

Cybercrimes Related to Attacks on Electronic Signatures and Credit Card Data in E-Commerce (A Comparative Analytical Study in Light of Palestinian Legislation and Selected Arab Legislations)

Dr. Majd Anwar Qumseya

Faculty of Law | Palestine Ahliya University | Palestine

Received:

29/04/2026

Revised:

07/05/2026

Accepted:

14/05/2026

Published:

30/08/2026

* Corresponding author:

mqumsieh@yahoo.com

Citation: Qumseya, M. A.

(2026). Cybercrimes related to attacks on electronic signatures and credit card data in e-commerce (a comparative analytical study in light of Palestinian legislation and selected Arab legislations).

Journal of Economic, Administrative and Legal Sciences, 10(8), 101–123.
<https://doi.org/10.26389/AJSRP.Q010526>

2026 © AISRP • Arab Institute for Sciences & Research Publishing (AISRP), United States, all rights reserved.

• Open Access



This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC) license

Abstract: Despite the rapid expansion of e-commerce, electronic payment systems, and electronic authentication mechanisms, traditional criminal rules still face difficulties in addressing digital crimes related to attacks on electronic signatures and credit card data, while Arab legal scholarship continues to lack a comprehensive comparative assessment of the adequacy of legislative frameworks governing such crimes. This study aims to evaluate the adequacy of legal and criminal regulation in confronting e-commerce crimes related to attacks on electronic signatures and credit card data. The study adopts a descriptive analytical approach supported by a comparative method through the analysis of Palestinian legislation, Egyptian legislation, and selected Arab and foreign laws related to cybercrimes and electronic transactions. The study reveals that the intangible and cross-border nature of the digital environment weakens the effectiveness of traditional criminal rules, and that Palestinian and Egyptian legislation lack specialized criminal provisions that independently criminalize the unlawful acquisition of credit card data and advanced forms of attacks on electronic signatures, leading to reliance on traditional legal characterizations that do not always accommodate the specific nature of financially valuable digital data. The study further demonstrates the need for a more appropriate legislative and technical framework capable of strengthening criminal protection for electronic transactions and improving the legal treatment of digital crimes within Arab legal systems.

Keywords: E-commerce, E-commerce Crimes, Electronic Signature, Credit Card Data, Digital Data, Criminal Protection, Digital Evidence.

جرائم التجارة الإلكترونية المرتبطة بالاعتداء على التوقيع الإلكتروني وبيانات بطاقات الائتمان (دراسة تحليلية مقارنة في ضوء التشريع الفلسطيني وبعض التشريعات العربية)

الدكتور/ مجد أنور قمصية

كلية الحقوق | جامعة فلسطين الأهلية | فلسطين

المستخلص: على الرغم من التوسع المتسارع في التجارة الإلكترونية ووسائل الدفع والتوقيع الإلكتروني، لا تزال القواعد الجزائية التقليدية تواجه صعوبات في ملاحقة الجرائم الرقمية المرتبطة بالاعتداء على التوقيع الإلكتروني وبيانات بطاقات الائتمان، كما تفتقر الأدبيات القانونية العربية إلى معالجة مقارنة شاملة لكفاية الأطر التشريعية المنظمة لهذه الجرائم، وتهدف هذه الدراسة إلى تقييم كفاية التنظيم القانوني والجزائي في مواجهة جرائم التجارة الإلكترونية المرتبطة بالاعتداء على التوقيع الإلكتروني وبيانات بطاقات الائتمان. واعتمدت الدراسة على المنهج الوصفي التحليلي مدعوماً بالمنهج المقارن، من خلال تحليل التشريع الفلسطيني والتشريع المصري وبعض التشريعات العربية والأجنبية المتعلقة بالجرائم المعلوماتية والمعاملات الإلكترونية، وقد أظهرت الدراسة أن الطبيعة اللامادية والعابرة للحدود للبيئة الرقمية تُضعف فعالية القواعد الجزائية التقليدية، وأن التشريع الفلسطيني والمصري يفتقران إلى نصوص جزائية متخصصة تُجرّم بصورة مستقلة الاستيلاء على بيانات بطاقات الائتمان وصور الاعتداء المتقدمة على التوقيع الإلكتروني، مما يؤدي إلى اللجوء إلى تكييفات تقليدية لا تستوعب دائماً الطبيعة الخاصة للبيانات ذات القيمة المالية، كما كشفت الدراسة الحاجة إلى تطوير تنظيم تشريعي وتقني أكثر ملاءمة للبيئة الرقمية، بما يعزز الحماية الجنائية للمعاملات الإلكترونية ويطوّر المعالجة القانونية للجرائم الرقمية في التشريعات العربية.

الكلمات المفتاحية: التجارة الإلكترونية، جرائم التجارة الإلكترونية، التوقيع الإلكتروني، بطاقات الائتمان، البيانات الرقمية، الحماية الجزائية، الإثبات الرقمي.

المقدمة:

شهد العالم خلال العقود الأخيرة تحولات عميقة بفعل الثورة الرقمية والتطور المتسارع في تقنيات المعلومات والاتصالات، الأمر الذي أسهم في إعادة تشكيل الأنماط التقليدية للنشاط الاقتصادي والتجاري، وأبرز ما يُعرف بالاقتصاد الرقمي بوصفه نموذجاً جديداً يقوم على المعرفة وتدفق البيانات والتفاعل الإلكتروني، وقد مثل ظهور شبكة الإنترنت نقطة تحول مركزية في هذا المسار، إذ أتاحت بيئة عالمية مفتوحة لتبادل المعلومات وإبرام المعاملات وتقديم الخدمات عبر الحدود، من دون التقيد بالحدود المكانية أو الزمنية التي كانت تحكم التجارة التقليدية.

وفي ظل هذه التحولات، برزت التجارة الإلكترونية باعتبارها إحدى أهم صور النشاط التجاري المعاصر، لما توفره من سرعة في إبرام المعاملات، واتساع في نطاق الأسواق، وانخفاض في تكاليف التشغيل، وسهولة في الوصول إلى المستهلكين، ولم يعد التطور منصباً على جوهر العمل التجاري ذاته، وإنما امتد إلى الوسائل القانونية والتقنية التي تُمارس من خلالها العلاقات التجارية، بما أوجد أنماطاً جديدة من التعاقد والوفاء والإثبات والتنفيذ.

غير أن هذا التطور، على ما ينطوي عليه من مزايا اقتصادية وعملية، أفرز في المقابل تحديات قانونية متزايدة، تمثلت في صعوبة ضبط بعض المعاملات الإلكترونية، وإثبات التصرفات القانونية، وتحديد المسؤولية الناشئة عن استخدام الوسائل الرقمية في البيئة التجارية الإلكترونية.

كما أدى هذا التطور إلى ظهور أنماط مستحدثة من الجرائم الإلكترونية المرتبطة بالتجارة الإلكترونية، سواء من خلال المساس بوسائل التوثيق الإلكتروني، كالتوقيع الإلكتروني، أو عبر الاستيلاء غير المشروع على البيانات المالية ومعلومات الدفع، أو من خلال صور الاحتيال والاختراق وانتحال الهوية وغيرها من الأنماط الإجرامية التي تستفيد من الطبيعة التقنية والعابرة للحدود للفضاء الرقمي، الأمر الذي أدى إلى بروز تحديات متصلة بالاختصاص والتعاون الدولي وتفاوت المقاربات التشريعية المنظمة للجرائم السيبرانية⁽¹⁾.

وتشير التقديرات الحديثة إلى أن الخسائر العالمية الناجمة عن الاحتيال في المدفوعات الرقمية المرتبطة بالتجارة الإلكترونية تُقدَّر بنحو 362 مليار دولار عالمياً خلال الفترة الممتدة بين عامي 2023 و2028، في ظل التوسع المتسارع في استخدام وسائل الدفع الإلكتروني والمعاملات الرقمية العابرة للحدود، الأمر الذي يعكس تنامي المخاطر المرتبطة بالجرائم السيبرانية والاعتداءات الواقعة على البيانات المالية ووسائل التوثيق الإلكتروني⁽²⁾.

ولذلك، لم تعد مواجهة الجرائم المرتبطة بالتجارة الإلكترونية تقتصر على التجريم التقليدي، بل أصبحت ترتبط بمفاهيم الحوكمة الرقمية، التي تقوم على تكامل الأبعاد القانونية والتقنية والتنظيمية والإجرائية، بهدف حماية الثقة في البيئة الرقمية، وضمان أمن المعاملات الإلكترونية، وتعزيز موثوقية وسائل الدفع والتوثيق الإلكتروني.

إشكالية الدراسة

تتمحور إشكالية الدراسة حول التساؤل الرئيس الآتي:

ما مدى كفاية التنظيم القانوني للتجارة الإلكترونية في بيان ماهيتها وخصائصها ومزاياها، وفي توفير حماية جزائية فعالة من الجرائم التي تستهدف وسائلها ومعاملاتها الإلكترونية؟

ويُقصد بالكفاية في نطاق هذه الدراسة مدى قدرة التنظيم القانوني على توفير حماية فعالة للمعاملات الإلكترونية، من خلال وجود نصوص تجريم صريحة، وعقوبات ملائمة، وآليات فعالة للإثبات الرقمي، وقواعد تتيح التعاون القضائي الدولي في مواجهة الجرائم الإلكترونية ذات الطابع العابر للحدود، وهي المعايير التي تستند إليها الدراسة في تقييم التشريعات محل المقارنة.

ولتحقيق قدر أكبر من الانضباط التحليلي في الدراسة المقارنة، اعتمدت الدراسة على مصفوفة تحليلية تقوم على تقييم التشريعات محل المقارنة في ضوء مجموعة من معايير الكفاية المحددة مسبقاً، والمتمثلة في: وجود نصوص تجريم صريحة، وملاءمة العقوبات، وكفاية قواعد الإثبات الرقمي، ومدى فعالية آليات التعاون القضائي الدولي، وذلك بهدف الانتقال من العرض الوصفي للتشريعات إلى تقييم مدى قدرتها على توفير حماية جزائية فعالة للمعاملات الإلكترونية.

ويتفرع عن هذا التساؤل عدد من الأسئلة الفرعية، أهمها:

1- ما المقصود بالتجارة الإلكترونية، وما أبرز التعريفات القانونية والفقهية لها؟

(1)- Fidler, M. (2025). Fragmentation of international cybercrime law. Utah Law Review, 2025(3), pp. 750 – 751, 791 – 794.

<https://doi.org/10.63140/wez4rujib0>

(2) - Juniper Research. (2023, June 26). Losses from online payment fraud to exceed 362\$ billion globally over next 5 years.

<https://www.juniperresearch.com/press/losses-online-payment-fraud-exceed-362-billion/>

- 2- ما الخصائص التي تميز التجارة الإلكترونية عن التجارة التقليدية؟
- 3- ما أهم الفوائد التي تحققها التجارة الإلكترونية بالنسبة للشركات والزبائن؟
- 4- ما المقصود بالتوقيع الإلكتروني، وما أهميته في المعاملات التجارية الإلكترونية؟
- 5- ما أبرز صور الاعتداء التي يمكن أن تقع على التوقيع الإلكتروني؟
- 6- ما الطرق والأساليب المستخدمة في السطو على أرقام البطاقات الائتمانية؟
- 7- ما الأركان القانونية لجريمة الاستيلاء على أرقام بطاقات الائتمان؟

أهمية الدراسة

تنبع أهمية هذه الدراسة من المكانة المتنامية التي تحتلها التجارة الإلكترونية في الاقتصاد المعاصر، وما أفرزته من تحول جوهري في أساليب التبادل التجاري وإبرام المعاملات على المستويين الوطني والدولي، الأمر الذي جعلها أحد المرتكزات الأساسية للنشاط الاقتصادي الحديث، كما تستمد الدراسة أهميتها من الحاجة إلى بيان الإطار القانوني الناظم لهذا النوع من التجارة، بما يكفل حماية المتعاملين، وتعزيز الثقة في البيئة الرقمية، وترسيخ الأمن القانوني في المعاملات الإلكترونية. وتتأكد أهمية الموضوع كذلك في ظل تصاعد الجرائم المرتبطة بالتجارة الإلكترونية وتطور وسائل ارتكابها، ولا سيما ما يتصل بالاعتداء على التوقيع الإلكتروني والسطو على أرقام البطاقات الائتمانية، بما يفرض ضرورة مراجعة القواعد التشريعية والجزائية القائمة، وبيان مدى كفايتها في توفير حماية فعالة تواكب التطور التقني وتحد من المخاطر الناشئة عنه.

الدراسات السابقة والفجوة البحثية

تناولت العديد من الدراسات العربية موضوع الجرائم الإلكترونية والمعاملات الإلكترونية من زوايا متفرقة، فركّز بعضها على حجية التوقيع الإلكتروني وتنظيمه القانوني، بينما اهتمت دراسات أخرى بجرائم الاحتيال المعلوماتي أو حماية بيانات بطاقات الائتمان في البيئة الرقمية. غير أن هذه الدراسات غالباً ما عالجت الموضوع معالجة جزئية أو وصفية، دون تقديم تحليل مقارن يجمع بين الاعتداء على التوقيع الإلكتروني وجرائم الاستيلاء على بيانات بطاقات الائتمان ضمن إطار واحد يختبر كفاية التنظيم الجزائي في البيئة الرقمية الحديثة. كما أن جانباً من الأدبيات العربية لا يزال يعتمد على معالجات تقليدية، في وقت تشهد فيه الجرائم السيبرانية والتحقيقات الرقمية تطورات تشريعية وتقنية متسارعة تتطلب تحديثاً مستمراً للأطر القانونية المنظمة للأدلة الرقمية والمعاملات الإلكترونية⁽³⁾. وتبعاً لذلك، تأتي هذه الدراسة لسدّ هذا الفراغ من خلال تقديم تحليل قانوني مقارن يجمع بين التشريع الفلسطيني والتشريع المصري وبعض التشريعات العربية والأجنبية، مع التركيز على خصوصية الجرائم المرتبطة بوسائل الثقة والدفع في التجارة الإلكترونية، وبيان مدى كفاية القواعد الجزائية التقليدية في مواجهتها. ويرى الباحث أن الطابع الوصفي الذي لا يزال يغلب على جانب من الدراسات القانونية العربية في مجال الجرائم المرتبطة بالتجارة الإلكترونية يعود إلى حداثة الظاهرة الرقمية وتسارع تطورها التقني مقارنة بوتيرة التطور التشريعي والفقه، فضلاً عن استمرار تأثر بعض المعالجات القانونية بالمفاهيم التقليدية للمال والمحركات ووسائل الإثبات. ومن ثمّ، فإن دراسة الجرائم الرقمية لم تعد تقتصر على مجرد تكييف السلوك الإجرامي في ضوء القواعد الجزائية التقليدية، بل أصبحت تقتضي إعادة النظر في مدى ملاءمة البنية القانونية القائمة لاستيعاب خصوصية البيئة الرقمية الحديثة.

الإسهام العلمي للدراسة

تتمثل الأصلة العلمية لهذه الدراسة في أنها لا تقتصر على تناول جرائم التجارة الإلكترونية من منظور وصفي تقليدي، وإنما تسعى إلى بناء معالجة قانونية تحليلية تجمع بين جرائم الاعتداء على التوقيع الإلكتروني وجرائم الاستيلاء على بيانات بطاقات الائتمان ضمن إطار مقارن موحد، مع ربط ذلك بخصوصية البيئة الفلسطينية والتحديات المرتبطة بحماية الثقة الرقمية في المعاملات الإلكترونية. كما تحاول الدراسة توظيف نتائج المقارنة التشريعية في استخلاص ملامح إطار تنظيمي وتشريعي أكثر ملاءمة للبيئة الرقمية الحديثة، بما يتجاوز مجرد عرض أوجه القصور التشريعي إلى اقتراح توجهات تنظيمية يمكن أن تسهم في تطوير الحماية الجزائية للمعاملات الإلكترونية في التشريعات العربية.

