات الزبائن .وما توثقه من تدابير وقائية، كتقييد الصلاحيات وتدريب الموظفين، يصلح دليلاً على أنها بذلت العناية المطلوبة.

الفرع الثالث :حماية المنشأة من المنافسة غير المشروعة في البيئة الرقمية

كثيراً ما يكون المستفيد الأول من الاعتداء السيبراني منافساً للمنشأة .هو من يشتري قاعدتها المسروقة، أو يسقط موقعها في الموسم، أو يتسمى باسمها ليجتذب عملاءها .ولا يوجد في قانون

التجارة العراقي نص خاص بالمنافسة غير المشروعة، فتقوم الدعوى على القاعدة العامة في المسؤولية التقصيرية، ويُعد تعدياً موجباً للتعويض كل فعل يخالف العادات والأصول المرعية في التجارة.

أما في مصر فالأمر أوضح .فقانون التجارة عدّ من المنافسة غير المشروعة كل ما يخالف الأعراف والأصول الجارية في المعاملات التجارية، ومثّل لذلك بالتعدي على علامات الغير واسمه التجاري، وبإغراء عماله بكشف أسراره، وأجاز الحكم بالتعويض وبإزالة الضرر[٦٦]. وفي الإمارات تناول قانون المعاملات التجارية الموضوع بتفصيل، فمنع وسائل الغش، وإفشاء الأسرار، والتضليل الذي يُقصد به صرف العملاء عن المنافس[٦٧]. ومع إقرار القانون الإماراتي بالمحل التجاري الذي يعمل بالتقنيات الحديثة، تصبح هذه الدعوى أداة نافعة للمنشأة الإلكترونية؛ إذ يستطيع القاضي بموجبها أن يوقف الفعل ويمحو أثره، بحجب الموقع المنتحل مثلاً، فضلاً عن الحكم بالتعويض.

المطلب الثاني :مسؤولية المنشأة تجاه زبائنها عن تسرب بياناتهم

الفرع الأول :طبيعة التزام المنشأة بحماية بيانات الزبائن

إذا سُرقت بيانات الزبائن من نظام المنشأة انقلب مركزها :من ضحية إلى مدين يُطالب بالتعويض .فالزبون الذي أعطى المنشأة بياناته الشخصية وبيانات الدفع يرجع عليها بالمسؤولية العقدية لأنها لم تحفظ ما اؤتمنت عليه، وهو التزام نص عليه النظام رقم (4)لسنة 2025، ويمكن استخلاصه قبل ذلك من مبدأ حسن النية في تنفيذ العقود[٦٨]. وله كذلك أن يرجع عليها بالمسؤولية التقصيرية للمساس بخصوصيته، وهي من حقوق الشخصية التي يكفلها الدستور العراقي،[٦٩] ويستحق صاحبها التعويض عن الضرر الأدبي والنفسي ولو لم يلحقه ضرر مادي ظاهر[٧٠].

فهل تلتزم المنشأة بتحقيق نتيجة، فتُسأل لمجرد وقوع الخرق؟ أم ببذل عناية، فلا تُسأل إلا إذا ثبت أنها قصرت؟ نميل إلى الثاني .الأمن المطلق لا وجود له من الناحية التقنية، والنظام رقم (4)لسنة 2025طلب من التاجر أنظمة آمنة ولم يطلب منه أن يمنع كل اختراق .لكن هذا الترجيح لا يستقيم إلا بقيدين يحفظان حق الزبون .أولهما أن العناية المطلوبة هي عناية تاجر محترف يحوز بيانات الغير ويربح من معالجتها، لا عناية الشخص العادي .وثانيهما أن يُخفف عبء الإثبات عن الزبون؛ فسجلات النظام وآثار الاختراق كلها بيد المنشأة، ولا سبيل له إليها . وللقاضي أن يستعين هنا بالقرائن وبوسائل التقدم العلمي،[٧١] فيعد الخرق، مع امتناع المنشأة عن تقديم ما يثبت أنها اتخذت التدابير المعتادة، قرينة على تقصيرها.

وفي اللائحة الأوربية لحماية البيانات ما يشد أزر هذا الرأي .فهي تكلف المتحكم بأن تكون تدابيره الفنية والتنظيمية على قدر الخطر، وتفرض عليه إعلام الجهة الرقابية بالخرق في غضون ثلاثة أيام من علمه، وتمنح المتضرر حق التعويض عن الضرر المادي وغير المادي، ولا تعفي المتحكم إلا إذا برهن على أنه لا يُنسب إليه شيء في الواقعة[٧٢]. فعبء البرهان هناك على من يحوز البيانات، لا على من تضرر من تسربها، وهذا ما ندعو إليه.

وتكتب بعض المتاجر في صفحة الخصوصية أنها لا تتحمل أي مسؤولية إذا تسربت البيانات . عبارة كهذه لا تنفعها .فهي باطلة في نطاق المسؤولية التقصيرية عن المساس بالخصوصية، لأن القانون المدني العراقي لا يعتد بأي اتفاق على الإعفاء من المسؤولية الناشئة عن العمل غير المشروع[٧٣]. وهي بلا أثر في المسؤولية العقدية متى كان الخرق نتيجة خطأ جسيم .وهي فوق ذلك شرط جائر في عقد لم يُناقش فيه الزبون، وللقاضي أن يعفيه منه.

