

والأمن السيبراني. كما يبرز البحث أهمية الموازنة بين حماية الحقوق الرقمية من جهة، وضرورة تعزيز الابتكار والنمو الاقتصادي من جهة أخرى، وذلك من خلال تحديث التشريعات، وتبني سياسات وقائية ضدّ الجرائم الإلكترونية، وتفعيل التعاون الدولي لمواجهة التحديات العابرة للحدود. وبذلك يخلص البحث إلى أن التحوّل الرقمي لم يعد خياراً، بل هو مسار حتمي لنهضة الاقتصاد الوطني وضمان استدامة المعاملات التجارية في العصر الحديث

يتناول هذا البحث بالتحليل التحوّلات الرقمية وانعكاساتها على الأعمال التجارية التقليدية، وما أفرزته من آثار قانونية تتعلق بالعقود الإلكترونية، وحجية التوقيعات الرقمية، وحماية البيانات الشخصية، فضلاً عن التحديات المرتبطة بالجرائم السيبرانية. ويؤكد البحث أن هذه التحوّلات تمثل تحوّلاً بنيوياً عميقاً في بيئة الأعمال، يستوجب إعادة صياغة المنظومة التشريعية الوطنية بما ينسجم مع المعايير الدولية، ولا سيّما في ظلّ غياب إطار قانوني متكامل في العراق لحماية البيانات والأمن السيبراني. كما يبرز البحث أهمية الموازنة بين حماية الحقوق الرقمية من جهة، وضرورة تعزيز الابتكار والنمو الاقتصادي من جهة أخرى، وذلك من خلال تحديث التشريعات، وتبني سياسات وقائية ضدّ الجرائم الإلكترونية، وتفعيل التعاون

الآثار القانونية للتحوّلات الرقمية على الأعمال التجارية التقليدية (دراسة مقارنة)
م.د. سارة صباح لفطة الهداوي

كلية الحقوق - جامعة النهرين

sarah.sabah@nahrainuniv.edu.iq

The Legal implications of digital transformation on traditional businesses

Dr. Sarah Sabah Lafta Al-Hindawy
College of Law / Al-Nahrain University

المخلص

يتناول هذا البحث بالتحليل التحوّلات الرقمية وانعكاساتها على الأعمال التجارية التقليدية، وما أفرزته من آثار قانونية تتعلق بالعقود الإلكترونية، وحجية التوقيعات الرقمية، وحماية البيانات الشخصية، فضلاً عن التحديات المرتبطة بالجرائم السيبرانية. ويؤكد البحث أن هذه التحوّلات تمثل تحوّلاً بنيوياً عميقاً في بيئة الأعمال، يستوجب إعادة صياغة المنظومة التشريعية الوطنية بما ينسجم مع المعايير الدولية، ولا سيّما في ظلّ غياب إطار قانوني متكامل في العراق لحماية البيانات

between

safeguarding digital rights on the one hand, and fostering innovation and economic growth on the other, through legislative modernization, the adoption of preventive policies against cybercrimes, and the promotion of international cooperation to address cross-border challenges. Accordingly, the study concludes that digital transformation is no longer a matter of choice but rather an inevitable pathway for the advancement of the national economy and the sustainability of commercial transactions in the modern era.

الكلمات المفتاحية:

التحول الرقمي – الأعمال التجارية – العقود الإلكترونية – حماية البيانات – الجرائم الإلكترونية – الأمن السيبراني

مقدمة

شهد العالم في ظلّ الثورة الصناعيّة الرابعة انطلاقة جديدة للجيل الرابع من العولمة، حيث فرضت التحوّلات الرقمية تحديات وفرصاً جديدة

الدولي

لمواجهة التحدّيات العابرة للحدود. وبذلك يخلص البحث إلى أن التحوّل الرقمي لم يعد خياراً، بل هو مسار حتمي لنهضة الاقتصاد الوطني وضمان استدامة المعاملات التجارية في العصر الحديث

Abstract

This research analyzes the digital transformations and their implications for traditional commercial activities, focusing on the legal consequences arising from electronic contracts, the evidentiary value of digital signatures, and the protection of personal data, in addition to the challenges posed by cybercrimes. The study emphasizes that such transformations constitute a profound structural shift in the business environment, necessitating a reform of the national legislative framework in line with international standards, particularly given the absence of a comprehensive legal system in Iraq governing data protection and cybersecurity. The research further highlights the importance of striking a balance

أمام

الفحم والطاقة

الحكومات وصنّاع القرار. في هذا السياق، أصبح التحوّل الرقمي ضرورة استراتيجية لمواكبة التطوّرات التكنولوجية وتعزيز القدرة التنافسية في بيئة الأعمال. ويُعرّف التحوّل الرقمي بأنّه عملية دمج التقنيات الرقمية في جميع جوانب النشاط الاقتصادي والإداري، ممّا يؤديّ إلى تحسين الكفاءة التشغيلية، وتقديم خدمات أكثر سرعة ومرونة، وتعزيز تجربة العملاء من خلال الابتكار والتطوير المستمر¹.

البخارية خلال الثورة الصناعيّة الأولى، بينما ركّزت الثورة الثانية على الصلب والسكك الحديدية والبتروكيمياويات والكهرباء. ومع ظهور الحواسيب، برزت الثورة الصناعيّة الثالثة، التي قامت على صنّاعة البرمجيات والإنترنت والاتصالات الحديثة، ممّا أحدث تطورات واسعة في مختلف المجالات، لا سيّما الاقتصادية والتجارية².