(3) - Allah Rakha, N. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. Mexican Law Review, 16(2), pp. 46 – 53. <https://doi.org/10.22201/ijj.24485306e.2024.2.18892>

منهج الدراسة

اعتمدت الدراسة على المنهج الوصفي التحليلي، من خلال بيان ماهية التجارة الإلكترونية وخصائصها وأهم فوائدها، وتحليل أبرز الجرائم الواقعة عليها، ولا سيما الاعتداء على التوقيع الإلكتروني والسطو على أرقام البطاقات الائتمانية، مع بيان الأركان القانونية لهذه الجرائم وصور السلوك الإجرامي المرتبط بها، كما استعانت الدراسة بالمنهج المقارن من خلال الإفادة من بعض التشريعات العربية والأجنبية ذات الصلة، بقصد الوقوف على الاتجاهات التشريعية الحديثة وبيان مدى كفاية الحلول القانونية المعتمدة في مواجهة الجرائم المرتبطة بالتجارة الإلكترونية.

واعتمدت الدراسة في تحليلها على المصادر التشريعية والفقهية والأحكام القضائية والدراسات القانونية الحديثة ذات الصلة بموضوع الجرائم الإلكترونية والمعاملات الإلكترونية، مع التركيز على الأدبيات المرتبطة بحماية التوقيع الإلكتروني وبيانات الدفع الرقمي. وقد استند اختيار التشريعات محل المقارنة إلى اعتبارات منهجية تتصل بطبيعة الدراسة وأهدافها، إذ جرى اختيار بعض التشريعات العربية والأجنبية بالنظر إلى تفاوت مستويات التطور التشريعي في مجال الجرائم الإلكترونية والمعاملات الإلكترونية، ولتمثيل اتجاهات قانونية مختلفة في تنظيم الاعتداءات الواقعة على التوقيع الإلكتروني وبيانات بطاقات الائتمان، كما أخذ في الاعتبار عند اختيار هذه التشريعات انتماءها إلى بيئات قانونية متقاربة مع التشريع الفلسطيني، وأخرى تمثل نماذج تشريعية متقدمة في مجال التنظيم الرقمي، بما يسمح بتقييم مدى كفاية القواعد القانونية القائمة واستخلاص اتجاهات تشريعية يمكن الإفادة منها في تطوير الحماية الجزائية للتجارة الإلكترونية في السياق الفلسطيني.

ولتوضيح المعايير المعتمدة في تقييم كفاية التشريعات محل المقارنة، يمكن بيانها في الجدول الآتي:

جدول (1): معايير تقييم كفاية التنظيم القانوني في التشريعات محل المقارنة

مضمون التقييم	معايير الكفاية
مدى وجود نصوص قانونية صريحة تُجرّم الاعتداء على التوقيع الإلكتروني وبيانات بطاقات الائتمان	نصوص التجريم
مدى تناسب الجزاءات الجنائية مع طبيعة السلوك الإجرامي وخطورته في البيئة الرقمية	تناسب العقوبات
مدى الاعتراف القانوني بالأدلة الرقمية وتنظيم إجراءات جمعها وحجبتها	كفاية قواعد الإثبات الرقمي
مدى تنظيم آليات المساعدة القضائية والتعاون العابر للحدود في الجرائم الإلكترونية	فعالية التعاون الدولي

ولا تقتصر أهمية هذه المعايير على قياس وجود الحماية القانونية من الناحية الشكلية، بل تمتد إلى اختبار مدى فعالية هذه الحماية في البيئة الرقمية من الناحية العملية؛ إذ قد تتوافر نصوص التجريم من حيث الوجود، دون أن تكون قادرة على توفير حماية فعالة في ظل صعوبات الإثبات الرقمي والطابع العابر للحدود للجرائم الإلكترونية. ولذلك، تنطلق الدراسة من فكرة مؤداها أن كفاية التنظيم القانوني لا تُقاس بعدد النصوص الجزائية فحسب، وإنما بمدى قدرتها على الاستجابة للخصوصية التقنية والوظيفية التي تميز المعاملات الإلكترونية والجرائم المرتبطة بها.

خطة الدراسة

وانطلاقاً من ذلك، تم تقسيم هذه الدراسة إلى مبحثين رئيسيين: خُصص المبحث الأول لبيان الإطار المفاهيمي للتجارة الإلكترونية، من حيث تعريفها وخصائصها وأهم فوائدها بالنسبة للشركات والزبائن، في حين خُصص المبحث الثاني لدراسة الجرائم الواقعة على التجارة الإلكترونية، وذلك من خلال تناول الاعتداء على التوقيع الإلكتروني، وجرائم الاستيلاء على أرقام البطاقات الائتمانية، بوصفها من أبرز الصور العملية للجرائم المرتبطة بهذا النوع من المعاملات.

المبحث الأول: ماهية التجارة الإلكترونية

أدى التطور المتسارع في تقنيات المعلومات والاتصالات، واتساع نطاق استخدام الوسائط الرقمية في مختلف مجالات الحياة، إلى إحداث تحول جوهري في الأنماط التقليدية للنشاط الاقتصادي، ولم يكن النشاط التجاري بمنأى عن هذه التحولات، بل كان من أكثر المجالات استجابة لهذه التحولات وتكيفاً معها.

وقد أسهمت البيئة الرقمية في إعادة تشكيل وسائل عرض السلع والخدمات، وطرق التفاوض والتعاقد، وآليات الدفع والتنفيذ، بما أفرز نموذجاً تجارياً جديداً يقوم على استخدام الوسائط الرقمية في إدارة المعاملات التجارية وإنجازها.

وقد أصبحت التجارة الإلكترونية إحدى أبرز صور التجارة الحديثة، لما توفره من مزايا عملية واقتصادية تتمثل في اختصار الوقت والجهد، وخفض تكاليف التشغيل، وتوسيع نطاق الأسواق، وإتاحة الوصول إلى المستهلكين في مختلف الدول، فضلاً عن المرونة العالية التي

تميزها مقارنة بالتجارة التقليدية، كما أن اعتمادها على البنية التقنية والشبكات المفتوحة جعلها أداة رئيسة في تنشيط التجارة الداخلية والدولية، وعاملاً مؤثراً في تعزيز التنافسية وتحفيز الابتكار الاقتصادي.

ومع ذلك، فإن هذا التطور لم يقتصر أثره على الجانب الاقتصادي فحسب، بل امتد إلى المجال القانوني، إذ فرضت التجارة الإلكترونية تحديات جديدة تتعلق بتكييفها القانوني، وتحديد طبيعة العلاقات الناشئة عنها، وبيان القواعد الواجبة التطبيق على المعاملات التي تتم في بيئة افتراضية تتجاوز الحدود الجغرافية التقليدية.

وعليه، أصبح من الضروري الوقوف على ماهية التجارة الإلكترونية من خلال تحديد مفهومها وخصائصها، ثم بيان ما تحققه من فوائد على مستوى الأفراد والمؤسسات والأسواق.

المطلب الأول: مفهوم التجارة الإلكترونية

أصبحت التجارة الإلكترونية من المفاهيم المحورية في البيئة الاقتصادية المعاصرة، نتيجة الانتشار الواسع لتقنيات الاتصال الحديثة، واعتماد الأفراد والمؤسسات على الوسائط الرقمية في إنجاز المعاملات التجارية بمختلف صورها، وقد ساهم التطور التقني المتسارع، واتساع نطاق استخدام شبكة الإنترنت، في انتقال جانب كبير من الأنشطة التجارية من صورتها التقليدية إلى الفضاء الإلكتروني، بما جعل التجارة الإلكترونية واقعاً اقتصادياً وقانونياً لا يمكن تجاوزه⁽⁴⁾.

ولا يقتصر مفهوم التجارة الإلكترونية على كونه وسيلة تقنية لإبرام العقود أو تسويق المنتجات، بل يعكس نمطاً متكاملًا من الممارسات التجارية التي تشمل الإعلان والتفاوض والتعاقد والدفع والتسليم وخدمات ما بعد البيع. وتتم هذه العمليات عبر وسائل إلكترونية تتيح السرعة والمرونة وتجاوز القيود المكانية والزمانية، الأمر الذي أسهم في اتساع نطاق المعاملات التجارية الرقمية وتطورها. ولذلك، تقتضي الإحاطة بمفهوم التجارة الإلكترونية الوقوف على التعريفات التي قُدمت لها في الفقه والتشريعات والاتفاقيات ذات الصلة، ثم بيان الخصائص التي تميزها عن التجارة التقليدية وتبرز طبيعتها الخاصة في المجالين القانوني والاقتصادي.

الفرع الأول: تعريف التجارة الإلكترونية

يثير تعريف التجارة الإلكترونية إشكالاً دقيقاً يرتبط بطبيعتها المركبة؛ فهي ليست مجرد صورة حديثة من صور البيع والشراء، وإنما تمثل نمطاً متكاملًا من التعامل التجاري الذي يجري عبر وسائل إلكترونية، بدءاً من عرض السلع والخدمات والتفاوض بشأنها، مروراً بإبرام العقود وتنفيذ الالتزامات، وانتهاءً بوسائل الدفع والتسليم الإلكتروني أو المادي بحسب طبيعة محل المعاملة. ولذلك، فإن تحديد مفهومها لا يقتصر على الجانب التقني، بل يمتد إلى بيان آثارها القانونية، ولا سيما ما يتعلق بالإثبات، والتعاقد، وحماية المستهلك، والمسؤولية، ومواجهة صور الاعتداء التي قد تقع في بيئتها الرقمية.

وقد تعددت الاتجاهات في تعريف التجارة الإلكترونية تبعاً لاختلاف زاوية النظر إليها؛ فبعض التعريفات ركزت على الوسيلة المستخدمة في إتمام المعاملة، أي الوسائل الإلكترونية وشبكات الاتصال، في حين اتجهت تعريفات أخرى إلى التركيز على موضوع النشاط التجاري ذاته، من حيث كونه يشمل إنتاج السلع والخدمات وتسويقها وتوزيعها والوفاء بثمانها عبر الوسائل الرقمية⁽⁵⁾، كما أن التشريعات والهيئات الدولية لم تعتمد تعريفاً موحداً جامعاً، وإنما تناولت التجارة الإلكترونية من خلال مفاهيم قريبة منها، كرسالة البيانات، والعقد الإلكتروني، والمعاملة الإلكترونية، وخدمات مجتمع المعلومات.

ويقتضي بيان مفهوم التجارة الإلكترونية التمييز بين اتجاهين رئيسين: أولهما الاتجاه القانوني، الذي يستند إلى ما ورد في التشريعات الوطنية والنماذج الدولية ذات الصلة، وثانها الاتجاه الفقهي، الذي يحاول تقديم تعريف أكثر مرونة واتساعاً لطبيعة هذا النشاط في ضوء تطوره العملي والتقني.

أولاً: التعريف القانوني للتجارة الإلكترونية

نظراً لحدائث مفهوم التجارة الإلكترونية وتعدد تطبيقاته العملية، لم يستقر الفقه أو التشريع على تعريف موحد جامع لها، الأمر الذي دفع عدداً من الهيئات الدولية والتشريعات الوطنية إلى محاولة وضع تعريفات قانونية تُبرز عناصرها الأساسية وتحدد نطاقها، وقد اختلفت هذه التعريفات بحسب الغاية التنظيمية لكل جهة وبحسب زاوية النظر إلى النشاط الإلكتروني محل التنظيم.

(4) - Chukurna, O., Tardaskina, T., Chaikovska, M., Nitsenko, V., Pankovets, L., & Kofman, V. (2024). Transformation of E-Commerce Business Models in the Digital Economy. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, (5), p. 192 – 193. <https://doi.org/10.33271/nvngu/2024-5/192>

(5) - Laudon, K. C., & Traver, C. G. (2023). *E-commerce 2023 – 2024: Business, Technology, Society* (18th ed.) Pearson, pp. 40 – 41.

فقد عرفت منظمة التعاون والتنمية الاقتصادية التجارة الإلكترونية بأنها جميع أشكال المعاملات المرتبطة بالأنشطة التجارية، سواء كانت منظمة أو فردية، والتي تتم استناداً إلى معالجة البيانات الرقمية أو تبادلها أو نقلها، بما في ذلك النصوص والأصوات والصور، ويُستفاد من هذا التعريف اتساع نطاق التجارة الإلكترونية ليشمل مختلف الأنشطة التجارية التي تعتمد على الوسائط الرقمية في إنجازها⁽⁶⁾. كما أن لجنة الأمم المتحدة للقانون التجاري الدولي (الأونسيترال)، وإن لم تضع تعريفاً مباشراً للتجارة الإلكترونية في قانونها النموذجي لسنة 1996، فإنها أرست الأساس المفاهيمي لها من خلال تعريف رسالة البيانات بأنها المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة، وهو ما يمثل البنية القانونية التي تقوم عليها المعاملات التجارية الإلكترونية⁽⁷⁾. وعرفت منظمة التجارة العالمية التجارة الإلكترونية بأنها إنتاج السلع والخدمات وتسويقها وبيعها وتوزيعها من خلال شبكات الاتصالات، وهو تعريف يركز على الوظائف الاقتصادية والتجارية التي تمارس عبر البيئة الرقمية⁽⁸⁾. وفي السياق الأوروبي، اتجه التنظيم الأوروبي إلى ربط التجارة الإلكترونية بفكرة التعاقد عن بُعد وتقديم خدمات مجتمع المعلومات عبر المنصات الرقمية، بما يعكس الطبيعة العابرة للمكان التي تميز هذا النوع من التعاملات⁽⁹⁾. وعلى مستوى التشريعات العربية، عرّف القانون التونسي المتعلق بالمبادلات والتجارة الإلكترونية رقم (83) لسنة 2000 التجارة الإلكترونية بأنها العمليات التجارية التي تتم عبر المبادلات الإلكترونية. كما نص مشروع قانون التجارة الإلكترونية المصري في المادة رقم (1) على أنها تبادل السلع والخدمات عن طريق وسيط إلكتروني. وكذلك عرّف تشريع المعاملات التجارية الإلكترونية رقم (2) لسنة 2002 في إمارة دبي التجارة الإلكترونية بأنها المعاملات التجارية التي تتم بواسطة المراسلات الإلكترونية. أما في التشريع الفلسطيني، فلا يوجد تنظيم خاص مستقل يُعرّف التجارة الإلكترونية تعريفاً مباشراً، إلا أن القرار بقانون رقم (15) لسنة 2017 بشأن المعاملات الإلكترونية تناول بعض مفاهيمها الأساسية، ومن ذلك تعريف العقد الإلكتروني بأنه الاتفاق الذي ينعقد بين شخصين أو أكثر بوسائل أو وسائط إلكترونية، وهو ما يمكن أن يشكل أساساً تشريعياً لتنظيم المعاملات التجارية التي تتم في البيئة الرقمية⁽¹⁰⁾. ويلاحظ من مجموع هذه التعريفات أنها، رغم اختلاف صياغاتها، تتفق في اعتبار التجارة الإلكترونية امتداداً للنشاط التجاري التقليدي، إلا أنها تتميز عنه باستخدام الوسائل الرقمية كأداة رئيسة لإبرام المعاملات وتنفيذها.