الفرع الثاني :هل يعد الهجوم السيبراني سبباً أجنبياً؟

الأصل في القانون المدني العراقي أن من يثبت أن الضرر جاء من سبب لا يد له فيه لا يلزمه ضمان، ومن أمثلة هذا السبب الآفة السماوية، والحادث الفجائي، والقوة القاهرة، وفعل الغير، وخطأ المتضرر نفسه[٧٤]. ولأن من يشن الهجوم السيبراني شخص غريب عن المنشأة، قد يُظن أن الأمر يدخل ببساطة في فعل الغير .غير أن فعل الغير لا يرفع المسؤولية كلها إلا إذا جمع صفتي القوة القاهرة :أن يتعذر توقعه، وأن يستحيل صده.

وهنا لب المسألة .الهجمات السيبرانية بوجه عام لم تعد مفاجأة؛ يعرفها كل من يدير متجراً على الشبكة، وقامت على مواجهتها صناعة كاملة من برامج الحماية وخدماتها .فلا تستطيع المنشأة أن تقول إن الاختراق باغتها .غير أن هذا لا يعني أن الهجوم لا يكون سبباً أجنبياً في أي حال . خذ مثلاً معتدياً استغل ثغرة لم يكن يعرفها أحد يوم الهجوم، ولم يصدر لها إصلاح من صانع البرنامج، في منشأة لم تترك تدبيراً معتاداً إلا اتخذته .هنا يمكن القول إن الهجوم لم يكن في وسعها دفعه، فينتفي خطؤها وتنقطع السببية.

والمعيار الذي نقترحه على القضاء العراقي إذن :لا يُعد الهجوم السيبراني بذاته سبباً أجنبياً، بل يُنظر إلى ما كانت المنشأة قد اتخذته من تدابير معتادة في مثل نشاطها يوم وقع الهجوم .إن كانت قد أخذت بها، ونفذ المعتدي مما لا تدفعه تلك التدابير، أُعفيت .وإن قصّرت، فتركت برامجها بلا تحديث، أو اكتفت بكلمات مرور ضعيفة، أو حفظت بيانات البطاقات بلا تشفير، سُئلت وإن كان الفاعل المباشر غيرها .وهذا المعيار يوافق ما قرره القانون المدني العراقي فيمن تحت تصرفه أشياء تتطلب عناية خاصة للوقاية من ضررها، إذ جعله مسؤولاً ما لم يثبت أنه

اتخذ الحيطة الكافية لمنع الضرر[٧٥]. ونحسب أن نظاماً معلوماتياً يحوي بيانات آلاف الزبائن من هذه الأشياء.

الفرع الثالث :الإثبات في منازعات الحوادث السيبرانية

نجاح المنشأة في الرجوع على المعتدي أو المزود، ونجاحها في دفع المسؤولية عن نفسها أمام الزبائن، يتوقف في النهاية على ما تملكه من دليل .وقد أعطى قانون التوقيع الإلكتروني والمعاملات الإلكترونية للمستندات والكتابة الإلكترونية حجية مثيلتها الورقية متى استوفت شروطها،[٧٦] فيمكن الاحتجاج بسجلات النظام ورسائل البريد الإلكتروني وتقارير الفحص الفني . لكن الدليل الرقمي في الحوادث السيبرانية سريع الزوال وسهل التغيير .يكفي أن تعيد المنشأة تشغيل النظام أو تحذف الملفات المصابة قبل توثيقها، ليضيع الدليل الذي كان سيبرئها أو يدين المعتدي.

لذلك نرى أن على المنشأة أن تحتفظ بسجلات نظامها مدة معقولة، كما ألزم المشرع المصري مقدمي الخدمة،[٧٧] وأن توثق الحادث بمجرد اكتشافه عن طريق خبير مختص قبل أي معالجة . ونرى كذلك أن يُنظم في التشريع العراقي طريق قضائي مستعجل تطلب به المنشأة المتضررة إلزام مزودي الخدمة بحفظ البيانات المتصلة بالهجوم والكشف عنها، فهي في الغالب الخيط الوحيد الذي يقود إلى الفاعل.

المطلب الثالث :التأمين من المخاطر السيبرانية

الفرع الأول :مفهوم التأمين السيبراني وقابلية الخطر للتأمين

إذا لم يُعرف المعتدي، أو عُرف ولم يكن له مال، فالتأمين هو الأمل الأقرب لتعويض المنشأة؛ إذ ينقل عبء الخسارة إلى شركة التأمين دون حاجة إلى إثبات خطأ على أحد .ويعرّف القانون المدني العراقي التأمين بأنه عقد يلتزم فيه المؤمن بأن يدفع للمؤمن له أو للمستفيد عوضاً مالياً إذا تحقق الخطر المؤمن منه، في مقابل ما يؤديه المؤمن له من أقساط[٧٨]. وليس في هذا التعريف ما يحول دون أن يكون الخطر المؤمن منه هجوماً على نظام المنشأة، ما دام وقوعه غير محقق ولا يتوقف على مشيئة المؤمن له.

ويرى الفقه أن الاقتصار على قواعد المسؤولية التقليدية يترك المتضرر في الفضاء الإلكتروني بلا حماية كافية، لأن كلفة التعويض فيه عالية قد لا يقوى المسؤول على تحملها وحده، ومن ثم يأتي التأمين من الأخطار الإلكترونية ليكمل المسؤولية المدنية لا ليحل محلها[٧٩]. والوثيقة السيبرانية في صورتها المعتادة تغطي صنفين من الخسائر :ما يصيب المنشأة مباشرة، كأجور

خبراء الفحص وكلفة استعادة البيانات وما يضيع بتوقف العمل؛ وما تُطالب به من الغير، كتعويضات الزبائن وأتعاب المحامين في الدعاوى.

الفرع الثاني :إشكاليات التأمين السيبراني في القانون العراقي

لا يكفي أن نقول إن التأمين السيبراني جائز .فتطبيقه في العراق يثير مسائل أدق، نتوقف عند ثلاث منها.