وتتجلّى أهميّة التحوّل الرقمي في تأثيره المباشر على الأعمال التجارية التقليدية، حيث أدّى إلى إعادة تشكيل أساليب العمل، وتغيير نماذج التشغيل، وإدخال تقنيات جديدة مثل الذكاء الاصطناعي، والحوسبة السحابية، وسلاسل الكتل (Blockchain) ونتيجة لهذا التحوّل، أصبحت الشركات مطالبة بالتكيف مع البيئة الرقمية لضمان استدامتها ومواصلة النمو في ظلّ المنافسة المتزايدة.

أدّى هذا التطوّر إلى زيادة المنافسة بين الشركات وتنوع المنتجات والخدمات، ممّا عزّز ظهور التجارة الإلكترونيّة كأداة حديثة أحدثت تحوّلًا في بيئة الأعمال. فقد ساهمت في تسهيل عمليات البيع والشراء إلكترونياً، وتحسين كفاءة الشركات، وتعزيز تنافسيّتها من خلال تقليل تكاليف التسويق وتقديم الخدمات بسرعة ومرونة.

شهدت الثورات الصناعيّة تحولات جوهرية في تاريخ البشرية، حيث انتقل الإنسان من العمل اليدوي إلى استخدام الآلة بفضل اكتشاف

وتعدّ التجارة الإلكترونيّة امتداداً للتجارة التقليدية، حيث ترتبط بعلم الإدارة والقانون والاقتصاد، ممّا يتطلّب بيئة تنظيمية وتشريعية ملائمة لضمان حماية المتعاملين وتعزيز نمو هذا القطاع الحيوي.

² رنا عبدالرحمن موسى عامر، دور المنظمات الدولية في حماية حقوق الإنسان، المركز الديمقراطي العربي، 2022، بحث منشور على الإنترنت، <https://democraticac.de/?p=84988>

¹ الحداد، محرم صالح: محمد، محمد إبراهيم 2021، " الثورة الصناعيّة الرابعة (الذكاء الاصطناعي – التحوّل الرقمي) تحديات وفرص الاستحواذ علي القوة الرقمية الجديدة"، سلسلة أوراق السياسات في التخطيط والتنمية المستدامة، الإصدار رقم 8، يناير 2021، معهد التخطيط القومي، مصر. ص2

كما تلعب

دعم الناتج المحلي

الإجمالي وتعزيز التنمية الاقتصادية في مختلف الدول⁴.

إذ يتطلب التحوّل الرقمي جمع ومعالجة كمّيات كبيرة من البيانات. ومع ذلك، يواجه العراق تحديات في هذا المجال بسبب ضعف التشريعات المتعلقة بحماية البيانات الشخصية، ممّا يعرض الأفراد والشركات لمخاطر انتهاك الخصوصية⁵

منهج الدراسة

يعتمد المنهج على مزيج من أساليب البحث القانوني كالمنهج الوصفي التحليلي يهدف إلى وصف وتحليل الأنواع المختلفة للجرائم الإلكترونية التي تحدث في البيئات الرقمية والاعمال التجارية التقليدية سيعتمد هذا المنهج على تحليل التشريعات والقوانين العراقية والدولية المتعلقة بالجرائم الإلكترونية. ستشمل الدراسة التفاعل مع الجهات القانونية المختلفة مثل محاكم جرائم الإنترنت، ومنظمات الأمن السيبراني، والمؤسسات المالية التي تأثرت بالجرائم الإلكترونية.

تكنولوجيا المعلومات والاتصالات دورًا محوريًا في تعزيز كفاءة الأداء الحكومي وتحفيز الاقتصاد الرقمي، حيث انتقلت الخدمات العامّة من النمط التقليدي أحادي الاتجاه إلى أنموذج أكثر تفاعلية، يتيح للمواطنين المشاركة الفاعلة في صنع القرار والتخطيط. وتعد الحكومة الإلكترونية إحدى الركائز الأساسية لهذا التحوّل، إذ تسعى الدول إلى تطوير بنيتها الرقمية من خلال نشر خدمات الاتصالات والإنترنت، وتمكين الخدمات الحكومية إلكترونياً، وتعزيز الثقافة الرقمية على مستوى الأفراد والمؤسسات³. ورغم عدم وجود تعريف موحد للاقتصاد الرقمي، فإن منظمة التعاون الاقتصادي والتنمية (OECD) تعرفه بأنّه يشمل جميع الأنشطة الاقتصادية القائمة على المدخلات الرقمية، بما في ذلك التقنيات والبنية التحتية والخدمات الرقمية، ودورها في تعزيز الكفاءة التشغيلية وتحسين جودة الخدمات. ويعكس النمو المتسارع للصادرات الرقمية عالمياً، مقارنة بالخدمات التقليدية، مدى أهمّية الاقتصاد الرقمي في

³ د. وائل مجدي رزق، دور التحول الرقمي في دعم بيئة الأعمال وجذب الاستثمارات في مصر في ضوء رؤية 2030، أكاديمية السادات للعلوم الإدارية مركز الاستشارات والبحوث والتطوير، مجلة البحوث الإدارية المجلد الأربعون، العدد الرابع، أكتوبر 2022، ص 04

⁴ OECD, (2020), " A Roadmap Toward A Common Framework for Measuring the Digital Economy ", Report for the G20 Digital Economy Task Force Saudi Arabia, 2020.