ثانياً: التعريف الفقهي للتجارة الإلكترونية

إلى جانب التعريفات التشريعية والرسمية، سعى الفقه القانوني إلى تقديم تعريفات أكثر اتساعاً ومرونة للتجارة الإلكترونية، انطلاقاً من الطبيعة المتجددة لهذا المفهوم وصعوبة حصره في صورة قانونية جامدة. فقد عرّف بعض الفقه التجارة الإلكترونية بأنها جميع المعاملات التي تتم عبر شبكة الإنترنت، ولو لم تتوافر فيها الصفة التجارية بالمعنى التقليدي، وإن كان الغالب أن ترتبط بتقديم سلعة أو خدمة من جانب مورد محترف أو تاجر⁽¹¹⁾. ويؤخذ من هذا الاتجاه اتساع مفهوم التجارة الإلكترونية ليشمل مختلف التعاملات التي تتم عبر البيئة الرقمية. وعرف اتجاه آخر التجارة الإلكترونية بأنها عمليات الإعلان عن السلع والخدمات، والتعريف بها، والتفاوض بشأنها، ثم إبرام عقود بيعها وشراؤها، وسداد مقابلها عبر شبكات الاتصال المختلفة، سواء عبر الإنترنت أو غيرها من الشبكات الإلكترونية⁽¹²⁾. كما ذهب بعض الفقه إلى تعريفها بأنها إنتاج السلع والخدمات وتوزيعها وتسويقها وبيعها أو تسليمها للمستهلك من خلال الوسائط الإلكترونية، ويركز هذا التعريف على الوظيفة الاقتصادية الكاملة للتجارة الإلكترونية، لا على مجرد مرحلة التعاقد.

(6) - هادي مسلم يونس البشكاني، التنظيم القانوني للتجارة الإلكترونية، دار الكتب والبرمجيات، مصر، سنة 2009، ص 30.

(7) - United Nations Commission on International Trade Law. (1999). UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, with additional Article 5 bis as adopted in 1998. Art. 2(a), p. 4.

(8) - نضال إسماعيل برهم، غازي أبو عرابي، أحكام عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، سنة 2005، ص 15.

(9) - European Parliament and Council of the European Union. (2000). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Official Journal of the European Communities, L 178, 1 – 16, Recitals 17 – 19, art. 2(a).

(10) - دولة فلسطين. (2017). قرار بقانون رقم (15) لسنة 2017 بشأن المعاملات الإلكترونية، الوقائع الفلسطينية، العدد 14، المادة (1).

(11) - عامر محمود الكسواني، التجارة عبر الحاسوب، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، سنة 2008، ص 53.

(12) - أمانج رحيم أحمد، التراضي في العقود الإلكترونية عبر شبكة الانترنت، دار وائل للنشر، الطبعة الأولى، الأردن، سنة 2011، ص 39.

ويرى اتجاه فقهي آخر أن التجارة الإلكترونية هي كل المبادلات التجارية التي تعتمد على تبادل المعلومات عبر شبكات الاتصال السلكية أو اللاسلكية، سواء تمت عبر الإنترنت أو عبر غيره من الوسائل التقنية الحديثة⁽¹³⁾. ويتميز هذا الاتجاه بتركيزه على البنية المعلوماتية كأساس للعملية التجارية.

ويُستفاد من مجمل التعريفات الفقهية أنها تتسم بمرونة أكبر من التعريفات التشريعية، إذ تسعى إلى استيعاب التطور التقني المستمر وعدم قصر التجارة الإلكترونية على وسيلة تقنية بعينها أو صورة تعاقدية محددة.

ثالثاً: التعريف الراجح للتجارة الإلكترونية

في ضوء ما تقدم من تعريفات قانونية وفقهية، يمكن القول إن التجارة الإلكترونية هي: مجموعة المعاملات والأنشطة ذات الطبيعة التجارية التي تتم كلياً أو جزئياً عبر المنصات الرقمية وشبكات الاتصال، وتشمل عرض السلع والخدمات والتفاوض بشأنها وإبرام العقود وتنفيذ الالتزامات والوفاء بالمقابل المالي، وذلك دون اشتراط التواجد المادي المتزامن لأطرافها. ويمتاز هذا التعريف بأنه يجمع بين العناصر الجوهرية للتجارة الإلكترونية، من حيث طبيعة النشاط، والوسيلة المستخدمة، والمراحل التي تمر بها المعاملة، والطابع غير المادي للعلاقة بين الأطراف، كما أنه تعريف مرن يسمح باستيعاب التطبيقات المستحدثة، مثل الأسواق الرقمية، والمنصات التجارية، والتطبيقات الذكية، ووسائل الدفع الإلكتروني الحديثة. وعليه، فإن التجارة الإلكترونية لا تمثل قطيعة مع التجارة التقليدية، وإنما تعد تطوراً وظيفياً في وسائل ممارستها وآليات تنفيذها، مع ما يستتبع ذلك من آثار قانونية خاصة تستوجب تنظيمها تشريعياً ملائماً. ولا تتبنى هذه الدراسة هذا التعريف بوصفه تعريفاً وصفيّاً للتجارة الإلكترونية فحسب، بل بوصفه مدخلاً لتحليل المخاطر الجزائية التي تنشأ عن انتقال العلاقة التجارية إلى بيئة رقمية تقوم على البيانات والتوثيق الإلكتروني والدفع غير المادي. فكل عنصر من عناصر هذا التعريف، من عرض السلع والخدمات إلى الدفع والتنفيذ، قد يشكل نقطة تعرض قانوني أو تقني يمكن أن تستغل في ارتكاب جرائم تمس الثقة في المعاملات الإلكترونية.

الفرع الثاني: خصائص التجارة الإلكترونية

تتميز التجارة الإلكترونية بخصائص قانونية واقتصادية وتقنية جعلتها تختلف عن التجارة التقليدية في الوسائل والآليات وآثار التعامل، فمع أن الغاية النهائية في الحالتين تتمثل في تبادل السلع والخدمات وتحقيق المنفعة الاقتصادية، إلا أن البيئة الرقمية أفرزت سمات جديدة تتصل بطريقة التعاقد، ووسائل التنفيذ، وطبيعة الإثبات، ومدى انتشار الأسواق، وسرعة إنجاز المعاملات. وتبرز أهمية هذه الخصائص في أنها تكشف الأساس الذي يبرر إخضاع التجارة الإلكترونية لقواعد قانونية تتلاءم مع طبيعتها الخاصة، كما تفسر كثيراً من الإشكالات العملية التي ثور بشأن حماية المتعاملين، وحجية المحررات الإلكترونية، والاختصاص القضائي، وأمن البيانات، وحماية المستهلك في البيئة الرقمية.

وفي ضوء ذلك، يمكن بيان أبرز خصائص التجارة الإلكترونية على النحو الآتي:

1. غياب العلاقة المباشرة بين الأطراف: تقوم التجارة الإلكترونية غالباً بين أطراف لا يجمعهم وجود مادي في مجلس واحد، إذ يتم التفاوض والتعاقد وتبادل الإرادة عبر وسائل الاتصال الإلكترونية من دون لقاء مباشر بين البائع والمشتري، ويحل النظام التقني محل الاتصال الشخصي التقليدي، بحيث تصبح المنصات الرقمية والتطبيقات ومواقع الويب هي الوسيط الرئيس في إتمام المعاملة. وتُعد هذه السمة من أبرز الفوارق بين التجارة الإلكترونية والتجارة التقليدية⁽¹⁴⁾.
2. إمكان تسليم المنتجات إلكترونياً: تتيح التجارة الإلكترونية، في بعض صورها، تسليم محل المعاملة بطريق إلكتروني مباشر، ولا سيما بالنسبة للمنتجات الرقمية غير المادية، مثل البرامج الحاسوبية، والكتب الإلكترونية، والملفات الإعلامية، والخدمات الرقمية المختلفة. ويمثل ذلك تطوراً نوعياً في مفهوم التسليم، إذ لم يعد مقصوراً على المناولة المادية للسلع التقليدية⁽¹⁵⁾.
3. كثافة المعلومات وشفافية السوق: تقوم البيئة الرقمية على التدفق المستمر للمعلومات، بما يتيح للمستهلكين والمتعاملين الوصول السريع إلى بيانات الأسعار والمواصفات وشروط التعاقد وتجارب المستخدمين والمقارنات بين المنتجات والخدمات، الأمر الذي يعزز الشفافية ويوسع قدرة المستهلك على اتخاذ القرار الاقتصادي⁽¹⁶⁾.

(13) - محمد مأمون سليمان، التحكيم الإلكتروني، دار الجامعة الجديدة، مصر، سنة 2011، ص 39.

(14) - مرجع سابق، (2023)، Laudon, K. C., & Traver, C. G.، ص 40 – 41.

(15) - خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، الدار الجامعية، الطبعة الأولى، مصر، سنة 2007، ص 63.

(16) - مرجع سابق، (2023)، Laudon, K. C., & Traver, C. G.، ص 50 – 52.

4. **السرعة في إنجاز المعاملات:** تتسم التجارة الإلكترونية بدرجة عالية من السرعة في عرض المنتجات وإبرام العقود وتنفيذ عمليات الدفع وتأكيد الطلبات، نتيجة الاعتماد على الأنظمة الإلكترونية والمعالجة الفورية للبيانات، بما يؤدي إلى تقليص الزمن التجاري وزيادة الكفاءة التشغيلية⁽¹⁷⁾.
 5. **الطبيعة الدولية والعابرة للحدود:** تُمارس التجارة الإلكترونية عبر شبكة عالمية مفتوحة، الأمر الذي يجعلها بطبيعتها غير مقيدة بالحدود الجغرافية للدول. فالتاجر قد يوجد في دولة، والمستهلك في دولة أخرى، والخادم الإلكتروني في دولة ثالثة، بينما تتم عملية الدفع عبر نظام مالي دولي، وهو ما يثير إشكالات قانونية تتعلق بالاختصاص والقانون الواجب التطبيق والتنفيذ العابر للحدود.
 6. **تراجع الاعتماد على الوثائق الورقية:** في البيئة الإلكترونية، تحل الرسائل الرقمية والمحركات الإلكترونية وسجلات البيانات محل المستندات الورقية التقليدية، وقد أدى ذلك إلى بروز وسائل حديثة في الإثبات، مثل التوقيع الإلكتروني والسجلات الرقمية ورسائل البيانات، بما عزز الاعتراف القانوني بالأدلة الإلكترونية⁽¹⁸⁾.
 7. **تعزيز القدرة التنافسية وتوسيع الأسواق:** أتاحت التجارة الإلكترونية للمشروعات فرصاً أوسع للوصول إلى الأسواق المحلية والدولية بتكاليف أقل، كما أسهمت في زيادة المنافسة وسهولة الوصول إلى المستهلكين عبر الوسائط الرقمية.
 8. **التطور المستمر والمرونة التقنية:** ترتبط التجارة الإلكترونية بالتغير المستمر في الوسائل التقنية، مثل تطبيقات الهواتف الذكية والمنصات الرقمية ووسائل الدفع الحديثة، الأمر الذي يقتضي مرونة تشريعية وتنظيمية قادرة على مواكبة تطور الوسائل الرقمية⁽¹⁹⁾.
- ولا تُعد هذه الخصائص مجرد سمات تقنية أو اقتصادية للتجارة الإلكترونية، بل يترتب عليها آثار قانونية مباشرة تمس قواعد الاختصاص والإثبات والحماية الجزائية؛ فغياب العلاقة المادية بين الأطراف، والطابع العابر للحدود، واعتماد المعاملات على البيانات الرقمية، كلها عوامل تحدّ من فعالية التصورات التقليدية للحماية القانونية، وتُفسّر - في جانب منها - تنامي الصعوبات المرتبطة بملاحقة الجرائم الإلكترونية وإثباتها.
- ولا تكمن أهمية هذه الخصائص في بعدها الاقتصادي أو التقني فقط، بل في أثرها المباشر على نطاق الحماية الجزائية؛ فغياب العلاقة المباشرة بين الأطراف يضعف التحقق من الهوية، والطابع العابر للحدود يعقّد الاختصاص والتعاون القضائي، والاعتماد على البيانات الرقمية يجعل محل الاعتداء غير مادي وقابلًا للنسخ والتداول. وبذلك، تصبح خصائص التجارة الإلكترونية ذات صلة مباشرة ببنية الجريمة الإلكترونية ذاتها.
- وبعد بيان الخصائص المميزة للتجارة الإلكترونية، يتعين الانتقال إلى بيان ما تحققه من فوائد وآثار إيجابية على الشركات والمستهلكين والأسواق، وهو ما سيتم تناوله في المطلب التالي.

المطلب الثاني: فوائد التجارة الإلكترونية

أصبحت التجارة الإلكترونية من الظواهر الاقتصادية المؤثرة في بنية الأسواق الحديثة. ولم تعد أهميتها مقصورة على كونها وسيلة بديلة لإجراء المعاملات التجارية، بل غدت أداة استراتيجية تسهم في تطوير النشاط الاقتصادي وتحسين كفاءة المبادلات وتوسيع نطاق الوصول إلى السلع والخدمات. ويرجع ذلك إلى ما توفره من مزايا عملية وتقنية جعلتها خياراً رئيساً للأفراد والمؤسسات في البيئة الرقمية المعاصرة.

وتتعدد فوائد التجارة الإلكترونية بتعدد الأطراف المستفيدة منها؛ فهي تحقق مزايا مباشرة للشركات من حيث خفض التكاليف، وتوسيع الأسواق، وتحسين إدارة العمليات، كما توفر مزايا مهمة للمستهلكين من حيث سهولة الوصول إلى المنتجات، وحرية الاختيار، وتوفير الوقت والجهد، وتعزيز القدرة على المقارنة بين البدائل المتاحة، ويمتد أثرها كذلك إلى الاقتصاد والمجتمع من خلال دعم الابتكار، وتنشيط المنافسة، وتحفيز التحول الرقمي.

وتكمن الأهمية القانونية والعملية لبحت فوائد التجارة الإلكترونية في أن هذه الفوائد تمثل أحد أبرز الدوافع التي دفعت التشريعات إلى الاعتراف بالمعاملات الإلكترونية وتنظيمها، والعمل على تعزيز الثقة في البيئة الرقمية، وتوفير الحماية اللازمة للمتعاملين فيها.

(17) - المرجع السابق، ص 49، 51، 56.

(18) - محمود حسين الوادي، بلال محمود الوادي، المعرفة والإدارة الإلكترونية، دار الصفاء للنشر والتوزيع، الطبعة الأولى، الأردن، سنة 2011، ص 93 - 95.

(19) - مرجع سابق، (2023)، Laudon, K. C., & Traver, C. G.، ص 52 - 53، 56.

الفرع الأول: فوائد التجارة الإلكترونية بالنسبة للشركات

حققت التجارة الإلكترونية تحولاً جوهرياً في بيئة الأعمال المعاصرة، إذ وفّرت للشركات أدوات جديدة لإدارة النشاط التجاري وتسويق المنتجات والتواصل مع العملاء وإنجاز المعاملات بكفاءة أعلى من الأساليب التقليدية، ولم تعد الاستفادة من التجارة الإلكترونية مقتصورة على الشركات الكبرى، بل امتدت إلى المشروعات الصغيرة والمتوسطة التي أصبحت قادرة، بفضل الوسائط الرقمية، على النفاذ إلى الأسواق ومنافسة الفاعلين الاقتصاديين بتكاليف أقل ومرونة أكبر.