تغطية مبلغ الفدية. إذا نصت الوثيقة على أن يدفع المؤمن ما تدفعه المنشأة للمعتدي مقابل فك التشفير، فهل هذا مشروع؟ نرى أنه يخالف النظام العام، لأن الدفع يمول الجريمة ويغري بتكرارها .ويبقى للوثيقة أن تغطي نفقات استرجاع البيانات والتفاوض والاستشارة وخسائر التوقف، دون الفدية نفسها.

استثناء الأعمال الحربية. تستبعد الوثائق في العادة الأضرار الناشئة عن الحرب والأعمال العدائية .وقد يتذرع المؤمن بأن الهجوم جزء من حملة تقف وراءها دولة، ليخرجه من الضمان . وفي منطقة مضطربة كمنطقتنا تصبح هذه المسألة شديدة الحساسية .فلا يصح أن تُترك لتقدير المؤمن وحده؛ عليه هو أن يثبت انطباق الاستثناء، وعلى القاضي أن يفسره تفسيراً ضيقاً.

ما يُطلب من المؤمن له قبل الحادث. جرت عادة شركات التأمين على أن تشترط على المنشأة مستوى معيناً من الحماية التقنية، وأن تحرمها من التعويض إن لم تلتزم به .لا اعتراض على الشرط من حيث المبدأ .المشكلة في صياغته؛ فإذا جاء بعبارات مطاطة صار في يد المؤمن ذريعة جاهزة يجد بها في كل حادث تقصيراً يتخلص به من الدفع .والصواب أن تُسمى التدابير المطلوبة في الوثيقة واحداً واحداً، وأن يُشترط لحرمان المؤمن له من التعويض أن يكون إخلاله بأحدها هو الذي أدى إلى وقوع الحادث.

ويبقى أن سوق التأمين العراقية قليلة الخبرة بهذا النوع من التغطية، وأن المنشآت الصغيرة، وهي أكثر من يمارس التجارة الإلكترونية في العراق، لا تعرف ثقافة التأمين في الغالب ولا تقدر على أقساطه .لذا نرى أن يكون تدخل الدولة هنا بالتحفيز لا بالإلزام :أن يُحتسب التأمين مثلاً عند تجديد إجازة التاجر، أو أن تُمنح المنشآت المؤمَّن عليها مزايا ضريبية محددة.

الخاتمة

في نهاية هذه الدراسة لحماية المنشأة التجارية الإلكترونية من المخاطر السيبرانية في القانون العراقي، مقروءة في ضوء التجربتين المصرية والإماراتية، نعرض ما وصلنا إليه في أمرين.

أولاً :النتائج

١-لا يعرف التشريع العراقي المنشأة التجارية الإلكترونية بوصفها مالاً؛ فالنظام رقم (4)لسنة 2025عرّف المتجر الإلكتروني أداةً للعرض ليس غير .ومع ذلك يتسع مفهوم المتجر في القانون التجاري العراقي لهذه المنشأة، لأنه يقوم على الاتصال بالعملاء والسمعة التجارية ولا يشترط مكاناً مادياً .أما المشرع الإماراتي فقد قطع الشك بنص يُدخل في المحل التجاري ما يعمل عبر وسائل التقنية الحديثة.

٢-جوهر المنشأة الإلكترونية عناصرها المعنوية، وأغلبها بيانات :اسم النطاق، وسجل العملاء، والبرمجيات، والحسابات، والسمعة الرقمية .فحمايتها من المخاطر السيبرانية هي في الحقيقة حماية لهذه العناصر.

٣-تقف المنشأة أمام الخطر السيبراني في موقفين في آن :ضحية للاعتداء، ومدينة بحفظ بيانات زبائنها .وقد تُسأل أمامهم عن هجوم كانت هي هدفه.

٤-ألزم النظام رقم (4)لسنة 2025التاجر بحماية بيانات الزبائن والإبلاغ عن خرقها، وسكت عن مقدار الأمن المطلوب ومهلة الإبلاغ والجهة التي يُبلَّغ إليها .وضوابط الصمود السيبراني لا تخاطب إلا القطاع المالي، والإطار الذي أصدرته هيأة الإعلام والاتصالات يطرح سؤال تداخل الاختصاص.

٥-الاسم التجاري لا يُحمى في القانون العراقي إلا داخل المحافظة التي سُجل فيها، والتجارة الإلكترونية لا تعرف حدود المحافظات .ثم إن الضوابط رقم (3)لسنة 2025اشترطت التسجيل في النطاق العراقي، ومع ذلك لا نجد قواعد منشورة تحكم النزاع على هذه الأسماء.

٦-نصوص قانون العقوبات العراقي تنفع المنشأة في مواضع وتخذلها في أخرى .تنفعها إذا انتحل المعتدي صفة ليحتال، أو إذا كشف موظف سراً عرفه بحكم عمله .وتخذلها إذا نُسخت بياناتها أو مُحيت أو تعطل نظامها، لأن مبدأ الشرعية لا يسمح بمد نصوص السرقة والإتلاف إلى أشياء غير مادية .ولا يغني عن ذلك انضمام العراق إلى الاتفاقية العربية، فهي لا تكفي بذاتها لإنزال عقوبة.

٧-لم يتجاوز مشروع قانون مكافحة جرائم تقنية المعلومات قراءته الأولى، وقد طغى الخلاف على نصوص المحتوى فيه على حاجة ملحة لا خلاف فيها :تجريم الاعتداء على سلامة الأنظمة والبيانات.