⁵ ايمن مظهر بدر، تحقيق التوازن بين الفوائد والمخاطر: التحول الرقمي وحماية الحقوق والخصوصية في العراق، جامعة ديالى كلية العلوم السياسية،

<https://law.uodiyala.edu.iq/>

أهداف الدراسة

1. دراسة تأثير التقنيات الرقمية على العمليات التجارية والعقود الإلكترونية.
2. استعراض التشريعات الخاصة بحماية البيانات والخصوصية في البيئة الرقمية.
3. فحص التحديات القانونية الناتجة عن الجرائم الإلكترونية وكيفية مواجهتها.
4. اقتراح تعديلات تشريعية لمواكبة التحول الرقمي وحماية المعاملات التجارية.

إشكالية الدراسة

تتمحور إشكالية الدراسة حول تحديد الفجوات القانونية التي قد تظهر نتيجة التحول الرقمي وكيفية تكييف الإطار القانوني لتلبية هذه المتغيرات المتسارعة. وهنا يأتي السؤال كيف يمكن تعديل وتطوير التشريعات القانونية لتواكب التحول الرقمي في بيئة الأعمال، مع التركيز على حماية البيانات، تنظيم العقود الإلكترونية، ومكافحة الجرائم الإلكترونية؟

تكمن أهمية هذه الدراسة في تسليط الضوء على التحول الهائل الذي يواجهه العالم بسبب التكنولوجيا والثورة الرقمية ومدى تأثيرها على المعاملات التجارية والقانون. ومع الاعتماد المتزايد على التكنولوجيا في مجال الاقتصاد والإدارة، هناك حاجة لفهم ودراسة آثار التحول الرقمي على عمل الشركات والآثار القانونية الناشئة في أعقاب هذا التحول. ولهذا الغرض، توضح الدراسة كيف تؤثر التقنيات الرقمية على العمليات التجارية مثل العقود والتوقعات الإلكترونية وكيف تسهل جعل العملية التجارية أكثر كفاءة وخفض التكاليف. بالإضافة إلى ذلك، تسلط الدراسة الضوء أيضاً على النظام القانوني لحماية البيانات والخصوصية، خاصة مع التطورات القانونية مثل اللائحة العامة لحماية البيانات (GDPR) التي أصبحت من التحديات الرائدة للشركات، وتلخص الحاجة إلى تحديث القوانين في محاولة لمواكبة هذه الثورة. كما يقدم البحث نظرة ثاقبة على الصعوبات في الجرائم الإلكترونية التي تشكل تهديداً لاستقرار الشركات، مما يستلزم سياسات وقوانين جديدة لمكافحة مثل هذه الجرائم وتأمين المعاملات التجارية الإلكترونية. وبشكل عام، تعكس الدراسة أهمية الإصلاح القانوني لمواكبة التطور الرقمي والمساعدة في بناء نظام قانوني متكامل يساعد على

المبحث

الأول: التحوّل الرقمي وآثاره على المعاملات التجارية

ومع ذلك، يتطلّب

تطبيق هذه التعليمات تحديث البنية التحتية المالية وضمان الامتثال للمعايير الدولية⁷

يشير التحوّل الرقمي إلى توظيف تكنولوجيا الحاسوب والإنترنت لتعزيز الكفاءة والفعالية في خلق القيمة الاقتصادية. وبمفهوم أوسع، يعكس التحوّل الرقمي التغيرات التي تحدثها التقنيات الحديثة في أساليب العمل والتفاعل معها، إضافةً إلى كيفية تحقيق الثروة ضمن هذا النظام. وقد تنوّعت تعريفات الدراسات السابقة لهذا المفهوم، حيث وصفته بعض الأبحاث بأنه "عملية تغييرات جوهرية في سلسلة خلق القيمة داخل الشركات أو في هيكلها الداخلي، والتي قد تكون سبباً أو شرطاً مسبقاً لاعتماد التكنولوجيا"⁶

إنّ التكنولوجيا الرقمية لا تسهم فقط في تطوير المنتجات والخدمات، بل تسهل أيضاً عمليات التواصل وتعزز القدرة على استخدام البيانات لاتخاذ قرارات أكثر استنارة تدعم النمو والابتكار. ومع ذلك، لضمان نجاح هذا التحوّل، يجب أن يُنظر إلى الموظفين كشركاء في العملية، من خلال توفير التدريب المناسب واستقطاب المواهب القادرة على دعم تنفيذ الاستراتيجيات الرقمية الجديدة، ممّا يضمن تكيف المؤسسات مع البيئة الرقمية الحديثة وتحقيق استدامتها. وبهذا سنبحث في هذا المبحث مفهوم التحوّل الرقمي وخصائصه في المجال التجاري.

إنّ التحوّل الرقمي ليس مجرد إدخال للتكنولوجيا في بيئة الأعمال، بل هو عملية دمج شاملة للتقنيات الرقمية في جميع الأنشطة والعمليات داخل المؤسسات، ممّا يؤديّ إلى تغيير جذري في نماذج التشغيل، وأساليب العمل، وآليات اتخاذ القرار. وفي هذا السياق أقر العراق تعليمات المدفوعات الإلكترونية رقم 2 لعام 2024 بهدف تقليل الاعتماد على النقد وتعزيز الشمول المالي.