وتتجلى أهمية التجارة الإلكترونية بالنسبة للشركات في كونها لا تمثل مجرد قناة للبيع، وإنما منظومة متكاملة تشمل التسويق، وخدمة العملاء، وإدارة البيانات، وتوسيع قاعدة المستهلكين، وتحسين الكفاءة التشغيلية، ورفع القدرة التنافسية. ومن أبرز هذه الفوائد ما يأتي:

1. خفض التكاليف التشغيلية والتسويقية: تسهم التجارة الإلكترونية في تقليص عدد كبير من النفقات التي تلازم النشاط التجاري التقليدي، مثل تكاليف استئجار المواقع التجارية، والمصاريف المرتبطة بالعرض المادي للمنتجات، وكلفة الإعلانات التقليدية واسعة النطاق، كما أن إدارة المنصات الإلكترونية وصيانتها غالباً ما تكون أقل تكلفة من تشغيل الفروع التقليدية، الأمر الذي ينعكس إيجاباً على كفاءة الإنفاق وتحسين هامش الربح⁽²⁰⁾.
2. توسيع نطاق الأسواق والوصول إلى عملاء جدد: تمكن التجارة الإلكترونية الشركات من تجاوز النطاق الجغرافي المحلي والوصول إلى أسواق وطنية وإقليمية ودولية من خلال المنصات الرقمية، فالموقع الإلكتروني أو التطبيق التجاري يتيح عرض المنتجات والخدمات على مدار الساعة أمام جمهور واسع، دون أن يكون النشاط مقيداً بالموقع الجغرافي للمشروع أو بعدد فروعه⁽²¹⁾.
3. تطوير قنوات التواصل وإدارة العلاقة مع العملاء والشركاء: توفر الوسائط الإلكترونية قنوات مباشرة وسريعة للتواصل مع العملاء والموردين والشركاء التجاريين، مثل البريد الإلكتروني، والدردشة الفورية، وخدمات الدعم الرقمي، ومنصات التواصل المختلفة، ويساعد ذلك في بناء علاقات أكثر استقراراً، وسرعة الاستجابة للاستفسارات، وتحسين تجربة العميل، وتبادل المعلومات التجارية بكفاءة أعلى.
4. تسريع دورة الأعمال وإنجاز المعاملات: تُخفض التجارة الإلكترونية المدة الزمنية الفاصلة بين عرض المنتج، وإتمام الطلب، وتحصيل المقابل المالي، والشروع في إجراءات التسليم أو تقديم الخدمة، كما يسهم التشغيل الآلي للعمليات التجارية، مثل معالجة الطلبات، وإدارة البيانات، وأنظمة الدفع الإلكتروني، في تسريع دورة العمل والحد من التأخير الإداري⁽²²⁾.
5. التسويق المستمر دون انقطاع زمني: تتيح التجارة الإلكترونية للشركات عرض منتجاتها وخدماتها بصورة مستمرة دون التقيد بساعات عمل محددة، بما يزيد من فرص الوصول إلى العملاء وتوسيع نطاق النشاط التجاري.
6. تحسين السمعة التجارية وبناء العلامة التجارية: يسهم الحضور الرقمي المنظم وجودة الخدمات الإلكترونية في تعزيز السمعة التجارية للشركات وبناء الثقة لدى المستهلكين، وهو ما أصبح عنصراً مؤثراً في القدرة التنافسية في الأسواق الرقمية⁽²³⁾.
7. زيادة القدرة التنافسية: أتاحت التجارة الإلكترونية للشركات أدوات فعالة لمنافسة المنشآت الأخرى من خلال سرعة الاستجابة، وتحسين الأسعار، وتخصيص العروض، وتحليل سلوك المستهلكين، وتطوير الخدمات، كما ساعدت على تقليص الفجوة بين الشركات الكبيرة والصغيرة من حيث إمكان الوصول إلى الجمهور.
8. الاستفادة من البيانات في اتخاذ القرار: توفر التجارة الإلكترونية كمّاً كبيراً من البيانات المتعلقة بتفضيلات العملاء، وأنماط الشراء، والمنتجات الأكثر طلباً، ومواسم النشاط التجاري، وتمثل هذه البيانات مورداً استراتيجياً يساعد الإدارة في تطوير الخطط التسويقية، وتحسين المخزون، ورفع جودة الخدمات.
9. المرونة في إدارة الأعمال: تمنح البيئة الرقمية الشركات مرونة أكبر في تحديث المنتجات والأسعار وإدارة الحملات التسويقية والاستجابة السريعة لتغيرات السوق مقارنة بالأنشطة التقليدية.
10. رفع مستوى رضا العملاء: تسهم التجارة الإلكترونية في رفع مستوى رضا العملاء من خلال سهولة الوصول إلى الخدمات وسرعة الاستجابة وتعدد وسائل التواصل والدعم الفني⁽²⁴⁾.

(20) - ناصر خليل، التجارة والتسويق الإلكتروني، دار أسامة للنشر والتوزيع، الطبعة الأولى، الأردن، سنة 2009، ص32.

(21) - مرجع سابق، (2023) Laudon, K. C., & Traver, C. G.، ص 49 – 50.

(22) - المرجع السابق، ص 49، 51، 56.

(23) - المرجع السابق، ص 49، 51 – 52.

(24) - مرجع سابق، ناصر خليل، ص 33.

ويتضح من ذلك أن التجارة الإلكترونية أصبحت عنصراً جوهرياً في تطوير الأداء المؤسسي وتعزيز استدامة الشركات في الأسواق الحديثة، الأمر الذي يفسر اتجاه عدد متزايد من المنشآت إلى الاستثمار في التحول الرقمي وتبني نماذج الأعمال الإلكترونية. غير أن هذه المزايا، بقدر ما تعزز الاعتماد على التجارة الإلكترونية، تؤدي في المقابل إلى توسيع نطاق المخاطر المرتبطة بالمعاملات الرقمية، إذ يزداد الاعتماد على وسائل الدفع الإلكتروني والتوثيق الرقمي وتبادل البيانات، بما يرفع من احتمالات التعرض للاعتداءات السيبرانية والجرائم التي تستهدف الثقة في البيئة الإلكترونية.

الفرع الثاني: فوائد التجارة الإلكترونية بالنسبة للزبائن

لا تقتصر آثار التجارة الإلكترونية على الشركات والمؤسسات التجارية، بل تمتد بصورة مباشرة إلى الزبائن والمستهلكين، باعتبارهم الطرف الأكثر احتياجاً إلى الحماية والشفافية في المعاملات التجارية، وقد أسهمت البيئة الرقمية في تمكين المستهلك من الوصول إلى خيارات أوسع، ومعلومات أكثر، وخدمات أسرع، بما عزز مركزه التعاقدية مقارنة ببعض صور التعامل التقليدي.

وتتمثل أبرز فوائد التجارة الإلكترونية بالنسبة للزبائن فيما يأتي:

1. تحسين جودة الخدمة المقدمة للمستهلك: أتاحت التجارة الإلكترونية وسائل متعددة للتواصل بين المستهلك ومقدم السلعة أو الخدمة، من خلال المواقع الإلكترونية، والبريد الإلكتروني، والدردشة الفورية، والتطبيقات الذكية، وخدمات الدعم الرقمي. ويسهم ذلك في سرعة تلقي الاستفسارات والشكاوى ومعالجتها، وتقديم المساعدة الفنية، ومتابعة طلبات المستهلك، بما يؤدي إلى تحسين تجربة المستخدم وتعزيز رضاه عن الخدمة المقدمة⁽²⁵⁾.
 2. سهولة الوصول إلى المعلومات: توفر التجارة الإلكترونية للمستهلك قدراً واسعاً من المعلومات المتعلقة بالسلع والخدمات، مثل السعر، والمواصفات، وشروط البيع، وطرق الدفع، وسياسات الاستبدال والإرجاع، وآراء المستخدمين السابقين، وتساعد هذه المعلومات المستهلك على اتخاذ قرار تعاقدية أكثر وعياً، وتحدّ من حالات الغموض أو عدم التوازن المعرفي بينه وبين البائع⁽²⁶⁾.
 3. حرية الاختيار والمقارنة بين البدائل: تمنح التجارة الإلكترونية المستهلك قدرة واسعة على المقارنة بين المنتجات والخدمات والأسعار عبر منصات متعددة، بما يعزز حرية الاختيار واتخاذ القرار.
 4. خفض الأسعار وزيادة فرص الحصول على عروض أفضل: غالباً ما تؤدي التجارة الإلكترونية إلى تقليل بعض تكاليف التشغيل التي يتحملها التجار، وهو ما قد ينعكس على الأسعار المعروضة للمستهلكين، كما أن شدة المنافسة بين المنصات والمتاجر الرقمية تدفع كثيراً من الشركات إلى تقديم خصومات وعروض ترويجية وخيارات دفع متعددة، بما يحقق منفعة اقتصادية للمستهلك.
 5. توفير الوقت والجهد: من أهم مزايا التجارة الإلكترونية بالنسبة للمستهلك أنها تتيح له إتمام المعاملة التجارية دون الحاجة إلى الانتقال إلى المتجر أو التقيد بساعات عمل محددة أو الانتظار في أماكن البيع، فالسوق الإلكترونية متاحة في أي وقت، ويمكن للمستهلك البحث والشراء والدفع ومتابعة الطلب من خلال الوسائل الرقمية، بما يوفر الوقت والجهد ويجعل عملية التسوق أكثر سهولة ومرونة.
 6. تجاوز القيود الجغرافية: تمكن التجارة الإلكترونية المستهلك من الوصول إلى منتجات وخدمات تتجاوز حدود السوق المحلي، بما يوسع نطاق الخيارات المتاحة أمامه.
 7. تعزيز مشاركة المستهلك في تقييم السوق: أتاحت البيئة الرقمية للمستهلك دوراً أكثر فاعلية من خلال تقييم المنتجات والخدمات، ونشر التجارب الشخصية، وتبادل الآراء مع مستخدمين آخرين، وقد غدت هذه التقييمات عاملاً مؤثراً في قرارات الشراء، كما تسهم في دفع الشركات إلى تحسين جودة منتجاتها وخدماتها حفاظاً على سمعتها التجارية⁽²⁷⁾.
- وعلى الرغم من هذه الفوائد، فإن استفادة المستهلك من التجارة الإلكترونية لا تكون كاملة إلا إذا اقترنت ببيئة قانونية آمنة تضمن حماية بياناته الشخصية والمالية، وتكفل شفافية التعاقد، وتوفر وسائل فعالة لمواجهة الغش والاحتيال والاعتداءات الرقمية⁽²⁸⁾، ومن هنا تظهر الصلة الوثيقة بين مزايا التجارة الإلكترونية وبين ضرورة توفير حماية جزائية فعالة لها.

(25) - Pasaribu, F., Sari, W. P., Bulan, T. R. N., & Astuty, W. (2022). The effect of e-commerce service quality on customer satisfaction, trust and loyalty. *International Journal of Data and Network Science*, 6, 1077, 1082. <https://doi.org/10.5267/j.ijdns.2022.8.001>

(26) - نصار محمد الحلامة، التجارة في القانون، دار الثقافة للنشر والتوزيع، الطبعة الأولى، السودان، سنة 2013، ص 72.

(27) - مرجع سابق، (2023)، Laudon, K. C., & Traver, C. G. ص 51 – 52، 57.

(28) - European Data Protection Supervisor. (2021). Tech Dispatch 2/2021 – Card-based payments, pp. 2 – 4. <https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-2021-card-based-payments>

غير أن هذه الفوائد، بقدر ما تعزز انتشار التجارة الإلكترونية، تكشف في الوقت ذاته عن اتساع نطاق المخاطر القانونية المرتبطة بها؛ فكلما زاد الاعتماد على الدفع الإلكتروني والتوثيق الرقمي وتبادل البيانات، اتسعت فرص الاعتداء على وسائل الثقة والدفع. ومن ثم، فإن إبراز فوائد التجارة الإلكترونية في هذه الدراسة لا يهدف إلى العرض الاقتصادي المجرد، بل إلى بيان الخلفية التي تفسر الحاجة إلى حماية جزائية متخصصة.

ويتضح مما تقدم أن التجارة الإلكترونية أصبحت بيئة قانونية واقتصادية متكاملة، تتداخل فيها عناصر التعاقد الإلكتروني والدفع الرقمي والإثبات الإلكتروني. غير أن هذه البيئة أفرزت في المقابل أنماطاً مستحدثة من السلوك الإجرامي تستهدف الثقة في المعاملات الإلكترونية، الأمر الذي يقتضي بحث الجرائم المرتبطة بها في المبحث التالي. وعليه، فإن دراسة التجارة الإلكترونية لا تكتمل بالوقوف عند مزاياها وخصائصها، بل تقتضي بحث الجرائم المرتبطة بها، ولا سيما تلك التي تستهدف وسائل الثقة والتوثيق، كالتوقيع الإلكتروني، أو تمسّ الذمة المالية للمستهلكين والشركات، كجرائم الاستيلاء على بيانات البطاقات الائتمانية، وذلك على النحو الذي سيتم تناوله في المبحث الثاني.

المبحث الثاني: الجرائم الواقعة على التجارة الإلكترونية

تمثل الجريمة، في معناها العام، اعتداءً على مصلحة يراها المشرع جديرة بالحماية الجزائية، فيتدخل لتجريم السلوك الماسّ بها وبيان العقوبة المقررة له، وإذا كانت التجارة التقليدية قد عرفت صوراً متعددة من الجرائم، كالاختيال والتزوير والسرقة وخيانة الأمانة، فإن التجارة الإلكترونية أفرزت صوراً أكثر تعقيداً بسبب اعتمادها على الوسائط الرقمية وشبكات الاتصال وأنظمة الدفع الإلكتروني. وتتميز الجرائم الواقعة على التجارة الإلكترونية بأنها غالباً ما تُرتكب في بيئة غير مادية وعابرة للحدود، كما قد يصعب فيها تحديد الجاني أو مكان ارتكاب الفعل أو القانون الواجب التطبيق. فضلاً عن ذلك، فإن محل الاعتداء قد لا يتمثل في مال مادي بالمعنى التقليدي، وإنما في بيانات أو رموز أو توقيعات إلكترونية أو معلومات مالية ذات قيمة اقتصادية وقانونية.

وقد أدى الطابع العابر للحدود للجرائم السيبرانية إلى تنامي الاتجاه الدولي نحو تعزيز التعاون التشريعي والإجرائي بين الدول، من خلال تطوير اتفاقيات وأطر دولية تهدف إلى تقريب المقاربات التشريعية، وتيسير تبادل المعلومات والأدلة الرقمية، وتعزيز آليات المساعدة القانونية المتبادلة في مجال الجرائم الإلكترونية⁽²⁹⁾.

وتتجلى خطورة هذه الجرائم في أنها لا تقتصر على الإضرار بضحية فردية، بل تمتد إلى تقويض الثقة في المعاملات الإلكترونية ذاتها، وإضعاف اطمئنان المستهلكين والشركات إلى استخدام الوسائل الرقمية في البيع والشراء والدفع والتعاقد. ومن ثم، فإن مواجهة القانونية لهذه الجرائم تقتضي فهم طبيعتها الخاصة، وبيان صورها العملية، ومدى كفاية القواعد الجزائية القائمة لملاحقتها.