٨-التشريعات المقارنة تحمي المنشأة ذاتها لا بيانات الأفراد وحدها .فالقانون المصري يشدد العقاب إذا وقع الاعتداء على حساب أو موقع لشخص اعتباري خاص، ويلزم المنشأة الضحية بالإبلاغ .

والقانون الإماراتي يخص البيانات السرية للمنشآت التجارية بنص، ويجرّم اصطناع المواقع المزورة بنص آخر.

٩-المادة (204)من القانون المدني العراقي أداة واسعة لحماية المنشأة، لأنها لا تتقيد بمبدأ الشرعية الجزائية فتطال أفعالاً تفلت من العقاب .غير أن جهالة المعتدي تُفقد الدعوى عليه قيمتها العملية في كثير من الحالات.

١٠-التزام المنشأة بحفظ بيانات زبائنها التزام ببذل عناية، والعناية المطلوبة عناية المهني .والهجوم السيبراني لا يكون بذاته سبباً أجنبياً، وإنما يُعفي المنشأة إذا ثبت أنها أخذت بالتدابير المعتادة يوم وقوعه .وهذا يتسق مع حكم المادة (231)من القانون المدني العراقي.

١١-التأمين من المخاطر السيبرانية أقرب الطرق إلى جبر الضرر حين يُجهل الفاعل، ولا يمنعه القانون المدني العراقي .لكنه يثير مسائل تحتاج إلى حسم :تغطية الفدية، واستثناء الأعمال الحربية، وشروط سقوط الضمان.

ثانياً :المقترحات

١-إذا تعذر التوافق على مشروع قانون مكافحة جرائم تقنية المعلومات بمجمله، فالأجدى أن تُستخرج منه الأحكام المتعلقة بسلامة الأنظمة والبيانات وتُقر وحدها دون إبطاء .ويكفي أن تغطي هذه الأحكام :النفاذ إلى النظام دون إذن، والتنصت على البيانات المتداولة، والعبث بالبيانات أو الأنظمة، والاحتيال عبر الوسائل التقنية، وسرقة بيانات الدفع، وإنشاء المواقع والحسابات المنتحلة.

٢-أن يُشدد العقاب متى كان النظام المعتدى عليه عائداً لمنشأة تجارية أو مالية، وأن تُحمى أسرار المنشأة المحفوظة إلكترونياً بنص قائم بذاته .ونقترح أن يُصاغ على هذا النحو" :كل من توصل، دون سند من القانون وعن طريق وسيلة تقنية، إلى معلومات أو بيانات سرية عائدة لمنشأة تجارية أو مالية، فاطلع عليها أو استنسخها أو غيّرها أو كشفها لغيره، يعاقب بالحبس أو بالغرامة أو بهما معاً، ويضاعف الحد الأعلى للعقوبة إذا كان الغرض من الفعل خدمة منشأة منافسة."

٣-أن يصدر قانون عام لحماية البيانات الشخصية، يبين ما على المتحكم من واجبات في أمن البيانات، ويلزمه بإبلاغ جهة رقابية معينة بأي خرق خلال اثنتين وسبعين ساعة في الأكثر من علمه به، وبإخطار أصحاب البيانات إذا كان الخرق يمس حقوقهم.

٤-أن تحدد وزارة التجارة، بالتعاون مع الجهة الوطنية المسؤولة عن الأمن السيبراني، الإجراءات الأمنية التي لا يجوز للتاجر الإلكتروني أن ينزل عنها، على أن تختلف باختلاف حجم المنشأة وحجم البيانات التي تتعامل بها، وأن يُعد التقيد بها قرينة على أن التاجر قام بما عليه.

٥-أن تُعدل المادة (24)من قانون التجارة لتشمل حماية الاسم التجاري المستعمل في التجارة الإلكترونية أرض العراق كلها، وأن تصدر تعليمات منشورة لتسجيل أسماء النطاق العراقية وتسوية منازعاتها.

٦-أن يُنص صراحة على أن المتجر يشمل ما يباشر نشاطه كله أو بعضه بالوسائل الإلكترونية، وأن اسم النطاق وقواعد بيانات العملاء والحسابات المخصصة للنشاط من عناصره المعنوية، على نحو ما فعل المشرع الإماراتي.

٧-أن يتضمن التشريع القادم حكماً في الإثبات يلزم المنشأة التي خُرقت بيانات زبائنها بتقديم ما يثبت أخذها بتدابير الأمن المعتادة، وإلا عُد الخرق قرينة على تقصيرها، مع إجراء قضائي مستعجل لإلزام مزودي الخدمة بحفظ البيانات المتصلة بالهجوم.

٨-أن ينظم ديوان التأمين وثائق التأمين السيبراني بتعليمات تحظر أن تشمل التغطية ما يُدفع فدية للمعتدين، وتفسر استثناء الحرب تفسيراً ضيقاً وتلقي عبء إثباته على شركة التأمين، وتمنع حرمان المؤمن له من التعويض ما لم يكن تقصيره في الأمن هو ما أحدث الضرر .ويحسن أن تقترن هذه التعليمات بمزايا تشجع المنشآت الصغيرة على التأمين.

٩-أن تُنظم برامج توعية وتدريب لصغار التجار الإلكترونيين في أساسيات أمن المعلومات؛ فأكثر الحوادث يقع بسبب أخطاء بسيطة يمكن اجتنابها، والقانون مهما اكتمل لا يغني عن الوقاية.

الهوامش

(١) دلال تفكير مراد و رغد عبد مسلم عبيد الحسناوي، دور المسؤولية المدنية في الحد من الهجمات الإلكترونية)دراسة مقارنة(، مجلة النهرين للعلوم القانونية، المجلد (27)، العدد (3)، الجزء (2)، 2025، ص .232-231

(٢)نظام تنظيم التجارة الإلكترونية رقم (4)لسنة 2025، المنشور في جريدة الوقائع العراقية، العدد (4818)، في 10/3/2025.