المطلب الأول: مفهوم التحوّل الرقمي وخصائصه في المجال التجاري

إنّ التحوّل الرقمي هو عملية تكامل التقنيات الرقمية في مختلف جوانب الأعمال، ممّا يؤديّ إلى تغيير جوهرية في أساليب عمل الشركات وآليات تقديمها للقيمة لعملائها. يشمل هذا

https://www.undp.org/ar/iraq/blog/turning-point-iraqs-leap-digital-economy?utm_source=chatgpt.com [Accessed 23 Mar. 2025].

⁶ Muehlburger, M., Rueckel, D., & Koch, S. (2019), "A framework of factors enabling digital transformation"

⁷ الزهيري، علي 2024. نقطة التحوّل: قفزة العراق نحو الاقتصاد الرقمي . [online] UNDP. Available at:

التحوّل

المعلومات من

الوسائط التقليدية إلى أشكال إلكترونية، ممّا يسهل الوصول إليها عبر تطبيقات الحاسب الآلي، ويجعل المحتوى التقليدي متاحاً رقمياً.⁹

يشير مفهوم التحوّل الرقمي إلى توظيف التكنولوجيا لدعم عمليات التغيير الجذرية داخل المؤسسات،¹⁰ حيث يتم الانتقال من الأنظمة التقليدية إلى أنظمة رقمية تعتمد على تكنولوجيا المعلومات والاتصالات في مختلف مجالات العمل. ويتطلب هذا التحوّل وضع استراتيجية واضحة، ونشر ثقافة التحوّل الرقمي، وتوفير التمويل اللازم، إلى جانب تلبية المتطلبات البشرية، والتقنية، والأمنية، والتشريعية التي تضمن نجاحه واستدامته.¹¹

الفرع الثاني: خصائص التحوّل الرقمي في المجال التجاري

يساهم التحوّل الرقمي في تعزيز رفاهية الأفراد والمجتمعات من خلال توفير خدمات

اعتماد تقنيات متقدّمة مثل الذكاء الاصطناعي، وإنترنت الأشياء، والتحليلات الذكية بهدف تحسين العمليات وتعزيز الابتكار. وعليه سنبحث مفهوم التحوّل الرقمي في القطاع التجاري وخصائصه.

الفرع الأول: تعريف التحوّل الرقمي في القطاع التجاري

يُعرف التحوّل الرقمي بأنّه اعتماد المنظمة على التكنولوجيا في إدارة أعمالها وخدماتها وأنشطتها، إضافةً إلى معالجة البيانات وتحليلها وتعزيز التواصل بين أفرادها، ممّا يمكنها من تنفيذ تعاملاتها إلكترونياً بشكل كامل. ويتطلّب ذلك وجود بيئة تقنية آمنة تعتمد على قواعد بيانات محمية لضمان سلامة المعلومات وسلسلة العمليات.⁸

التحوّل الرقمي يُقصد به الاستثمار في الفكر وتغيير السلوك لإحداث تحوّل جذري في طرق العمل، من خلال الاستفادة من التطوّر التقني الكبير لتقديم الخدمات للمستفيدين بسرعة وكفاءة أكبر. كما يُعرّف على أنه عملية تحويل مصادر

الملك سلمان للدراسات والخدمات الاستشارية، العدد الرابع، يناير ٢٠٠٩، ص ١١.

¹⁰ Maye, Terry & Others, Transforming Higher Education Through TechnologyEnhanced Learning, The Higher Education Academy, York Science Park, Heslington, 2009,p11.

¹¹ د/ مصطفى أحمد أمين، التحوّل الرقمي في الجامعات المصرية كمتطلب لتحقيق مجتمع المعرفة، مجلة ٤ الإدارة التربوية، العدد التاسع عشر، ٢٠١٨، ص ٤٥.

⁸ فاطمة الزهراء فرحات، دور التحوّل الرقمي في تحسين أداء وظائف العلاقات العامة في المؤسسات ٢ العمومية الجزائرية، دراسة تحليلية لصفحة فيسبوك مديرية الصحة والسكان لولاية أم البواقي، رسالة ماجستير، كلية العلوم الاجتماعية والإنسانية، جامعة العربي بن مهيدي- أم البواقي، الجزائر، ٢٠٢٠، ص ٦٣.

⁹ أحمد فرج أحمد، الرقمنة داخل مؤسسات المعلومات أم خارجها؟ دراسة في الإشكالات ومعايير الاختيار، مجلة دراسات المعلومات، تصدر عن جمعية المكتبات والمعلومات السعودية بالتعاون مع معهد

متنوعة

تسهّل تبادل المعلومات والبيانات دون قيود زمانية أو مكانية، مستنداً إلى مجموعة من الخصائص المميزة¹²:

من أبرز هذه الخصائص التنوع في أشكال الاتصال، حيث تتيح الوسائل الرقمية، مثل الحاسب الشخصي، خيارات متعدّدة للتواصل يمكن استخدامها في أي وقت وأي مكان وفقاً لاحتياجات المستخدم. كما يوفر التحوّل الرقمي تنوعاً في المحتوى، إذ يمكن للأفراد الاختيار من بين مختلف المجالات والوظائف المتاحة عبر الإنترنت.

إنّ التكامل يُعدّ من السمات الأساسية للتحوّل الرقمي، حيث تجمع شبكة الإنترنت بين مختلف نظم الاتصال والوسائل الرقمية والمحتوى ضمن منظومة واحدة متكاملة، ممّا يمنح المستخدم خيارات متعدّدة من حيث أساليب التعرّض، التخزين، والإتاحة الفورية أثناء تصفح الإنترنت كما يتجاوز التحوّل الرقمي الحدود التقليدية للمكان والزمان، ممّا يتيح إمكانية التواصل عن بُعد دون الحاجة إلى التواجد الجسدي، على عكس التواصل التقليدي المباشر، وهو ما يعزّز المرونة والتفاعلية¹³.