المطلب الأول: الاعتداء على التوقيع الإلكتروني

يُعدّ التوقيع، في صورته التقليدية، من أهم الوسائل القانونية التي يُعبر بها الشخص عن إرادته في الالتزام بتصرف قانوني معين، كما يمثل أداة لإسناد المحرر إلى صاحبه وإثبات صدوره عنه، ولذلك ارتبط التوقيع تاريخياً بفكرة الكتابة الورقية، إذ جرى العمل على أن يتم بخط يد صاحبه أو بإمضائه الشخصي على المستند، بما يسمح بتمييز هويته وربط إرادته بمضمون التصرف المثبت في المحرر. ويستعمل مفهوم التوقيع في معنيين متكاملين: أولهما الفعل المادي المتمثل في وضع التوقيع على محرر أو وثيقة تتضمن بيانات معينة، وثانيهما العلامة أو الإشارة التي تدل على شخصية الموقع وتميّزه عن غيره. ومن ثم، فإن التوقيع لا يقتصر على كونه شكلاً ظاهرياً، بل يؤدي وظائف قانونية جوهرية تتمثل في تحديد هوية صاحبه، والتعبير عن رضاه بمضمون التصرف، وإضفاء الحجية على المحرر في الإثبات⁽³⁰⁾. وقد استقر الفقه والقضاء التقليديان على اشتراط الكتابة أو الإمضاء اليدوي في كثير من المعاملات، بوصفه الوسيلة المألوفة للتحقق من صدور الإرادة، إلا أن التطور التقني المتسارع، واتساع نطاق المعاملات التي تتم عبر البيئة الرقمية، أظهر قصور هذا التصور التقليدي عن مواكبة أنماط التعاقد الحديثة، حيث باتت المعاملات التجارية والمالية والإدارية تُبرم عن بُعد، وفي بيئة رقمية لا تتلاءم بطبيعتها مع التوقيع الورقي التقليدي.

(29) - United Nations. (2024). United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (Preamble). United Nations Office on Drugs and Crime. <https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html>

(30) - محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، سنة 2005، ص 235.

ومن هنا برز التوقيع الإلكتروني بوصفه بديلاً وظيفياً للتوقيع التقليدي، يحقق ذات الغايات القانونية المتمثلة في التوثيق، وإسناد التصرف إلى صاحبه، وإثبات الرضا، مع الاعتماد على وسائل تقنية تتناسب مع طبيعة البيئة الرقمية، وقد أدى الاعتراف القانوني المتزايد بهذا النوع من التوقيع إلى اتساع نطاق استخدامه في المعاملات الإلكترونية، الأمر الذي استتبع ظهور صور جديدة من الاعتداءات التي تستهدفه، كالتزوير، والاستعمال غير المشروع، والدخول غير المصرح به إلى الأنظمة المرتبطة به.

الفرع الأول: ماهية التوقيع الإلكتروني

يمثل التوقيع الإلكتروني الأداة القانونية والتقنية التي مكّنت المعاملات الإلكترونية من الانتقال من مجرد تبادل معلومات إلى علاقات تعاقدية منتجة لآثارها القانونية الكاملة، فكما يقوم التوقيع التقليدي بوظيفة إسناد المحرر إلى صاحبه والتعبير عن رضاه، فإن التوقيع الإلكتروني يؤدي الوظائف ذاتها بوسائل رقمية تتلاءم مع طبيعة البيئة الإلكترونية، وتحقق درجات متفاوتة من الأمان والثقة والإثبات⁽³¹⁾.

وقد أدى اتساع نطاق استخدام التوقيع الإلكتروني في المجالات التجارية والمصرفية والإدارية والقضائية إلى تدخل التشريعات الوطنية والمقارنة لتنظيمه، وبيان شروط الاعتداد به، وتحديد صورته المختلفة، وبيان الحماية القانونية المقررة له، كما اهتم الفقه القانوني بتحديد مفهومه وخصائصه وتمييزه عن غيره من وسائل التوثيق والتحقق من الهوية⁽³²⁾.

ويقضي بيان ماهية التوقيع الإلكتروني تناول تعريفه القانوني والفقه، ثم بيان خصائصه وأشكاله التقنية الأكثر شيوعاً، وذلك على النحو الآتي:

أولاً: التعريف القانوني للتوقيع الإلكتروني

حرصت التشريعات المقارنة على وضع تعريفات للتوقيع الإلكتروني تراعي تنوع وسائله التقنية وتؤكد وظائفه القانونية الأساسية، وإن اختلفت الصياغات التشريعية بحسب السياسة التنظيمية لكل نظام قانوني.

ففي التشريع الأمريكي، عُرِف التوقيع الإلكتروني بأنه صوت أو رمز أو عملية إلكترونية مرفقة بسجل أو مرتبطة به منطقياً، ويقوم شخص ما بتنفيذها أو اعتمادها بقصد التوقيع على ذلك السجل. ويكشف هذا التعريف عن اتجاه واسع لا يحصر التوقيع الإلكتروني في صورة تقنية محددة، وإنما يركز على عنصر نية الالتزام وارتباط الوسيلة بالمحرر الإلكتروني⁽³³⁾.

وفي التشريع الفرنسي، عُرِف التوقيع بأنه الوسيلة اللازمة لإتمام التصرف القانوني، والتي تسمح بتحديد هوية من صدر عنه وتعبير عن رضاه بالالتزامات الناشئة عنه، وعندما يكون إلكترونياً يجب أن يتم بوسيلة موثوقة تضمن تحديد هوية الموقع واتصال التوقيع بالمحرر اتصالاً مأموناً. ويظهر من ذلك تركيز المشرع الفرنسي على عنصرَي الهوية والموثوقية التقنية⁽³⁴⁾.

أما التشريع الألماني، فقد ميّز بين التوقيع الإلكتروني العادي والتوقيع الإلكتروني المتقدم، مع تشديد المتطلبات الفنية في الصورة المتقدمة، بحيث يرتبط التوقيع بصاحبه على نحو منفرد، ويتيح التحقق من هويته، ويكشف أي تعديل يطرأ على البيانات محل التوقيع. ويعكس هذا الاتجاه تدرجاً تشريعياً في مستويات الحماية والثقة.

وفي التشريع المصري، عُرِف التوقيع الإلكتروني بأنه ما يوضع على محرر إلكتروني في صورة حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون له طابع منفرد يسمح بتحديد شخص الموقع وتمييزه عن غيره. ويبرز هذا التعريف عنصر التفرد كضمانة قانونية للإسناد الصحيح⁽³⁵⁾.

وفي التشريع الفلسطيني، عُرِف التوقيع الإلكتروني بأنه بيانات إلكترونية مضافة أو ملحقة أو مرتبطة بمعاملة إلكترونية، يكون لها طابع يسمح بتحديد هوية الشخص الذي وقعها وتمييزه عن غيره، بقصد الموافقة على مضمون المعاملة. ويلاحظ أن هذا التعريف يجمع بوضوح

(31) - United Nations Commission on International Trade Law. (2001). UNCITRAL model law on electronic signatures with guide to enactment. Articles 6 – 7.

(32) - Gregušová, D., Halášová, Z., & Peráček, T. (2022). eIDAS regulation and its impact on national legislation: The case of the Slovak Republic. Administrative Sciences, 12(4), Article 187. pp. 1 – 7. <https://doi.org/10.3390/admsci12040187>

(33) - United States Congress. (2000). Electronic Signatures in Global and National Commerce Act, 15 U.S.C, 7006(5).

(34) - French Civil Code. (2016). Article 1367.

(35) - جمهورية مصر العربية. (2004). قانون رقم 15 لسنة 2004 بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، المادة رقم (ج/1).

بين الوظيفة التعريفية للتوقيع، من حيث إسناده إلى صاحبه، والوظيفة الإرادية، من حيث التعبير عن القبول والالتزام بمضمون المعاملة الإلكترونية⁽³⁶⁾.

ويستفاد من مجمل هذه التعريفات أن التشريعات المقارنة اتجهت إلى عدم حصر التوقيع الإلكتروني في تقنية بعينها، وإنما ركزت على وظائفه الأساسية، وهي تحديد الهوية، وإثبات الرضا، وربط الموقع بالمحرر، وتوفير قدر مناسب من الثقة والأمان في المعاملات الإلكترونية.

ثانياً: التعريف الفقهي للتوقيع الإلكتروني

لم يقتصر تحديد مفهوم التوقيع الإلكتروني على النصوص التشريعية، بل أسهم الفقه القانوني في تطوير تعريفات أكثر مرونة تستوعب التطور التقني المستمر وتبرز الأبعاد الوظيفية لهذا التوقيع.

فقد عرّفه جانب من الفقه الفرنسي بأنه مجموعة من الإجراءات أو الوسائل التقنية التي تسمح بتحديد الشخص الذي صدرت عنه البيانات، وتدل على قبوله بمضمون التصرف القانوني المرتبط بها. ويركز هذا الاتجاه على الوظيفة الإجرائية للتوقيع بوصفه أداة للتحقق والإسناد.

كما عرّفه بعض الفقه المصري بأنه كل إشارات أو رموز أو حروف مرخص باستخدامها من الجهة المختصة، وترتبط بالتصرف القانوني ارتباطاً وثيقاً، وتسمح بتمييز صاحبها وتحديد هويته، وتكشف بوضوح عن رضاه بهذا التصرف. ويجمع هذا التعريف بين الجوانب التقنية والتنظيمية والإرادية للتوقيع الإلكتروني⁽³⁷⁾.

ويلاحظ أن التعريفات الفقهية تتسم باتساع أكبر من التعريفات التشريعية، إذ لا تقف عند حدود النصوص القائمة، وإنما تسعى إلى بيان الغاية القانونية من التوقيع الإلكتروني وكيفية تكييفه في ضوء المستجدات التقنية.

ثالثاً: خصائص التوقيع الإلكتروني

1. يتميز التوقيع الإلكتروني بعدد من الخصائص التي تمنحه قيمته القانونية في البيئة الرقمية، ومن أبرزها ما يأتي⁽³⁸⁾:
ارتباطه بمحرر إلكتروني: لا يرد التوقيع الإلكتروني على ورقة مادية، وإنما ينشأ ويرتبط بمحرر أو سجل إلكتروني، ويُقرأ أو يُتحقق منه عبر وسائط تقنية.
2. تحديد هوية الموقع: يؤدي التوقيع الإلكتروني وظيفة تعريفية تتمثل في إسناد التصرف إلى شخص معين وتمييزه عن غيره من المتعاملين.
3. التعبير عن الرضا والالتزام: يمثل التوقيع الإلكتروني قرينة على قبول الموقع بمضمون التصرف القانوني، والالتزام بالآثار الناشئة عنه متى استوفى شروطه القانونية.
4. اعتماده على وسائل تقنية متنوعة: قد يتخذ شكل رموز أو أرقام أو بيانات مشفرة أو خصائص بيومترية أو غيرها من الوسائل التي تسمح بالتحقق من شخصية الموقع.
5. توفير الأمان والثقة: تستند كثير من صور التوقيع الإلكتروني إلى أنظمة تحقق وتشفير وحماية تقنية تحدّ من مخاطر الانتحال أو التعديل غير المشروع، بما يعزز الثقة في المعاملات الإلكترونية⁽³⁹⁾.

رابعاً: أشكال التوقيع الإلكتروني

لا يقتصر التوقيع الإلكتروني على صورة واحدة، بل يتخذ أشكالاً متعددة بحسب الوسيلة التقنية المستخدمة في إنشائه والتحقق منه، ومن أبرزها ما يأتي⁽⁴⁰⁾:

1. التوقيع الكودي أو السري: يقوم على استخدام أرقام أو حروف أو رموز سرية يختارها المستخدم أو تُخصص له، مثل الرقم الشخصي السري (PIN)، ويشيع استعماله في البطاقات الذكية وأنظمة الدفع الإلكتروني⁽⁴¹⁾.

(36) - دولة فلسطين. (2018). قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، المادة (1).

(37) - ثروت عبد الحميد، التوقيع الإلكتروني، مكتبة الجلاء، الطبعة الثانية، المنصورة، سنة 2003، ص 50.

(38) - مرجع سابق، (2001). United Nations Commission on International Trade Law، المادة (2 - 3)، (6)، (10).

(39) - ممدوح محمد علي مبروك، مدى حجية التوقيع الإلكتروني في الإثبات، دار النهضة العربية، القاهرة، سنة 2005، ص 8.

(40) - مرجع سابق، (2001). United Nations Commission on International Trade Law، ص 21 - 24.

(41) - إبراهيم الدسوقي أبو الليل، الجوانب القانونية للمعاملات الإلكترونية، مجلس النشر العلمي، جامعة الكويت، سنة 2003، ص 158.

2. التوقيع البيومتري: يعتمد على الخصائص الجسدية أو السلوكية للشخص، مثل بصمة الإصبع، أو بصمة العين، أو التعرف على الوجه، أو نبذة الصوت. ويتميز بارتفاع مستوى الارتباط بشخصية المستخدم.
3. التوقيع بالقلم الإلكتروني: يتمثل في نقل توقيع الشخص المكتوب بخط اليد إلى محرر إلكتروني باستخدام أجهزة تقنية، مثل القلم الرقعي أو المساح الضوئي.
4. التوقيع الرقمي: يُعد من أكثر الصور تطوراً وأماناً، ويعتمد على تقنيات التشفير والمفاتيح الرقمية للتحقق من هوية الموقع وسلامة البيانات وعدم تعديلها بعد التوقيع. ولذلك يُستخدم على نطاق واسع في المعاملات ذات الأهمية المالية والقانونية. ومن شأن هذه الصور المختلفة أن تؤكد مرونة التوقيع الإلكتروني وقدرته على التكيف مع متطلبات التعامل الحديث، إلا أن هذا التنوع ذاته قد يؤثر صوراً متعددة من الاعتداء والاستعمال غير المشروع، وهو ما يقتضي بحث الجرائم التي تستهدف التوقيع الإلكتروني، وهو ما سيتم تناوله في الفرع التالي.

الفرع الثاني: صور الاعتداء على التوقيع الإلكتروني

يمثل التوقيع الإلكتروني أداة أساسية في إضفاء الثقة والحجية على المعاملات الإلكترونية، لما يؤديه من وظائف قانونية تتعلق بتحديد هوية الموقع، والتعبير عن إرادته، وربط التصرف به، غير أن هذه الأهمية ذاتها جعلته محلاً لاعتداءات إجرامية مستحدثة تستهدف ذاته أو تستهدف الأنظمة التقنية المرتبطة به. وتتميز هذه الاعتداءات بخصوصية نابعة من طبيعتها الرقمية، إذ تُرتكب عبر أنظمة معلوماتية، وتنصب على بيانات غير مادية قابلة للنسخ أو التعديل، مما يثير صعوبات في الاكتشاف والإنابة والتكييف القانوني، فضلاً عن أثرها في تقويض الثقة في المعاملات الإلكترونية. وعليه، تتخذ صور الاعتداء على التوقيع الإلكتروني اتجاهين رئيسين: أولهما المساس بالتوقيع ذاته من خلال التزوير أو التقليد، وثانيهما الاعتداء على الأنظمة أو قواعد البيانات المرتبطة به من خلال الدخول غير المشروع، وهو ما سيتم تناوله تباعاً.

أولاً: تزوير وتقليد التوقيع الإلكتروني

تُعد جريمة تزوير وتقليد التوقيع الإلكتروني من أخطر صور الاعتداء على وسائل الثقة في المعاملات الإلكترونية، لما تنطوي عليه من مساس مباشر بوظيفة التوقيع في إسناد التصرف إلى صاحبه وإثبات صدور الإرادة عنه، وتندرج هذه الجريمة ضمن صور التزوير المعلوماتي الذي يستهدف البيانات أو المحررات الإلكترونية ذات الحجية القانونية. وللإحاطة الكاملة بجريمة تزوير وتقليد التوقيع الإلكتروني، يقتضي الأمر بيان أركانها الأساسية، والوسائل التي يمكن من خلالها ارتكابها، وذلك من خلال تحليل الركن المادي، ووسائل التنفيذ، ثم الركن المعنوي على النحو الآتي:

1. الركن المادي: يقوم الركن المادي في هذه الجريمة على فعل تغيير الحقيقة في محرر إلكتروني أو في بيانات مرتبطة بالتوقيع الإلكتروني، بما من شأنه إحداث أثر قانوني، سواء تم ذلك عن طريق الاصطناع أو التعديل أو المحو أو الإضافة. ويقصد بالتزوير المعلوماتي بوجه عام كل تغيير للحقيقة يرد على مخرجات الحاسب الآلي، سواء كانت هذه المخرجات في صورة ورقية مطبوعة أو في صورة رقمية محفوظة على دعامة إلكترونية، بشرط أن يكون من شأنها إثبات حق أو إنشاء التزام أو تعديل مركز قانوني⁽⁴²⁾. ويمتد محلّ التزوير في هذا السياق ليشمل التوقيع الإلكتروني ذاته، والبيانات المرتبطة به، وكذلك شهادات التصديق الإلكتروني الصادرة عن الجهات المختصة.