(٣) Mahmood Alaloosh, Ali Shaker Mahmood & Sabir Hussien Eliwy, "Securing Digital Trade: A Techno-Legal Analysis of E-Commerce Safeguards in Iraq's Regulation No. 4/2025", Nusantara: Journal of Law Studies, Vol. 5, No. 1, 2026, pp. 44-60.

(٤) دلال تفكير مراد ورغد عبد مسلم عبيد الحسناوي، مصدر سابق، ص .245-229

(٥) صباح محسن جلعوط، المسؤولية الجزائية عن الجرائم السيبرانية في ظل التحول الرقمي للهيئات الاقتصادية، مجلة جامعة الكوت، عدد خاص، 2026، ص .103-94

(٦)هالة الحديثي، قواعد التأمين عن الأخطار الإلكترونية)دراسة تحليلية(، مجلة الباحث العربي، المجلد (1)، العدد (1)، 2020، ص .26-13

(٧)رعد هاشم أمين، بروز ملامح التجارة الإلكترونية في التشريع العراقي :دراسة قانونية مقارنة، مجلة القادسية للقانون والعلوم السياسية، المجلد (17)، العدد (1)، الجزء (1)، 2026، ص .454-423

[٨]ينظر :نظام تنظيم التجارة الإلكترونية رقم (4)لسنة 2025، الأحكام الخاصة بالتعاريف؛ رعد هاشم أمين، مصدر سابق، ص 454-423.

[٩]المادة (66)من قانون التجارة العراقي رقم (149)لسنة 1970. ولم ينظم قانون التجارة النافذ رقم (30)لسنة 1984المتجر تنظيماً متكاملاً، وإن أشار إلى المحل التجاري في معرض أحكام الاسم التجاري في المادة (24/ ثانياً (منه، فظل الفقه يرجع في تحديد مفهومه وعناصره إلى أحكام القانون السابق.

[١٠]المادة (34)من قانون التجارة المصري رقم (17)لسنة 1999.

[١١] المادتان (36)و (37)من المرسوم بقانون اتحادي رقم (50)لسنة 2022بإصدار قانون المعاملات التجارية)دولة الإمارات العربية المتحدة.(

[١٢] رعد هاشم أمين، مصدر سابق، ص 454-423. وينظر في التاجر الرقمي :ياسر شاكر محمود ومصطفى ناطق صالح، النظام القانوني للتاجر الرقمي في ظل التطورات التشريعية، مجلة تويجر، المجلد (7)، العدد (2)، 2024، ص 183-170.

[١٣] ضوابط وزارة التجارة رقم (3)لسنة 2025الصادرة استناداً إلى البند)أولاً (من المادة (8)من نظام تنظيم التجارة الإلكترونية رقم (4)لسنة 2025، المتطلبات والوثائق المطلوبة للتسجيل.

[١٤] Aro Omar & Nawar Al-Ameri, "New Regulatory Framework for Digital Platforms and Services in Iraq", Mondaq, 30 September 2025.

[١٥]البنك المركزي العراقي، ضوابط الصمود السيبراني للقطاع المالي والمصرفي في العراق، منشورة على الموقع الرسمي للبنك في 26/6/2024.

[١٦] م .إخلاص لطيف محمد البحر، الإطار القانوني لوسائل الدفع الإلكتروني)دراسة مقارنة(، مجلة واسط للعلوم الإنسانية، المجلد (21)، العدد (2)، 2025، ص 398-377.

[١٧] دلال تفكير مراد و رغد عبد مسلم عبيد الحسناوي، مصدر سابق، ص 241-238.

[١٨] ينظر :نظام تنظيم التجارة الإلكترونية رقم (4)لسنة 2025، الأحكام الخاصة بحماية بيانات الزبائن؛ Aro Omar, Ali Al Dabbagh & Shangar Hussein, "Iraq's New E-Commerce Regulation", Mondaq, 11 July 2025.

[١٩] حسين كريم عبيد وأحمد عامر عبد الأمير وحيدر صلاح كاطع، قراءة نقدية في نظام تنظيم التجارة الإلكترونية العراقي رقم (4)لسنة 2025، مجلة المستقبل للدراسات القانونية، المجلد (1)، العدد (3)، 2026، ص 394-374.

[٢٠] نظام خدمات الدفع الإلكتروني للأموال رقم (2)لسنة 2024، المنشور في جريدة الوقائع العراقية، العدد (4771)، في 29/4/2024.

[٢١] Aro Omar & Nawar Al-Ameri, op. cit.

[٢٢] المادة (24)من قانون التجارة العراقي رقم (30)لسنة 1984.

[٢٣] ينظر في ذلك: Aro Omar & Nawar Al-Ameri, op. cit.؛ وفي أحكام الاسم التجاري :المواد (21- 25)من قانون التجارة العراقي رقم (30)لسنة 1984.

[٢٤] المادة (2)من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175)لسنة 2018، المنشور في الجريدة الرسمية، العدد (32)مكرر)ج(، في 14/8/2018.

[٢٥] المادة (29)من القانون ذاته.

[٢٦] المادة (35)من القانون ذاته.

[٢٧]المادة (4)من قانون حماية البيانات الشخصية المصري رقم (151)لسنة 2020.

[٢٨]المادة (7)من القانون ذاته.

[٢٩]المادة (20)من المرسوم بقانون اتحادي رقم (45)لسنة 2021بشأن حماية البيانات الشخصية)دولة الإمارات العربية المتحدة.(

[٣٠]المادة (9)من المرسوم بقانون ذاته.