كما يتميز

التحوّل الرقمي بخاصية الاستغراق في عملية الاتصال، حيث تسهم انخفاض تكاليف الاتصال وانتشار الأجهزة الرقمية وتطور البرمجيات بأسعار معقولة في زيادة تفاعل المستخدمين مع المحتوى الرقمي لفترات طويلة. وتساعد التقنيات الحديثة، مثل النصوص والوسائل الفائقة، في تسهيل التجول بين المعلومات والأفكار، سواء لأغراض التعلّم أو الترفيه، ممّا يجعل مدّة استخدام الحاسب والبرامج الرقمية تفوق في كثير من الأحيان الوقت المستغرق في الوسائل التقليدية مثل القراءة أو المشاهدة، خاصة بعد أن أصبحت الإنترنت منصة رئيسة لعرض المحتوى الإعلامي المقدم من وسائل الإعلام المختلفة¹⁴.

وفي هذا السياق لا بدّ أن نذكر أهميّة التحوّل الرقمي فقد ساهم التحوّل الرقمي في انتقال المؤسسات من بيئة محلية مغلقة إلى تكامل أوسع مع البيئات الخارجية، ممّا أدّى إلى تحقيق نمو مستمر وانعكاسات إيجابية مباشرة. ويتطلّب تحقيق التميز في هذا السياق تضافر الجهود الوظيفية والإدارية والرقابية، ممّا يخلق تفاعلاً ديناميكياً يسهم في تحفيز تغييرات جوهرية تدفع عجلة

¹³ محمد عبد الحميد، نظريات الاعلام واتجاهات التأثير، ط ٣، عالم الكتب، القاهرة، ٢٠٠٤، ص ١١٠، ١١١.

¹⁴ محمد عبد الحميد، المرجع السابق، ص ١١٥.

¹² ماجدة عبد الشافي محمد الهادي خالد منصور، الحماية الدستورية للأمن السبيري وأثره على النظام العام، جامعة بنها، ص 385.

التطوير

المستدام، وتعزز اندماج مختلف القطاعات ضمن منظومة رقمية متكاملة¹⁵.

وفي هذا الإطار، أطلق المنتدى الاقتصادي العالمي عام 2015 "مبادرة التحول الرقمي" ضمن جهوده الرامية إلى تشكيل مستقبل الاقتصاد العالمي من خلال استثمار التطورات الرقمية في مختلف القطاعات¹⁶.

أما في المجال العسكري، فقد أدى الاعتماد المتزايد على تكنولوجيا المعلومات إلى تعزيز القدرات القتالية للأسلحة التقليدية وتطوير الأنظمة الدفاعية الحديثة. ويُنظر إلى تكنولوجيا المعلومات والاتصالات في هذا السياق على أنها أداة استراتيجية مزدوجة، تمثل في آن واحد سلاحاً هجومياً وهدفاً محورياً في العمليات العسكرية. ويبرز ذلك بوضوح في إطار "حرب المعلومات"، حيث تُوظف التقنيات الرقمية لتحقيق التفوق المعلوماتي وتعزيز القدرة على إدارة العمليات العسكرية بكفاءة وفاعلية¹⁷.

وفي سياق

بحثنا علينا ذكر أهمية التحول الرقمي في المجال الاقتصادي إذ تكمن في دوره المحوري في تسريع الانتقال نحو الاقتصاد القائم على المعرفة، مما أسهم في ترسيخ مفهوم الاقتصاد الرقمي. فقد أدى التطور في تكنولوجيا المعلومات والاتصالات إلى اعتماد البرمجيات والتطبيقات الذكية لتحقيق تقدم ملموس في ريادة الأعمال والإدارة، بالإضافة إلى تعزيز الابتكار التكنولوجي في قطاعات اقتصادية حيوية مثل الطاقة، السياحة، والخدمات المالية والمصرفية، مما ساعد في تحسين الكفاءة وزيادة الإنتاجية في هذه المجالات¹⁸.

المطلب الثاني: تأثير التحول الرقمي على العقود والتوقيعات الإلكترونية

أدى التحول الرقمي إلى إحداث تغيير جذري في طريقة إبرام العقود وإجراء المعاملات القانونية، حيث أصبحت العقود والتوقيعات الإلكترونية جزءاً أساسياً من البيئة القانونية والتجارية الحديثة.

Paper, Committed To Improving The State Of The World, January 2017, p2.

¹⁷ حمدون اتوريه، البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، ٢٠١١، ص ٤٨.

¹⁸ ماجدة عبد الشافي محمد الهادي خالد منصور، مرجع سابق، ص

¹⁵ د/ محمد علي حسن شعلان، حوكمة التحول الرقمي في الرؤية السعودية ٢٠٣٠، مجلة المهندس، تصدر عن الهيئة السعودية للمهندسين، العدد ٩٩، ٢٠١٦، ص ٤٩.