وتكمن خطورة هذه الجريمة في أن تزوير شهادات التصديق الإلكتروني – التي تمثل أساس الثقة في التوقيع الإلكتروني – يُعد في أثره معادلاً لتزوير التوقيع ذاته، لما يترتب عليه من إضفاء مشروعية ظاهرية على توقيع غير صحيح، ومن ثم ترتيب آثار قانونية على غير أساس صحيح⁽⁴³⁾.

2. وسائل ارتكاب الجريمة: تتعدد الوسائل التي يمكن من خلالها ارتكاب جرائم التزوير أو الاستعمال غير المشروع للتوقيع الإلكتروني، إذ قد يتم ذلك عبر استهداف الأنظمة المعلوماتية من خلال هجمات التصيد الاحتيالي أو الهندسة الاجتماعية، بما يؤدي إلى الحصول غير المشروع على بيانات الدخول أو بيانات التوثيق الخاصة بالمستخدمين، ومن ثم استخدامها للوصول إلى الحسابات والأنظمة.

(42) - عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، سنة 2002، ص 170.

(43) - عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها الجنائية، دار الفكر الجامعي، الإسكندرية، سنة 2007، ص 306.

الإلكترونية ذات الصلة، كما قد تنطوي هذه الأفعال على استغلال الثغرات التقنية أو ضعف تدابير الحماية، بما يسمح بالاستيلاء على البيانات أو إساءة استخدامها في تنفيذ معاملات إلكترونية دون علم صاحبها أو رضاه⁽⁴⁴⁾.
وللاحظ أن هذه الوسائل تتسم بطابع تقني متطور، الأمر الذي يزيد من صعوبة اكتشافها وتتبع مرتكبيها، في ظل اعتمادها على أساليب إخفاء الأثر واستخدام تقنيات متقدمة تعزز من تعقيد البيئة الإجرامية الرقمية.
ولا يقف أثر هذه الوسائل عند الجانب التقني، بل يمتد إلى التأثير في التكييف القانوني للسلوك الإجرامي وفي مدى كفاية الحماية الجزائية المقررة لوسائل التوثيق الإلكتروني.

ويرى الباحث أن خطورة الاعتداء على التوقيع الإلكتروني لا ترتبط فقط بالضرر الذي قد يلحق بشخص معين، وإنما بكونه يمس الثقة في وسائل التوثيق الإلكتروني ذاتها، وهي الثقة التي تقوم عليها البيئة الرقمية الحديثة بأكملها. ولذلك، فإن الحماية الجزائية للتوقيع الإلكتروني لا ينبغي أن تُفهم بوصفها حماية لتوقيع فردي فحسب، بل بوصفها حماية للبنية الوظيفية للثقة التي تستند إليها المعاملات الإلكترونية.

3. **الركن المعنوي:** تُعد جريمة تزوير التوقيع أو المستند الإلكتروني من الجرائم العمدية التي لا يتصور وقوعها بطريق الخطأ، إذ يتطلب الركن المعنوي فيها توافر القصد الجنائي العام القائم على عنصري العلم والإرادة؛ بحيث ينصرف علم الجاني إلى إدراكه بأنه يُحدث تغييراً غير مشروع في الحقيقة ضمن محرر أو توقيع إلكتروني، وتتجه إرادته إلى إحداث هذا التغيير على نحو متعمد، كما يستلزم قيام هذه الجريمة توافر القصد الجنائي الخاص، المتمثل في نية استعمال المستند أو التوقيع الإلكتروني المزور فيما أُعد له، بما من شأنه إحداث ضرر مادي أو معنوي أو اجتماعي، وهو ما ينسجم مع الطبيعة الخاصة لجرائم التزوير في البيئة الإلكترونية⁽⁴⁵⁾.

ثانياً: الدخول غير المشروع إلى الأنظمة المرتبطة بالتوقيع الإلكتروني

تمثل جريمة الدخول غير المشروع إلى الأنظمة أو قواعد البيانات المرتبطة بالتوقيع الإلكتروني إحدى صور الاعتداء غير المباشر عليه، إذ لا ينصب الفعل على التوقيع ذاته، وإنما على البيئة التقنية التي يتم إنشاؤه أو تخزينه أو التحقق منه من خلالها، وتكمن خطورة هذه الجريمة في أنها تمس البنية التحتية للثقة الرقمية، بما قد يفتح المجال لارتكاب جرائم لاحقة أكثر جسامة، كالتزوير أو الاحتيال الإلكتروني. ولبيان الإطار القانوني لهذه الجريمة على نحو دقيق، يقتضي الأمر تحليلها من خلال عناصرها الجوهرية، وذلك ببحث الركن المادي الذي يتمثل في السلوك الإجرامي، ثم الوقوف على طبيعتها القانونية من حيث تصنيفها ضمن جرائم الخطر، وأخيراً بيان الركن المعنوي الذي يعبر عن القصد الجنائي اللازم لقيامها.

1. **الركن المادي:** يقوم الركن المادي لهذه الجريمة على الدخول غير المصرح به إلى نظام معلوماتي أو قاعدة بيانات تتعلق بالتوقيع الإلكتروني، سواء تم هذا الدخول بقصد الاطلاع على البيانات أو تعديلها أو نسخها أو إتلافها، وكفي لقيام الجريمة تحقق فعل الدخول ذاته دون اشتراط وقوع ضرر فعلي، وهو ما يجعلها من جرائم الخطر التي يُجرّم فيها السلوك لذاته لما ينطوي عليه من تهديد لأمن المعلومات⁽⁴⁶⁾.

2. **الطبيعة القانونية للجريمة:** تتسم هذه الجريمة بعدة خصائص تميزها عن الجرائم التقليدية، إذ تُعد جريمة شكلية لا يُشترط لقيامها تحقق نتيجة ضارة، بل يكفي مجرد ارتكاب فعل الدخول غير المشروع لقيام المسؤولية الجزائية، كما ترتبط هذه الجريمة بحماية أمن وسلامة الأنظمة المعلوماتية بوصفها محلاً للحماية الجنائية، نظراً لما تمثله من بنية أساسية لمعالجة البيانات وتخزينها، بما في ذلك البيانات المرتبطة بالتوقيع الإلكتروني.

1. (44) - Europol. (2020). Internet organized crime threat assessment (IOCTA). Pp. 18 – 21, 27 – 28.

<https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020>

1. (45) - المركز الديمقراطي العربي. (2025). جريمة التزوير في المستندات الإلكترونية الحكومية، مجلة العلوم السياسية والقانون، المجلد 11، العدد

(45)، ص 12 – 13. <https://www.democraticac.de/?p=106476>

(46) - يقصد بالنظام المعلوماتي: مجموعة العناصر التقنية المترابطة التي تشمل الأجهزة والبرمجيات وقواعد البيانات والإجراءات، والتي تعمل معاً على إدخال البيانات ومعالجتها وتخزينها واسترجاعها، بما يتيح إنتاج معلومات ذات دلالة، ومن بينها البيانات المرتبطة بإنشاء التوقيع الإلكتروني أو تخزينه أو التحقق منه.

في حين يقصد بقاعدة البيانات: مجموعة منظمة من البيانات المخزنة إلكترونياً، سواء داخل الحاسب الآلي أو على وسائط تخزين مستقلة، بحيث تكون قابلة للاسترجاع والمعالجة، ومن ذلك البيانات المتعلقة بهوية صاحب التوقيع الإلكتروني، كاسمه ومهنته وبياناته الشخصية، وسائر المعلومات المرتبطة بالتوقيع، والتي يفترض فيها طابع السرية والحماية. للمزيد من التفاصيل، أنظر في: مرجع سابق، عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، ص 296–297.

فضلاً عن ذلك، فإنها غالباً ما تُعد مرحلة تمهيدية لارتكاب جرائم معلوماتية أخرى، كالتزوير أو الاحتيال الإلكتروني، الأمر الذي يبرر تدخل المشرّع لتجريمها في ذاتها باعتبارها من جرائم الخطر التي تستهدف الوقاية قبل وقوع الضرر.

وقد يُفسّر اتجاه بعض التشريعات إلى تجريم مجرد الدخول غير المشروع دون اشتراط تحقق ضرر فعلي بالرغبة في توفير حماية وقائية للبيئة المعلوماتية قبل المساس الفعلي بالبيانات أو الأنظمة، كما يرى الباحث أن هذا الاتجاه يعكس إدراكاً متزايداً للطبيعة الخاصة للبيئة الرقمية، حيث قد يكون مجرد الدخول غير المشروع مقدمة لجرائم أكثر خطورة يصعب احتواؤها بعد وقوعها.

3. **الركن المعنوي:** تُعد هذه الجريمة من الجرائم العمدية، ويتحقق الركن المعنوي فيها بتوافر القصد الجنائي العام بعنصره، إذ يلزم أن يكون الجاني عالماً بعدم مشروعية الدخول إلى النظام المعلوماتي أو بتجاوزه حدود الترخيص الممنوح له، وأن تتجه إرادته – رغم هذا العلم – إلى ارتكاب فعل الدخول أو الاستمرار فيه. ولا يُتصور، في الأصل، وقوع هذه الجريمة بطريق الخطأ، نظراً لطبيعتها التقنية التي تفترض تدخلاً إرادياً واعياً لا يتحقق عادةً إلا من خلال سلوك إيجابي مقصود، بما يعزز وصفها ضمن الجرائم العمدية التي تقوم على تلازم العلم والإرادة في السلوك الإجرامي.

ويتضح مما تقدم أن الاعتداء على التوقيع الإلكتروني لا يقتصر على المساس المباشر به، بل يمتد إلى البيئة التقنية التي يقوم عليها، بما يعكس تطور أنماط الجريمة في هذا المجال، ومن أبرز صور الاعتداء الأخرى التي تستهدف المعاملات الإلكترونية بصورة مباشرة جرائم الاستيلاء على البيانات المالية، ولا سيما أرقام البطاقات الائتمانية، وهو ما سيتم تناوله في المطلب التالي.

المطلب الثاني: جرائم السطو على أرقام البطاقات الائتمانية

تُعد بطاقات الائتمان من أبرز أدوات الوفاء في المعاملات التجارية المعاصرة، وقد ارتبط انتشارها بتطور النشاط المصرفي واتساع نطاق التجارة الإلكترونية، حيث أصبحت وسيلة رئيسة لإتمام عمليات الدفع عبر شبكة الإنترنت، ويقوم نظام هذه البطاقات على فكرة الائتمان، بما يفترض وجود فاصل زمني بين تقديم وسيلة الوفاء من جهة مانح الائتمان وبين استيفاء المقابل المالي لاحقاً، الأمر الذي يعكس طبيعتها المركبة بوصفها أداة دفع وائتمان في آن واحد.

ومع انتقال استخدام بطاقات الائتمان إلى البيئة الرقمية، ولا سيما في إطار التجارة الإلكترونية، برزت إشكالات قانونية وأمنية متزايدة تتعلق بحماية بياناتها. وأصبحت هذه البيانات، وعلى رأسها رقم البطاقة والرموز المرتبطة بها، هدفاً مباشراً لصور متعددة من الاعتداءات الإلكترونية. ويزداد خطر هذه الاعتداءات في ظل الطبيعة المفتوحة لشبكة الإنترنت وغياب التفاعل المادي المباشر بين أطراف المعاملة⁽⁴⁷⁾.

وقد أدى ذلك إلى ظهور ما يُعرف بجرائم الاستيلاء على بيانات البطاقات الائتمانية، وهي من أبرز صور الجرائم الواقعة على التجارة الإلكترونية، لما تنطوي عليه من اعتداء على الذمة المالية للمتعاملين، وإخلال بالثقة في وسائل الدفع الإلكتروني، فضلاً عن ارتباطها بأساليب تقنية متطورة يصعب كشفها وتتبع مرتكبيها.

وتقتضي دراسة هذه الجرائم بيان الأساليب المستخدمة في الاستيلاء على بيانات البطاقات الائتمانية، ثم تحليل أركان الجريمة في ضوء طبيعتها الرقمية، بما يسمح بتحديد نطاق التجريم وبيان مدى كفاية القواعد الجزائية في مواجهتها.

الفرع الأول: الطرق والأساليب

تعتمد آلية الشراء عبر شبكة الإنترنت باستخدام البطاقات الائتمانية على قيام المستهلك بتزويد التاجر ببيانات البطاقة، وعلى رأسها رقمها وتاريخ صلاحيتها، إضافة إلى بيانات أخرى تتعلق بعملية التسليم، ورغم ما توفره هذه الآلية من سهولة وسرعة في إتمام المعاملات، فإنها في المقابل أفرزت نقاط ضعف تقنية استغلها مرتكبو الجرائم المعلوماتية، حيث أصبحت بيانات البطاقات الائتمانية عرضة للاعتراض أو الالتقاط أو الاستعمال غير المشروع، بما يؤدي إلى الاعتداء على الذمة المالية لحامل البطاقة أو الجهة المصدرة لها.

وفي هذا السياق، تعدد الأساليب التي يعتمد عليها الجناة في الاستيلاء على بيانات البطاقات الائتمانية، والتي يمكن تصنيفها – من الناحية التقنية – إلى أساليب اختراق مباشر، وأساليب خداع واحتيال، وأساليب اعتراض البيانات، وذلك على النحو الآتي⁽⁴⁸⁾:

(47) - عماد علي خليل، *التكييف القانوني لإساءة استخدام أرقام البطاقات الائتمانية عبر شبكة الإنترنت*، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، الذي نظّمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بالجامعة ذاتها، خلال الفترة من 1 – 5/5/2000، المجلد الثاني، ص 908.

Laxman, V., Ramesh, N., Jaya Prakash, S. K., & Aluvala, R. (2024). Emerging threats in digital payment and financial crime: A bibliometric review. *Journal of Digital Economy*, 3, pp. 205 – 206, 214 – 218. <https://doi.org/10.1016/j.jdec.2025.04.002>

(48) - عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، 2003، ص 306 – 303.

أولاً: أساليب الاختراق التقني المباشر

تقوم هذه الأساليب على التسلسل غير المشروع إلى الأنظمة المعلوماتية أو قواعد البيانات التي تحتوي على معلومات البطاقات الائتمانية، بهدف استخراجها أو نسخها أو استغلالها، ومن أبرز صورها:

1. الاختراق غير المشروع: يُعد من أخطر الوسائل المستخدمة، حيث يسعى الجاني إلى تجاوز أنظمة الحماية واختراق الخوادم وقواعد البيانات التي تخزن المعلومات المالية للعملاء، مستعيناً ببرامج متقدمة وتقنيات كسر التشفير، بما يمكنه من الوصول إلى بيانات حساسة واستخدامها بصورة غير مشروعة.
2. تفجير أو إغراق المواقع: يقوم هذا الأسلوب على توجيه عدد هائل من الطلبات أو الرسائل إلى النظام المستهدف، بما يؤدي إلى تعطيله أو إضعافه، ومن ثم استغلال حالة الخلل للوصول إلى البيانات المخزنة أو تسريبها⁽⁴⁹⁾.