[٣١]المادة (10)من المرسوم بقانون اتحادي رقم (14)لسنة 2023في شأن التجارة من خلال وسائل التقنية الحديثة.

[٣٢]المادة /19)ثانياً (من دستور جمهورية العراق لسنة 2005؛ والمادة (1)من قانون العقوبات العراقي رقم (111)لسنة 1969.

[٣٣]المادة (439)من قانون العقوبات العراقي.

[٣٤]المادة (456)من قانون العقوبات العراقي.

[٣٥]المادة (477)من قانون العقوبات العراقي.

[٣٦]المادة (437)من قانون العقوبات العراقي.

[٣٧] صباح محسن جلعوط، مصدر سابق، ص 103-94.

[٣٨]ينظر :المواد (6)و (8)و (11)من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، القاهرة، 21/12/2010.

[٣٩] ينظر :الشبكة العراقية للإعلام المجتمعي (INSM)، ورقة تقدير موقف ورأي قانوني في مسودة قانون مكافحة جرائم تقنية المعلومات العراقي لعام 2026، منشورة على الموقع الرسمي للشبكة، 2026.

[٤٠] Council of Europe, Convention on Cybercrime, ETS No. 185, Budapest, 23 November 2001, Articles 2–5 and 8.

[٤١] المادة (14)من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175)لسنة 2018.

[٤٢] المادة (15)من القانون ذاته.

[٤٣] المادة (16)من القانون ذاته.

[٤٤] المادة (17)من القانون ذاته.

[٤٥] المادة (18)من القانون ذاته.

[٤٦] المادة (21)من القانون ذاته.

[٤٧]المادة (23)من القانون ذاته.

[٤٨]المادة (36)من القانون ذاته.

[٤٩] المادة (2)من المرسوم بقانون اتحادي رقم (34)لسنة 2021في شأن مكافحة الشائعات والجرائم الإلكترونية)دولة الإمارات العربية المتحدة.(

[٥٠] المادة (4)من المرسوم بقانون ذاته.

[٥١] المادة (8)من المرسوم بقانون ذاته.

[٥٢] المادة (9)من المرسوم بقانون ذاته.

[٥٣] المادة (11)من المرسوم بقانون ذاته.

[٥٤] المادة (15)من المرسوم بقانون ذاته.

[٥٥] المادة (40)من المرسوم بقانون ذاته.

[٥٦] المادة (204)من القانون المدني العراقي رقم (40)لسنة 1951.

[٥٧] المادة (1 /207)من القانون المدني العراقي.

[٥٨] المادة (1 /205)من القانون المدني العراقي.

[٥٩] المادة (1 /217)من القانون المدني العراقي.

[٦٠] دلال تفكير مراد و رغد عبد مسلم عبيد الحسناوي، مصدر سابق، ص 245-242.

[٦١] المادة (168)من القانون المدني العراقي.

[٦٢] المادة (1 /251)من القانون المدني العراقي.

[٦٣] المادة (2 /259)من القانون المدني العراقي.

[٦٤] المادة (167)من القانون المدني العراقي .وينظر في مركز الوسيط الإلكتروني ومسؤوليته :د .ناجي العراك، الوسيط الإلكتروني في التجارة الإلكترونية في القانون العراقي، مجلة الباحث العربي، المجلد (2)، العدد (2)، 2021.

[٦٥] المادة (219)من القانون المدني العراقي.

[٦٦] المادة (66)من قانون التجارة المصري رقم (17)لسنة 1999.

[٦٧] المواد (66-60)من المرسوم بقانون اتحادي رقم (50)لسنة 2022بإصدار قانون المعاملات التجارية.

[٦٨] المادة (1 /150)من القانون المدني العراقي؛ ونظام تنظيم التجارة الإلكترونية رقم (4)لسنة 2025، الأحكام الخاصة بحماية بيانات الزبائن.

[٦٩] المادتان /17)أولاً (و (40)من دستور جمهورية العراق لسنة 2005.

[٧٠] م .سلمان علي حمادي، التعويض عن الضرر الناجم عن انتهاك الخصوصية الرقمية :دراسة مقارنة بين اللائحة العامة لحماية البيانات الأوربية والقانون المدني العراقي، مجلة المدارات العلمية للعلوم الإنسانية والاجتماعية، المجلد (4)، العدد (1)، 2026، ص 192-159.

[٧١] المادة (104)من قانون الإثبات العراقي رقم (107)لسنة 1979.

[٧٢] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Articles 32, 33 and 82.

[٧٣] المادة (3 /259)من القانون المدني العراقي.

[٧٤] المادة (211)من القانون المدني العراقي، وتقابلها في المسؤولية العقدية المادة (168)منه.

[٧٥] المادة (231)من القانون المدني العراقي.

[٧٦] المادة /13)أولاً (من قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم (78)لسنة 2012.

[٧٧] المادة (2)من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175)لسنة 2018.

[٧٨] المادة (1 /983)من القانون المدني العراقي .وينظر في تنظيم مزاولة أعمال التأمين :قانون تنظيم أعمال التأمين)الأمر رقم 10لسنة 2005).

[٧٩] هالة الحديثي، مصدر سابق، ص 26-13.

قائمة المصادر

أولاً :البحوث المنشورة

١-إخلاص لطيف محمد البحر، الإطار القانوني لوسائل الدفع الإلكتروني)دراسة مقارنة(، مجلة واسط للعلوم الإنسانية، المجلد (21)، العدد (2)، 2025، ص 398-377.