¹⁶ World Economic Forum , Digital Transformation Initiative Professional Services Industry, White

الفرع

الأول: الأثر القانوني والاعتراف الرسمي بالعقود والتوقيعات الإلكترونية

مع التطور التكنولوجي المتسارع، أصبحت العقود والتوقيعات الإلكترونية حجر الأساس في المعاملات التجارية والاقتصادية، مما استدعى تعديلات جوهرية على القوانين التقليدية لضمان توافقها مع متطلبات العصر الرقمي.¹⁹ وقد بادرت العديد من الدول، مثل الإمارات والكويت، إلى إصدار قوانين تنظم التجارة الإلكترونية وتعزز الثقة في العقود الرقمية، من خلال وضع أطر قانونية واضحة تعترف بحجيتها وتضمن موثوقيتها.²⁰ كما أنّ القوانين الدولية، مثل قانون الأونسيترال الأنموذجي بشأن التوقيعات الإلكترونية، ساهمت في تعزيز الاعتراف القانوني بهذه العقود على المستوى العالمي.

يتطلب الاعتراف القانوني بالعقود الإلكترونية توافر مجموعة من المعايير الأساسية، مثل التحقق من هوية الأطراف المتعاقدة، وضمان

الموافقة الصريحة،

والامتثال للتشريعات الدولية المتعلقة بحماية البيانات وأمن المعلومات.²¹ فالتحقق من الهوية الرقمية أصبح ضرورة أساسية لضمان صحة المعاملات، حيث تعتمد العديد من الأنظمة القانونية على التصديق الرقمي كأداة لإثبات الهوية ومنع الاحتيال. كما أنّ القوانين الحديثة تشترط أن تكون العقود الإلكترونية مصحوبة بآليات واضحة لموافقة الأطراف، مع الالتزام بسياسات خصوصية متوافقة مع معايير مثل اللائحة العامة لحماية البيانات (GDPR).²²

إنّ هذا التطور القانوني يساهم بشكل مباشر في تعزيز الثقة بالمعاملات الرقمية، حيث يضمن موثوقية العقود والتوقيعات الإلكترونية، مما يسمح بخلق بيئة تجارية أكثر أماناً وكفاءة في ظلّ التحول الرقمي العالمي.

وفي ظلّ تزايد التهديدات الإلكترونية التي تؤثر على الاستقرار الاقتصادي والأمن الوطني، تبرز الحاجة إلى شراكات دولية قوية لمواجهة

²¹ يحيى يوسف فلاح حسن، التنظيم القانوني للعقود الإلكترونية، جامعة النجاح الوطنية، الأطروحة استكمالاً لنيل درجة الماجستير في القانون الخاص بكلية الدراسات العليا في جامعة النجاح الوطنية في نابلس، فلسطين 2007، ص 64

²² د. خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، در الفكر الجامعي، 2007، الشكليات القانونية في عقود الإنترنت والتجارة الإلكترونية.

<https://kenanaonline.com/users/KhaledMamdouh/posts/77862>

¹⁹ المركز العالمي لحماية التجارة الإلكترونية 2023 التجارة الإلكترونية انطلاقة نحو المستقبل - المركز العالمي لحماية التجارة الإلكترونية [online] WCPEC. | المركز العالمي لحماية التجارة الإلكترونية | WCPEC. Available at: <https://wcpec.com> [Accessed 11 Mar. 2025].

²⁰ المستشار القانوني عبد الله (2025). (دليل الإثبات في عقود التجارة الدولية الإلكترونية في أبوظبي. Marketing Agency. [online]. Available at: <https://jurists.ae/blog> [Accessed 11 Mar. 2025].

الجرائم

السيبرانية. يدرك العراق خطورة هذه التهديدات ويسعى لتعزيز بنيته التحتية للأمن السيبراني، لكنه يواجه تحديات عدة تعيق مشاركته الفعالة في التعاون الدولي²³.

ومن أبرز التحديات التي تواجه العراق افتقاره إلى إطار قانوني شامل ومحدث، حيث تعيق القوانين القديمة تحقيق العدالة في الجرائم الإلكترونية، لا سيما مع صعوبة التحقق من الأدلة الرقمية. كما أنّ غياب قوانين صارمة لحماية البيانات يترك الأفراد والشركات عرضة لانتهاك خصوصيتهم. يضاف إلى ذلك نقص الكوادر المتخصصة في الأمن السيبراني وقلة الموارد، ممّا يحدّ من قدرته على مواجهة التهديدات بفعالية. كما أنّ التوتر بين تنظيم المحتوى الإلكتروني وضمان حرية التعبير يفرض تحديات إضافية، ما يستدعي تحقيق توازن بين الأمن وحماية الحقوق الرقمية²⁴.

الفرع الثاني:

التحديات التقنية والأمنية للعقود والتوقيعات الإلكترونية

أحدثت الثورة الرقمية تحوّلًا جذريًا في إبرام العقود، حيث أصبح التوقيع الإلكتروني عنصراً أساسياً، لكنه جلب تحديات أمنية جديدة، أبرزها الاختراقات والتزوير الرقمي. فمع تزايد الهجمات السيبرانية، أصبح من الضروري تعزيز الحماية عبر تقنيات متقدمة²⁵.

تشمل المخاطر البرامج الضارة والتصيد الاحتيالي واستغلال الثغرات الأمنية، ممّا يستدعي حلولاً مثل التشفير والتوقيع الرقمي لضمان الأمان وتعتمد التوقيعات الرقمية على خوارزميات تشفير متطورة، مثل RSA، للتحقق من هوية المرسل ومنع التلاعب بالمستندات تساعد هذه التقنيات في حماية المعاملات الرقمية، ممّا يعزّز الثقة والأمان في بيئة الأعمال الرقمية المتسارعة²⁶.