ثانياً: أساليب الخداع والاحتيال الإلكتروني

- تعتمد هذه الأساليب على استغلال ثقة المستخدمين بدلاً من اختراق الأنظمة مباشرة، ومن أبرزها (50):
1. التصيد الاحتيالي: يقوم الجاني بإنشاء مواقع وهمية تحاكي المواقع الرسمية للبنوك أو الشركات، ثم يطلب من المستخدم إدخال بياناته الشخصية والمالية، ليتم الاستيلاء عليها واستخدامها لاحقاً في عمليات غير مشروعة.
 2. إنشاء المواقع الوهمية: يتم إنشاء منصات إلكترونية مشابهة للمواقع الأصلية، تستقبل طلبات الشراء وبيانات الدفع، بما يؤدي إلى جمع معلومات البطاقات الائتمانية دون علم المستخدمين، وهو ما يهدد الثقة في التجارة الإلكترونية.

ثالثاً: أساليب التلاعب بالبيانات والاعتراض

- تتجه هذه الأساليب إلى اعتراض البيانات أثناء انتقالها أو توليد بيانات مزيفة، ومن أهمها:
1. التنصت على البيانات: يقوم الجاني باعتراض الاتصال بين المستخدم والتاجر، فيتمكن من الاطلاع على البيانات المتبادلة، بما في ذلك معلومات البطاقة، دون علم أي من الطرفين⁽⁵¹⁾.
 2. توليد أرقام البطاقات: يعتمد هذا الأسلوب على استخدام خوارزميات رياضية لتوليد أرقام بطاقات ائتمانية محتملة الصلاحية، ومن ثم استخدامها في عمليات الشراء الإلكترونية⁽⁵²⁾.
- ويتضح مما تقدم أن الأساليب المستخدمة في الاستيلاء على بيانات البطاقات الائتمانية تتسم بالتنوع والتطور المستمر، وتعتمد في جوهرها إما على اختراق الأنظمة التقنية أو استغلال العنصر البشري أو اعتراض البيانات أثناء انتقالها. ويعكس ذلك الطبيعة المركبة لهذه الجرائم وصعوبة مواجهتها بالوسائل التقليدية، ولا تقتصر دلالة هذه الوسائل على بعدها التقني، بل تنعكس مباشرة على التكيف القانوني للسلوك الإجرامي ومدى كفاية الحماية الجزائية المقررة له.
- ويكشف تنوع هذه الوسائل وتطورها المستمر أن جرائم الاستيلاء غير المشروع على بيانات البطاقات الائتمانية لم تعد تقوم على الاعتداء المادي التقليدي على المال، وإنما على استغلال القيمة الاقتصادية التي تمثلها البيانات ذاتها، الأمر الذي يثير تساؤلات قانونية تتعلق بمدى كفاية المفاهيم التقليدية للمال والحيازة والسرقة والاحتيال في استيعاب الطبيعة القانونية الخاصة للبيانات المالية الرقمية. وبناءً على ذلك، يمثل فهم هذه الأساليب خطوة أساسية لبيان الأركان القانونية لجريمة الاستيلاء على أرقام البطاقات الائتمانية، وهو ما سيتم تناوله في الفرع التالي.

الفرع الثاني: أركان جريمة الاستيلاء على أرقام بطاقات الائتمان

تقوم جريمة الاستيلاء على أرقام بطاقات الائتمان على نموذج إجرامي خاص يتصل بالبيئة الرقمية، إذ ينصب الاعتداء على بيانات ذات قيمة مالية وقانونية، ويُرتكب عبر وسائل تقنية متطورة دون حاجة إلى استعمال القوة المادية. ومن ثم، فإن تحليل هذه الجريمة يقتضي الوقوف على أركانها في ضوء خصوصيتها، وذلك ببيان الركن المادي بعناصره، ثم الركن المعنوي، مع إبراز الإشكالات المرتبطة بتكييفها القانوني.

مرجع سابق، عماد على خليل، ص 909.

(49) - المرجع السابق، ص 910.

(50) - European Payments Council. (2024). 2024 payment threats and fraud trends report. (EPC162-24, Version 1.0). pp. 15 – 17.

<https://www.europeanpaymentscouncil.eu>

(51) - المرجع السابق، ص 5.

(52) - على سبيل المثال، من بين هذه المواقع: www.dark-secrets.com

أولاً: الركن المادي

لا يخرج الركن المادي لهذه الجريمة عن القواعد العامة، إذ يتكون من سلوك إجرامي ونتيجة وعلاقة سببية، غير أن لكل عنصر منها خصوصية في البيئة الإلكترونية.

1. **السلوك الإجرامي:** يتمثل السلوك الإجرامي في كل فعل ينطوي على الحصول غير المشروع على بيانات بطاقات الائتمان أو تمكين الغير من الوصول إليها، سواء عبر اختراق الأنظمة وقواعد البيانات وما يتيح ذلك من نفاذ غير مصرح به إلى المعلومات المالية المخزنة. كما قد يتحقق هذا السلوك من خلال إنشاء مواقع وهمية أو استخدام أساليب التصيد الاحتيالي، بقصد خداع المستخدمين ودفعهم إلى الإفصاح عن بياناتهم السرية دون إدراك لطبيعة الجهة التي يتعاملون معها. ويمتد كذلك إلى اعتراض الاتصالات والتنصت على البيانات أثناء انتقالها عبر الشبكات، بما يسمح بالتقاط المعلومات المالية قبل وصولها إلى الجهة المقصودة. وقد يتم السلوك أيضاً باستخدام برمجيات خبيثة تُزرع في أجهزة المستخدمين أو الأنظمة المستهدفة لاستخراج البيانات المالية بصورة خفية ومنظمة⁽⁵³⁾.

ويمتاز هذا السلوك بطبيعته غير العنيفة، إذ يعتمد على الوسائل التقنية وأساليب الاحتيال المعلوماتي بدل الإكراه المادي، وهو ما يميزه عن جرائم السرقة التقليدية.

2. **النتيجة الإجرامية:** تتحقق النتيجة الإجرامية بمجرد تمكن الجاني من الحصول على بيانات البطاقة (رقم البطاقة، تاريخ الانتهاء، رمز التحقق)، بما يمكنه من استعمالها في عمليات دفع أو تحويل مالي. ويثور خلاف فقهي حول مدى اشتراط تحقق استعمال فعلي لهذه البيانات لقيام الجريمة؛ إذ يذهب اتجاه إلى كفاية مجرد الحصول غير المشروع على بيانات البطاقة باعتباره محققاً للنتيجة الإجرامية، في حين يرى اتجاه آخر ضرورة اقتران ذلك بعمل لاحق، كاستعمال البيانات أو التصرف فيها، حتى تتحقق النتيجة الإجرامية بصورة كاملة.

3. **علاقة السببية:** يتطلب قيام الجريمة ثبوت رابطة سببية بين السلوك الإجرامي والنتيجة، بحيث يكون الحصول على بيانات البطاقة نتيجة مباشرة للنشاط غير المشروع الذي قام به الجاني، سواء تم ذلك عبر الاختراق أو الخداع أو اعتراض البيانات. ويلاحظ أن إثبات هذه العلاقة قد يواجه صعوبات عملية في البيئة الرقمية، بسبب تعدد الوسائط التقنية، وإمكان تدخل أكثر من فاعل، وطبيعة البيانات القابلة للنسخ السريع والانتشار.

ثانياً: الطبيعة القانونية للجريمة

تؤثر هذه الجريمة إشكالاً قانونياً مهماً يتعلق بتكليفها، من حيث تحديد ما إذا كانت تُعد من جرائم الضرر أم من جرائم الخطر، وذلك بالنظر إلى طبيعتها المركبة وتعدد صور سلوكها ونتائجها.

فمن جهة، تمس هذه الجريمة الذمة المالية للمجني عليه متى تم استعمال بيانات البطاقة استعمالاً غير مشروع، إذ يترتب على ذلك إحداث خسارة مالية فعلية، وهو ما يقرّها من طائفة جرائم الضرر التي يشترط لقيامها تحقق نتيجة ضارة. ومن جهة أخرى، قد تتجه بعض التشريعات إلى تجريم مجرد الحصول غير المشروع على بيانات البطاقة، ولو لم يقتزن ذلك باستعمالها، تأسيساً على أن هذا السلوك ينطوي بذاته على تهديد كافٍ للأمن المالي ولثقة في المعاملات الإلكترونية، الأمر الذي يضيء عليها طابع جرائم الخطر.

ومن ثم، يمكن القول إن هذه الجريمة في صورتها البسيطة تميل إلى الاقتراب من جرائم الخطر، في حين تأخذ وصف جريمة الضرر متى تحقق الاستعمال الفعلي للبيانات أو ترتبت عليه خسارة مالية ملموسة.

ويرى الباحث أن التكليف التقليدي لهذه الجريمة ضمن جرائم السرقة أو الاحتيال لم يعد كافياً على نحو كامل في البيئة الرقمية الحديثة، لأن محل الاعتداء لا يتمثل دائماً في مال مادي بالمعنى التقليدي للحيازة، وإنما قد ينصب على بيانات رقمية تمثل في ذاتها قيمة مالية واقتصادية مستقلة وقابلة للاستغلال المالي لاحقاً، الأمر الذي يبرر اتجاه بعض التشريعات الحديثة إلى منح البيانات المالية حماية جزائية مستقلة.

(53) - Yeoman, M. C., Sitompul, R., Heriyanti, H., & Pakpahan, K. (2025). *Protection of consumer personal data against credit card data leaks in e-commerce cooperation agreements with payment gateway service*. In E. F. Pakpahan et al. (Eds.), *Proceedings of the 1st International Forum on Psychology, Law, and Education (IFPLE 2025)* (Advances in Social Science, Education and Humanities Research, Vol. 990, pp. 130 – 131). Atlantis Press.

ثالثاً: الركن المعنوي

تُعد جريمة الاستيلاء على أرقام بطاقات الائتمان من الجرائم العمدية، ويتحقق الركن المعنوي فيها بتوافر القصد الجنائي العام بعنصره، إذ يلزم أن يكون الجاني عالماً بأن البيانات محل الاعتداء مملوكة للغير، وأن الحصول عليها يتم بغير وجه حق، وأن تتجه إرادته إلى الاستيلاء على هذه البيانات أو استعمالها أو تمكين الغير من الانتفاع بها⁽⁵⁴⁾.

ولا يُشترط لقيام هذه الجريمة توافر قصد جنائي خاص، غير أن اتجاه إرادة الجاني إلى تحقيق منفعة غير مشروعة أو الإضرار بالغير يُعد قرينة قوية على توافر القصد الجنائي، ويعزز من قيام المسؤولية الجزائية في حقه، في ضوء ما تكشف عنه ظروف الواقعة وملابساتها.

رابعاً: الإشكال التشريعي (تحليل مقارنة)

تُلاحظ معالجة متفاوتة لهذه الجريمة في التشريعات المقارنة، إذ اتجهت بعض القوانين العربية إلى تنظيمها بنصوص صريحة ضمن تشريعات الجرائم المعلوماتية، مثل قانون الجزاء العماني، وقانون مكافحة جرائم تقنية المعلومات الإماراتي، وقانون العقوبات القطري⁽⁵⁵⁾، حيث تضمنت هذه التشريعات أحكاماً تجرم صور الاعتداء على البيانات والمعلومات الإلكترونية، بما في ذلك الحصول غير المشروع على البيانات المالية أو إساءة استخدامها.

في المقابل، يفترق كل من قانون العقوبات المصري والتشريع الفلسطيني إلى نص خاص يُجرّم الاستيلاء على بيانات بطاقات الائتمان بوصفه جريمة مستقلة، الأمر الذي يضطر القاضي إلى تكييف هذا السلوك ضمن الأطر التقليدية لجرائم الاعتداء على المال، كالسرقة أو النصب أو إساءة الائتمان، بحسب ظروف كل واقعة.

غير أن هذا التكييف التقليدي قد لا يكون كافياً في جميع الحالات، نظراً لاختلاف الطبيعة القانونية للمال المعلوماتي عن المال المادي، سواء من حيث قابليته للنسخ أو صعوبة حيازته بالمعنى التقليدي، وهو ما يُبرز الحاجة إلى تدخل تشريعي أكثر دقة وملاءمة، يراعي الخصوصية التقنية لهذه الجرائم ويكفل توفير حماية جزائية فعالة لها.

ويتضح مما تقدم أن جريمة الاستيلاء على أرقام بطاقات الائتمان تقوم على بنية قانونية معقدة تتداخل فيها العناصر التقنية والمالية، وأن تحليل أركانها يكشف عن قصور القواعد التقليدية في استيعاب جميع صورها، الأمر الذي يستدعي تطوير الأطر التشريعية لمواكبة تطورها المستمر وتعزيز الحماية الجنائية للمعاملات الإلكترونية.

واستناداً إلى معايير الكفاية التي سبق تحديدها في منجز الدراسة، يمكن استخلاص الموقف المقارن للتشريعات محل الدراسة من خلال المصنوفة الآتية، التي تُظهر مدى كفاية كل اتجاه تشريعي في مواجهة الجرائم المرتبطة بالتوقيع الإلكتروني وبيانات بطاقات الائتمان:

جدول (2): مصنوفة التقييم المقارن لكفاية التنظيم القانوني في التشريعات محل الدراسة

معايير الكفاية	التشريع الفلسطيني	التشريع المصري	الاتجاهات التشريعية المقارنة
وجود نصوص تجريم صريحة	لا يتضمن نصوصاً جزائية متخصصة بصورة كافية للاعتداء على بيانات بطاقات الائتمان أو بعض صور الاعتداء المتقدمة على التوقيع الإلكتروني	يتضمن تنظيماً جزئياً لبعض صور الجرائم المعلوماتية والمعاملات الإلكترونية	تميل بعض الاتجاهات المقارنة إلى تنظيم أكثر تفصيلاً للجرائم الرقمية ووسائل التوثيق والدفع الإلكتروني
تناسب العقوبات	العقوبات متفرقة وتعتمد أحياناً على التكييف التقليدي	توجد عقوبات أكثر تحديداً في بعض صور الجرائم المعلوماتية	تتجه بعض النظم المقارنة إلى مواءمة الجزاءات مع خطورة الاعتداءات الرقمية
كفاية قواعد الإثبات الرقمية	الاعتراف بالأدلة الرقمية قائم، لكن التنظيم الإجرائي ما يزال محدوداً	يوجد تنظيم أوسع نسبياً لحجية الأدلة الإلكترونية	تميل الاتجاهات الحديثة إلى تفصيل إجراءات جمع الأدلة الرقمية وحفظها وسلامتها
فعالية التعاون القضائي الدولي	محدود نسبياً بسبب الطبيعة الوطنية للنصوص	يتأثر بقيود الاختصاص والتعاون الإجرائي	تبرز أهمية الاتفاقيات والأطر الدولية في مواجهة الطابع العابر للحدود للجرائم الإلكترونية

(54) - Crown Prosecution Service. (2023). Computer Misuse Act: Unauthorised access to computer material. <https://www.cps.gov.uk/prosecution-guidance/computer-misuse-act>.

(55) - عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 180 - 181.