٢-أسماء مكي دباش، النظام القانوني للتجارة الإلكترونية وفق قانون رقم 4لسنة 2025، مجلة آشور للعلوم القانونية والسياسية، المجلد (3)، العدد (2)، 2026، ص 93-72.

٣-حسين كريم عبيد وأحمد عامر عبد الأمير وحيدر صلاح كاطع، قراءة نقدية في نظام تنظيم التجارة الإلكترونية العراقي رقم (4)لسنة 2025، مجلة المستقبل للدراسات القانونية، المجلد (1)، العدد (3)، 2026، ص 374- 394.

٤-دلال تفكير مراد ورغد عبد مسلم عبيد الحسناوي، دور المسؤولية المدنية في الحد من الهجمات الإلكترونية)دراسة مقارنة(، مجلة النهرين للعلوم القانونية، المجلد (27)، العدد (3)، الجزء (2)، 2025، ص 245-229.

٥-رعد هاشم أمين، بروز ملامح التجارة الإلكترونية في التشريع العراقي :دراسة قانونية مقارنة، مجلة القادسية للقانون والعلوم السياسية، المجلد (17)، العدد (1)، الجزء (1)، 2026، ص 454-423.

٦-سلمان علي حمادي، التعويض عن الضرر الناجم عن انتهاك الخصوصية الرقمية :دراسة مقارنة بين اللائحة العامة لحماية البيانات الأوربية والقانون المدني العراقي، مجلة المدارات العلمية للعلوم الإنسانية والاجتماعية، المجلد (4)، العدد (1)، 2026، ص 192-159.

٧-صباح محسن جلعوط، المسؤولية الجزائية عن الجرائم السيبرانية في ظل التحول الرقمي للهيئات الاقتصادية، مجلة جامعة الكوت، عدد خاص، 2026، ص 103-94.

٨-ناجي العراك، الوسيط الإلكتروني في التجارة الإلكترونية في القانون العراقي، مجلة الباحث العربي، المجلد (2)، العدد (2)، 2021.

٩-هالة الحديثي، قواعد التأمين عن الأخطار الإلكترونية)دراسة تحليلية(، مجلة الباحث العربي، المجلد (1)، العدد (1)، 2020، ص 26-13.

١٠-ياسر شاكر محمود ومصطفى ناطق صالح، النظام القانوني للتاجر الرقمي في ظل التطورات التشريعية، مجلة تويجر، المجلد (7)، العدد (2)، 2024، ص 183-170.

ثانياً :التشريعات

أ) الاتفاقيات الدولية(

١-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، القاهرة، 21/12/2010.

ب) التشريعات العراقية(

١-دستور جمهورية العراق لسنة 2005.
٢-القانون المدني رقم (40)لسنة 1951.
٣-قانون العقوبات رقم (111)لسنة 1969.
٤-قانون التجارة رقم (149)لسنة 1970.
٥-قانون الإثبات رقم (107)لسنة 1979.
٦-قانون التجارة رقم (30)لسنة 1984.
٧-قانون تنظيم أعمال التأمين)الأمر رقم 10لسنة 2005).
٨-قانون منع إساءة استعمال أجهزة الاتصالات في إقليم كوردستان رقم (6)لسنة 2008.
٩-قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم (78)لسنة 2012.
١٠-نظام خدمات الدفع الإلكتروني للأموال رقم (2)لسنة 2024.
١١-نظام تنظيم التجارة الإلكترونية رقم (4)لسنة 2025.
١٢-ضوابط وزارة التجارة رقم (3)لسنة 2025الصادرة بموجب المادة /8)أولاً (من نظام تنظيم التجارة الإلكترونية.

ج) التشريعات المصرية(

١-قانون التجارة رقم (17)لسنة 1999.
٢-قانون مكافحة جرائم تقنية المعلومات رقم (175)لسنة 2018.
٣-قانون حماية البيانات الشخصية رقم (151)لسنة 2020.

د) التشريعات الإماراتية(

١-المرسوم بقانون اتحادي رقم (34)لسنة 2021في شأن مكافحة الشائعات والجرائم الإلكترونية.
٢-المرسوم بقانون اتحادي رقم (45)لسنة 2021بشأن حماية البيانات الشخصية.
٣-المرسوم بقانون اتحادي رقم (50)لسنة 2022بإصدار قانون المعاملات التجارية.
٤-المرسوم بقانون اتحادي رقم (14)لسنة 2023في شأن التجارة من خلال وسائل التقنية الحديثة.

ثالثاً :الوثائق الرسمية وأوراق السياسات

١–البنك المركزي العراقي، ضوابط الصمود السيبراني للقطاع المالي والمصرفي في العراق، الموقع الرسمي للبنك المركزي العراقي، 26/6/2024.

٢–الشبكة العراقية للإعلام المجتمعي (INSM)، ورقة تقدير موقف ورأي قانوني في مسودة قانون مكافحة جرائم تقنية المعلومات العراقي لعام 2026، 2026.

٣–هيأة الإعلام والاتصالات، الإطار التنظيمي للمنصات والخدمات الرقمية، 17/2/2025.

رابعاً :المصادر الأجنبية

1.Alaloosh, Mahmood; Mahmood, Ali Shaker & Eliwy, Sabir Hussien, "Securing Digital Trade: A Techno-Legal Analysis of E-Commerce Safeguards in Iraq's Regulation No. 4/2025", Nusantara: Journal of Law Studies, Vol. 5, No. 1, 2026, pp. 44-60.

2.Council of Europe, Convention on Cybercrime, ETS No. 185, Budapest, 23 November 2001.