²⁵ حمود، لبنى (2023) مخاطر التحول الرقمي في عام ٢٠٢٣ للمؤسسات [online]. مجموعة ريناد للمجد لتقنية المعلومات RMG. Available at: <https://www.rmg-sa.com>.

²⁶ yemen-yba.com (2020). الإختراق الإلكتروني فخاخ خبيثة. جمعية البنوك اليمنية. [online]. وخيان | جمعية البنوك اليمنية. Available at: <https://yemen-yba.com/> [Accessed 11 Mar. 2025].

²³ kurdistanchronicle (2024). Cybercrime: Solutions for Iraq and the Kurdistan Region. [online] Kurdistanchronicle.com. Available at: <https://www.kurdistanchronicle.com/babat/3176> [Accessed 23 Mar. 2025].

²⁴ United States Central Command (CENTCOM) (2022). A Commitment to Cybersecurity. [online] Unipath. Available at: <https://unipath-magazine.com/a-commitment-to-cybersecurity/>.

المبحث

الثاني: الإطار القانوني لحماية البيانات والخصوصية في البيئة الرقمية

يشهد العالم الرقمي تطورًا متسارعًا صاحبه انتشار واسع لتقنيات جمع ومعالجة البيانات الشخصية، مما أفرز تحديات جديدة تتعلق بحماية الخصوصية. ومع اعتبار البيانات "النفط الجديد"، أصبح من الضروري وضع إطار قانوني قوي ينظم استخدامها، ويمنع أي استغلال أو انتهاك لها.

المطلب الأول: التشريعات المنظمة لحماية البيانات والمسؤولية القانونية للشركات

حماية البيانات الشخصية ليست مجرد التزام أخلاقي، بل مسؤولية قانونية تقع على عاتق الشركات والمؤسسات التي تتعامل مع هذه البيانات. فبموجب القوانين المحلية والدولية، يجب على الشركات اتخاذ التدابير اللازمة لضمان حماية البيانات الشخصية من الوصول غير المصرح به أو الاستخدام غير القانوني أو الإفصاح غير المصرح به.²⁷ وتشمل هذه التدابير وضع سياسات وإجراءات داخلية واضحة، وتدريب الموظفين على أفضل ممارسات أمن المعلومات، وتطبيق تقنيات التشفير والحماية الإلكترونية، بالإضافة إلى إجراء

تقييمات دورية

للمخاطر الأمنية. كما تلتزم الشركات بالإبلاغ الفوري عن أي اختراقات أمنية قد تعرض بيانات الأفراد للخطر، واتخاذ الخطوات اللازمة لتقليل الأضرار المحتملة. وتعتمد حماية البيانات أيضاً على مبدأ الشفافية، حيث يتوجب على الشركات إعلام المستخدمين بطريقة واضحة حول كيفية جمع بياناتهم ومعالجتها واستخدامها، بما في ذلك أنواع البيانات التي يتم جمعها، والأغراض التي تخدمها، والجهات التي قد يتم مشاركتها معها، مع ضمان حقوق الأفراد في التحكم ببياناتهم.²⁸

المطلب الثاني: أثر قوانين حماية البيانات (GDPR) على الأعمال التقليدية

إنّ تأثير قوانين حماية البيانات (GDPR) على الأعمال التقليدية يتجاوز مجرد الامتثال القانوني، ليصبح جزءاً أساسياً من استراتيجية الشركات في بناء الثقة، تحسين الأمان، وتعزيز الميزة التنافسية. فمعايير GDPR الصارمة تفرض على الشركات التعامل مع البيانات الشخصية بشفافية ومسؤولية، مما يعزز ثقة العملاء ويحسن سمعة المؤسسة. إذ يشجّع القانون على توفير آليات واضحة لطلبات الأفراد المتعلقة

²⁸ قانون حماية البيانات الشخصية في مصر، قانون رقم ١٥١ لسنة ٢٠٢٠

²⁷ DLA PIPER (2024). Definitions in the United States - Data Protection Laws of the World. [online] Dlapiperdataprotection.com. Available at: <https://www.dlapiperdataprotection.com/?t=definitions&c=US> [Accessed 11 Mar. 2025].

ببياناتهم،

مما يعكس احتراماً لحقوق الخصوصية ويزيد من مصداقية الشركة.²⁹

إلى جانب ذلك، فإن الامتثال لـ GDPR يحمي الشركات من الغرامات المالية الضخمة التي قد تصل إلى 20 مليون يورو أو 4% من إجمالي الإيرادات السنوية، وهو ما يجعل الالتزام بهذه القوانين أمراً ضرورياً لتجنب العقوبات القانونية والتأثيرات التشغيلية السلبية. كما أن تطبيق تدابير أمنية مشددة، مثل التشفير والتحقق متعدد العوامل، يقلل من مخاطر انتهاكات البيانات، في حين تفرض القوانين وجود خطط استجابة للحوادث لضمان التعامل الفوري والفعال مع أي اختراقات قد تحدث.³⁰ ولا يقتصر تأثير GDPR على الأمان والامتثال فقط، بل يمتد ليشكل ميزة تنافسية للشركات التي تضع خصوصية العملاء على رأس أولوياتها. إذ تشير الدراسات إلى أن نسبة كبيرة من المستهلكين تفضل التعامل مع الشركات التي تحترم خصوصيتهم، مما يمنح المؤسسات الممتثلة للقانون