تكشف هذه المصنوفة أن الإشكال في مواجهة الجرائم المرتبطة بالتجارة الإلكترونية لا يرتبط فقط بوجود النصوص الجزائية من عدمه، بل يمتد إلى مدى قدرة هذه النصوص على الاستجابة للخصوصية التقنية والوظيفية للبيئة الرقمية. فبينما تميل بعض الاتجاهات التشريعية المقارنة إلى تنظيم أكثر تخصصاً في مجال الأدلة الرقمية وجرائم البيانات ووسائل التوثيق الإلكتروني، لا تزال بعض التشريعات العربية تعتمد، في جانب من معالجتها، على قواعد تقليدية لا تستوعب بصورة كاملة الطبيعة غير المادية للبيانات المالية والوسائل الإلكترونية الحديثة.

الخاتمة:

تكشف هذه الدراسة أن التجارة الإلكترونية، رغم ما تحققة من كفاءة اقتصادية واتساع في نطاق التعاملات، قد أفرزت في المقابل بيئة إجرامية رقمية تتسم بالتعقيد وسرعة التطور، حيث تستهدف الجرائم المرتبطة بها عناصر الثقة في المعاملات الإلكترونية، وعلى رأسها وسائل التوثيق (كالتوقيع الإلكتروني) وأدوات الدفع (كالبطاقات الائتمانية). كما يبين التحليل أن خصوصية الوسط الرقمي – من حيث لا ماديته وطابعه العابر للحدود وسهولة تداول البيانات – تُضعف من فعالية الآليات التقليدية للحماية الجزائية، وتطرح تحديات عملية في مجالات الإثبات، وتحديد الاختصاص، وتتبع الجناة. كما كشفت الدراسة، في ضوء معايير الكفاية المعتمدة، عن قصور بعض الأطر التشريعية الخاصة، أو غيابها في بعض النظم، بما يفضي إلى اللجوء إلى تكييفات تقليدية (كالسرقة والنصب)، وهي تكييفات قد لا تستوعب الطبيعة الخاصة للبيانات الرقمية محل الحماية الجزائية ولا صور السلوك الإجرامي المستحدث، الأمر الذي ينعكس على مستوى الردع والثقة في البيئة الرقمية. ومن ثم، فإن تعزيز الحماية الجزائية للتجارة الإلكترونية يستلزم مقاربة تكاملية تجمع بين التنظيم التشريعي المتخصص، والضوابط التقنية، والتعاون الدولي. وتكشف الدراسة، في ضوء التحليل المقارن، أن الإشكال في مواجهة الجرائم المرتبطة بالتجارة الإلكترونية لا يرتبط فقط بغياب النصوص الجزائية الخاصة، بل يمتد إلى محدودية البنية القانونية التقليدية في استيعاب الطبيعة غير المادية للبيانات والمعاملات الرقمية. فالجريمة في البيئة الإلكترونية لم تعد تنصب دائماً على مال مادي أو محرر تقليدي، وإنما قد تستهدف الثقة الرقمية بوصفها أساساً لسلامة المعاملات الإلكترونية، أو البيانات التي تمثل قيمة اقتصادية مستقلة. وعليه، فإن تطوير الحماية الجزائية في هذا المجال لا يقتضي مجرد التوسع في التجريم، بل يتطلب إعادة بناء المقاربة القانونية بصورة تستوعب التحولات التقنية والوظيفية التي أفرزها الاقتصاد الرقمي الحديث.

أولاً: النتائج

1. تبين أن التجارة الإلكترونية تقوم على بنية رقمية تعتمد على تدفق البيانات والمعالجة التقنية والتعاقد عن بُعد، بما يميزها عن التجارة التقليدية ويؤثر بصورة مباشرة في قواعد الإثبات والحماية القانونية والاختصاص القضائي.
2. كشفت الدراسة أن التوقيع الإلكتروني يؤدي وظيفة محورية في إسناد التصرفات القانونية وإثباتها، وأن الاعتداء عليه لا يقتصر أثره على المحرر الإلكتروني ذاته، بل يمتد إلى تقويض الثقة في المعاملات الإلكترونية بوصفها بيئة تعاقدية متكاملة.
3. أظهر التحليل أن جرائم الاستيلاء على بيانات البطاقات الائتمانية تمثل اعتداءً مباشراً على الذمة المالية، وأن خطورتها ترتبط بخصائص البيئة الرقمية، ولا سيما سهولة تداول البيانات، والطابع العابر للحدود، وإمكان ارتكاب الجريمة دون تماس مادي مباشر مع المجني عليه.
4. كشفت الدراسة، في ضوء معايير الكفاية المعتمدة، أن التشريعين الفلسطيني والمصري لا يتضمنان نصوصاً جزائية مستقلة تُجرّم بصورة صريحة بعض صور الحصول غير المشروع على بيانات بطاقات الائتمان والاعتداءات المتقدمة على التوقيع الإلكتروني، الأمر الذي يؤدي إلى اللجوء إلى تكييفات تقليدية كالسرقة أو الاحتيال، وهي تكييفات لا تستوعب بصورة كاملة خصوصية البيانات الرقمية محل الحماية الجنائية.
5. بينت الدراسة أن الطابع العابر للحدود للجرائم المرتبطة بالتجارة الإلكترونية يثير صعوبات عملية وقانونية تتعلق بتحديد الاختصاص القضائي، والقانون الواجب التطبيق، وآليات تنفيذ الأحكام والتعاون القضائي الدولي.
6. أظهر التحليل المقارن تفاوتاً في تنظيم الأدلة الرقمية بين التشريعات محل الدراسة، من حيث حجيتها، وإجراءات جمعها، وضمان سلامة سلسلة حيازتها، بما يؤثر في فعالية الملاحقة الجزائية للجرائم الإلكترونية.
7. كشفت الدراسة المقارنة، في ضوء معايير الكفاية المعتمدة، أن بعض التشريعات المقارنة اتجهت إلى تبني تنظيمات أكثر تخصصاً في مجال حماية المعاملات الإلكترونية والأدلة الرقمية، في حين لا تزال بعض التشريعات العربية تعتمد بصورة واسعة على القواعد الجزائية العامة، وهو ما يحّد من كفاية الحماية القانونية في البيئة الرقمية.

8. تتمثل الإضافة العلمية للدراسة في الجمع بين جرائم الاعتداء على التوقيع الإلكتروني وجرائم الاستيلاء على بيانات بطاقات الائتمان ضمن إطار تحليلي مقارن قائم على معايير الكفاية، بما يساهم في تقديم معالجة قانونية أكثر تكاملاً للجرائم المرتبطة بوسائل الثقة والدفع في البيئة الرقمية.

ثانياً: التوصيات

1. وضع تنظيم تشريعي متخصص للتجارة الإلكترونية يحدد المفاهيم والالتزامات والجرائم المرتبطة بها، مع تضمين حماية صريحة لبيانات الدفع والتوقيع الإلكتروني، ويقتضي تعزيز الحماية القانونية في هذا المجال الانتقال من المقاربة الجزائية التقليدية القائمة على رد الفعل بعد وقوع الجريمة، إلى مقاربة تنظيمية وقائية تستند إلى تدابير الحماية التقنية والرقابية المسبقة، بما ينسجم مع الاتجاهات الحديثة في الحوكمة الرقمية والتنظيم الوقائي للبيئة الإلكترونية.
2. استحداث نصوص جزائية دقيقة تُجرّم الحصول غير المشروع على بيانات البطاقات الائتمانية واستعمالها والاتجار بها، مع مراعاة التدرج في العقوبات.
3. إلزام مزودي الخدمات الرقمية ومشغلي المنصات التجارية باعتماد معايير تقنية لأمن المعلومات، تشمل أنظمة التشفير، وإدارة المفاتيح الرقمية، والمصادقة متعددة العوامل، بما يعزز حماية بيانات المستخدمين ويحد من مخاطر الاختراق والاحتيال الإلكتروني.
4. تطوير القواعد الإجرائية الخاصة بالأدلة الرقمية بما يضمن سلامتها وقابليتها للاعتماد القضائي.
5. تعزيز حماية المستهلك في البيئة الرقمية من خلال متطلبات الإفصاح، وآليات الاسترداد، وتحديد المسؤوليات في حالات خروقات البيانات.
6. تفعيل التعاون الدولي في مكافحة الجرائم الإلكترونية عبر تبادل المعلومات والانضمام إلى الأطر والاتفاقيات ذات الصلة.
7. إنشاء وحدات متخصصة وبناء القدرات المؤسسية في مجال تتبع الجرائم الرقمية والتحليل الجنائي للأدلة الإلكترونية.
8. إرساء قواعد حوكمة للمنصات الرقمية تفرض سياسات تحقق فعالة وأنظمة رصد الاحتيال وإدارة الحوادث.
9. تعزيز الوعي الرقمي لدى المستخدمين من خلال برامج التوعية والتثقيف المتعلقة بمخاطر الاحتيال الإلكتروني، وأساليب حماية البيانات الشخصية والمالية، وطرق الاستخدام الآمن لوسائل الدفع والتعاملات الإلكترونية.

قائمة المصادر والمراجع:

قائمة المراجع باللغة العربية

أولاً: التشريعات

- دولة فلسطين. (2017). قرار بقانون رقم (15) لسنة 2017 بشأن المعاملات الإلكترونية، الوقائع الفلسطينية، العدد 14.
- دولة فلسطين. (2018). قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية.
- جمهورية مصر العربية. (2004). قانون رقم 15 لسنة 2004 بشأن التوقيع الإلكتروني.

ثانياً: الكتب والدراسات

- أبو الليل، إبراهيم الدسوقي. (2003). *الجوانب القانونية للمعاملات الإلكترونية*، مجلس النشر العلمي، جامعة الكويت.
- أحمد، أمانج رحيم. (2011). *التراضي في العقود الإلكترونية عبر شبكة الإنترنت*، ط 1، دار وائل للنشر، الأردن.
- إبراهيم، خالد ممدوح. (2007). *إبرام العقد الإلكتروني*، ط 1، الدار الجامعية، مصر.
- البشكاني، هادي مسلم يونس. (2009). *التنظيم القانوني للتجارة الإلكترونية*، دار الكتب والبرمجيات، مصر.
- برهم، نضال إسماعيل، وأبو عرابي، غازي. (2005). *أحكام عقود التجارة الإلكترونية*، ط 1، دار الثقافة للنشر والتوزيع، الأردن.
- الحلالمة، نصار محمد. (2013). *التجارة في القانون*، ط 1، دار الثقافة للنشر والتوزيع، السودان.
- حجازي، عبد الفتاح بيومي. (2002). *الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت*، دار الكتب القانونية، القاهرة.
- حجازي، عبد الفتاح بيومي. (2003). *النظام القانوني لحماية الحكومة الإلكترونية*، ط 1، دار الفكر الجامعي، الإسكندرية.
- حجازي، عبد الفتاح بيومي. (2007). *التجارة الإلكترونية وحمايتها الجنائية*، دار الفكر الجامعي، الإسكندرية.
- خليل، عماد علي. (2000). *التكييف القانوني لإساءة استخدام أرقام البطاقات الائتمانية عبر شبكة الإنترنت*، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، المجلد الثاني.
- خليل، ناصر. (2009). *التجارة والتسويق الإلكتروني*، ط 1، دار أسامة للنشر والتوزيع، الأردن.
- سليمان، محمد مأمون. (2011). *التحكيم الإلكتروني*، دار الجامعة الجديدة، مصر.
- عبد الحميد، ثروت. (2003). *التوقيع الإلكتروني*، ط 2، مكتبة الجلاء، المنصورة.

- الكسواني، عامر محمود. (2008). *التجارة عبر الحاسوب*، ط1، دار الثقافة للنشر والتوزيع، الأردن.
- الكعبي، محمد عبيد. (2005). *الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت*، دار النهضة العربية، القاهرة.
- مبروك، ممدوح محمد علي. (2005). *مدى حجية التوقيع الإلكتروني في الإثبات*، دار النهضة العربية، القاهرة.
- الوادي، محمود حسين، والوادي، بلال محمود. (2011). *المعرفة والإدارة الإلكترونية*، ط1، دار الصفاء للنشر والتوزيع، الأردن.

ثالثاً: المقالات والدوريات

- المركز الديمقراطي العربي. (2025). *جريمة التزوير في المستندات الإلكترونية الحكومية*، مجلة العلوم السياسية والقانون، مجلد 11، عدد 45. <https://www.democraticac.de/?p=106476>

قائمة المراجع باللغة الإنجليزية

أولاً: القوانين والأنظمة الدولية

- European Parliament and Council of the European Union. (2000). *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Official Journal of the European Communities.*
- French Civil Code. (2016). Article 1367.
- United Nations. (2024). United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (Preamble). United Nations Office on Drugs and Crime. <https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html>
- United Nations Commission on International Trade Law. (1999). UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, with additional Article 5 bis as adopted in 1998.
- United Nations Commission on International Trade Law. (2001). UNCITRAL model law on electronic signatures with guide to enactment.
- United States Congress. (2000). Electronic Signatures in Global and National Commerce Act.

ثانياً: الكتب والدراسات

- Laudon, K. C., & Traver, C. G. (2023). *E-commerce 2023–2024: Business, Technology, Society* (18th ed.). Pearson.

ثالثاً: الأبحاث والمقالات

- Allah Rakha, N. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review*, 16(2). <https://doi.org/10.22201/ij.24485306e.2024.2.18892>
- Chukurna, O., Tardaskina, T., Chaikovska, M., Nitsenko, V., Pankovets, L., & Kofman, V. (2024). Transformation of E-Commerce Business Models in the Digital Economy. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, (5). <https://doi.org/10.33271/nvngu/2024-5/192>
- Fidler, M. (2025). Fragmentation of international cybercrime law. *Utah Law Review*, 2025(3), 737 - 804 <https://doi.org/10.63140/wez4rujib0>
- Gregušová, D., Halášová, Z., & Peráček, T. (2022). eIDAS regulation and its impact on national legislation: The case of the Slovak Republic. *Administrative Sciences*, 12(4), Article 187. <https://doi.org/10.3390/admsci12040187>
- Laxman, V., Ramesh, N., Jaya Prakash, S. K., & Aluvala, R. (2024). Emerging threats in digital payment and financial crime: A bibliometric review. *Journal of Digital Economy*, 3, <https://doi.org/10.1016/j.jdec.2025.04.002>
- Pasaribu, F., Sari, W. P., Bulan, T. R. N., & Astuty, W. (2022). The effect of e-commerce service quality on customer satisfaction, trust and loyalty. *International Journal of Data and Network Science*, 6, 1077–1084. <https://doi.org/10.5267/j.ijdns.2022.8.001>
- Yeoman, M. C., Sitompul, R., Heriyanti, H., & Pakpahan, K. (2025). *Protection of consumer personal data against credit card data leaks in e-commerce cooperation agreements with payment gateway service*. In E. F. Pakpahan et al. (Eds.), *Proceedings*

of the 1st International Forum on Psychology, Law, and Education (IFPLE 2025) (Advances in Social Science, Education and Humanities Research, Vol. 990). Atlantis Press.

رابعاً: التقارير الدولية

- Crown Prosecution Service. (2023). Computer Misuse Act: Unauthorised access to computer material. <https://www.cps.gov.uk/prosecution-guidance/computer-misuseact>
- European Data Protection Supervisor. (2021). Tech Dispatch 2/2021 – Card-based payments. <https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-22021-card-based-payments>
- European Payments Council. (2024). 2024 payment threats and fraud trends report. (EPC162-24, Version 1.0). <https://www.europeanpaymentscouncil.eu>
- Europol. (2020). *Internet Organised Crime Threat Assessment (IOCTA) 2020*. <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020>
- Juniper Research. (2023, June 26). Losses from online payment fraud to exceed 362\$ billion globally over next 5 years. <https://www.juniperresearch.com/press/losses-online-payment-fraud-exceed-362-billion/>