3.Omar, Aro; Al Dabbagh, Ali & Hussein, Shangar, "Iraq's New E-Commerce Regulation", Mondaq, Contracts and Commercial Law – Iraq, 11 July 2025.

4.Omar, Aro & Al-Ameri, Nawar, "New Regulatory Framework for Digital Platforms and Services in Iraq", Mondaq, Financial Services – Iraq, 30 September 2025.

5.Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

List of Sources

First: Published Research

1- Ikhlas Latif Muhammad Al-Bahr, The Legal Framework for Electronic Payment Methods (A Comparative Study), Wasit Journal of Human Sciences, Volume (21), Issue (2), 2025, pp. 377-398.

2- Asmaa Makki Dabash, The Legal System of E-Commerce According to Law No. 4 of 2025, Ashur Journal of Legal and Political Sciences, Volume (3), Issue (2), 2026, pp. 72-93.

3- Hussein Karim Obeid, Ahmed Amer Abdul-Amir, and Haider Salah Katea, A Critical Reading of the Iraqi E-Commerce Regulation No. (4) of 2025, Al-Mustaqbal

Journal of Legal Studies, Volume (1), Issue (3), 2026, pp. 374-394. 4- Dalal Tafkir Murad and Raghad Abdul Muslim Ubaid Al-Hasnawi, The Role of Civil Liability in Reducing Cyberattacks (A Comparative Study), Al-Nahrain Journal of Legal Sciences, Volume (27), Issue (3), Part (2), 2025, pp. 229-245.

5- Raad Hashim Amin, The Emergence of E-Commerce Features in Iraqi Legislation: A Comparative Legal Study, Al-Qadisiyah Journal of Law and Political Science, Volume (17), Issue (1), Part (1), 2026, pp. 423-454.

6- Salman Ali Hammadi, Compensation for Damages Resulting from Violations of Digital Privacy: A Comparative Study Between the European General Data Protection Regulation and Iraqi Civil Law, Al-Madarat Al-Ilmiyah Journal of Humanities and Social Sciences, Volume (4), Issue (1), 2026, pp. 159-192. 7- Sabah Mohsen Jalout, Criminal Liability for Cybercrimes in Light of the Digital Transformation of Economic Entities, Al-Kut University Journal, Special Issue, 2026, pp. 94-103.
8- Naji Al-Arak, The Electronic Intermediary in E-Commerce in Iraqi Law, Arab Researcher Journal, Volume (2), Issue (2), 2021.

9- Hala Al-Hadithi, Rules of Insurance Against Electronic Risks (An Analytical Study), Arab Researcher Journal, Volume (1), Issue (1), 2020, pp. 13-26.
10- Yasser Shaker Mahmoud and Mustafa Natiq Saleh, The Legal System of the Digital Merchant in Light of Legislative Developments, Tawjir Journal, Volume (7), Issue (2), 2024, pp. 170-183.

Second: Legislation

(A) International Agreements

1- Arab Convention on Combating Information Technology Crimes, Cairo, December 21, 2010. (b) Iraqi Legislation

1- Constitution of the Republic of Iraq of 2005.

2- Civil Code No. (40) of 1951.

3- Penal Code No. (111) of 1969.

4- Commercial Code No. (149) of 1970.

5- Evidence Law No. (107) of 1979.

6- Commercial Code No. (30) of 1984.

7- Law Regulating Insurance Business (Order No. 10 of 2005). 8- Law No. (6) of 2008 on Preventing Misuse of Telecommunications Devices in the Kurdistan Region.

9- Law No. (78) of 2012 on Electronic Signatures and Electronic Transactions.

10- Electronic Payment Services Regulation No. (2) of 2024.

11- Electronic Commerce Regulation No. (4) of 2025.

12- Ministry of Commerce Regulations No. (3) of 2025 issued pursuant to Article (8/First) of the Electronic Commerce Regulation.

(c) Egyptian Legislation

1- Commercial Law No. (17) of 1999.

2- Law No. (175) of 2018 on Combating Information Technology Crimes.

3- Law No. (151) of 2020 on the Protection of Personal Data.

(d) UAE Legislation

1- Federal Decree-Law No. (34) of 2021 on Combating Rumors and Cybercrimes. 2- Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data.

3- Federal Decree-Law No. (50) of 2022 promulgating the Commercial Transactions Law.

4- Federal Decree-Law No. (14) of 2023 on Trade through Modern Technology.

Third: Official Documents and Policy Papers

1- Central Bank of Iraq, Cyber Resilience Controls for the Financial and Banking Sector in Iraq, Central Bank of Iraq Official Website, June 26, 2024.

2- Iraqi Network for Community Media (INSM), Position Paper and Legal Opinion on the Draft Iraqi Cybercrime Law of 2026, 2026.

3- Communications and Media Commission, Regulatory Framework for Digital Platforms and Services, February 17, 2025.

Fourth: Foreign Sources

1.Alaloosh, Mahmood; Mahmood, Ali Shaker & Eliwy, Sabir Hussien, "Securing Digital Trade: A Techno-Legal Analysis of E-Commerce Safeguards in Iraq's Regulation No. 4/2025", Nusantara: Journal of Law Studies, Vol. 5, No. 1, 2026, pp. 44-60.

2.Council of Europe, Convention on Cybercrime, ETS No. 185, Budapest, 23 November 2001.

3.Omar, Aro; Al Dabbagh, Ali & Hussein, Shangar, "Iraq's New E-Commerce Regulation", Mondaq, Contracts and Commercial Law – Iraq, 11 July 2025.
4.Omar, Aro & Al-Ameri, Nawar, "New Regulatory Framework for Digital Platforms and Services in Iraq", Mondaq, Financial Services – Iraq, 30 September 2025.
5.Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).