فرصاً أكبر للنمو

وتعزيز مكانتها في السوق. كما أن الالتزام بـ GDPR يفتح آفاقاً جديدة للشركات التي تسعى لدخول السوق الأوروبية، حتى لو كانت تعمل خارج الاتحاد الأوروبي.³¹

ومن ناحية أخرى يسهم الامتثال لهذه القوانين في تحسين كفاءة إدارة البيانات، من خلال تقليل جمع المعلومات إلى الحد الأدنى الضروري، مما يرفع من جودة البيانات ويخفض التكاليف التشغيلية. كما يساعد في تنظيم العمليات الداخلية للشركة، حيث تصبح إدارة البيانات أكثر وضوحاً وتماسكاً، مما يعزز التعاون بين الأقسام المختلفة مثل القانون، تكنولوجيا المعلومات، التسويق، والموارد البشرية.³² ومع ذلك، تواجه الشركات التقليدية تحديات في دمج متطلبات GDPR مع بنيتها الحالية دون الحاجة إلى تغييرات جذرية، كما أن الالتزام بهذه القوانين ليس عملية تتم لمرة واحدة، بل يتطلب مراجعة وتحديثاً مستمرين لضمان الامتثال الدائم. في النهاية، لم يعد GDPR مجرد

³¹ Eccenca (2020). The GDPR Challenges Classic Data Management Approaches. [online] Eccenca.com. Available at: <https://eccenca.com/blog/article/the-gdpr-challenges-classic-data-management-approaches> [Accessed 11 Mar. 2025].

³² cookieyes Team (2024).ibid

²⁹ cookieyes Team (2024). 7 Key Benefits of GDPR Compliance for Your Business in 2024 - CookieYes. [online] CookieYes. Available at: <https://www.cookieyes.com/blog/benefits-of-gdpr-compliance/>.

³⁰ Massar (2024). التسويق بمبدأ الخصوصية أولاً: المبادئ والتطبيقات والتحديات. [online] Masaar. Available at: <https://masaar.net/ar> [Accessed 11 Mar. 2025].

إطار

قانوني، بل تحوّل إلى عنصر رئيس في استراتيجيات الأعمال، حيث يوفّر الحماية، يعزّز الثقة، ويمنح المؤسسات ميزة تنافسية مستدامة في عالم رقمي سريع التطوّر.³³

المبحث الثالث: الجرائم الإلكترونية والتحديات القانونية في الأعمال الرقمية

شهد العالم تحوّلاً جذرياً نحو الاقتصاد الرقمي، حيث تُشكّل التكنولوجيا الرقمية العمود الفقري لمختلف المجالات الاقتصادية والتجارية. وقد ولّد هذا التحوّل تحديات جديدة من المنظور القانوني، لا سيّما فيما يتعلق بالجرائم الإلكترونية التي تُشكّل تهديداً متزايداً لعمليات الأعمال الرقمية. وقد أدّى الاستخدام المتزايد للأنظمة الإلكترونية والمعلومات الرقمية إلى ظهور جرائم جديدة، تتراوح بين الاحتيال المالي، وانتهاكات الخصوصية والأمن، ووصولاً إلى الهجمات الإلكترونية على المؤسسات والشركات. كما يُعدّ الإطار القانوني لمكافحة الجرائم الإلكترونية من أكثر القضايا إثارة للجدل على الصعيدين الوطني والدولي، نظراً لطبيعة هذه الجرائم العابرة للحدود،

وصعوبة تحديد

مرتكبيها. وي طرح المشهد الرقمي المتغير باستمرار إشكاليات قانونية معقدة، تستدعي مراجعة القوانين والتشريعات بانتظام لضمان حماية الحقوق الرقمية وتعزيز الأمن السيبراني. ومن هذا المنطلق، يحلّ هذا المبحث الاحتيال الإلكتروني والمسؤولية القانونية للمؤسسات التجارية مكافحة الجرائم الإلكترونية وأثرها على استقرار الأعمال التجارية.

المطلب الأول: الاحتيال الإلكتروني والمسؤولية القانونية للمؤسسات التجارية

تُعدّ جريمة الاحتيال عبر شبكة المعلومات الدولية من أخطر الجرائم الحديثة التي تتطوّر باستمرار تبعاً للتحوّلات الاجتماعية والاقتصادية. وتعتمد أساليب مرتكبيها على استغلال القابلية النفسية للأفراد للإقناع، مستغلين الظروف المحيطة بهم لخداعهم بوسائل احتيالية تدفعهم إلى تسليم أموالهم طوعاً دون إكراه أو عنف. وتتميز هذه الجريمة بكونها غير قائمة على القوة أو التهديد، وغالباً ما يكون للمجني عليه دور فيها، ممّا يجعله متردداً في الإبلاغ عنها، سواء بسبب الشعور بالإحراج أو الخوف من العواقب.³⁴ وعليه يُعدّ

companies-make-when-implementing-gdpr-tariq-syed-htave/ [Accessed 11 Mar. 2025].

³⁴ الشوابكة، محمد امين. (2004). جرائم الحاسوب والانترنت، عمان، دار الثقافة للنشر والتوزيع، الأردن، ط.1

³³ Syed, T. (2024). In today's data-driven world, the importance of GDPR (General Data Protection Regulation) compliance cannot be overstated. Yet, many companies, despite good intentions, stumble in their efforts to implement privacy processes. [online] LinkedIn.com. Available at: <https://www.linkedin.com/pulse/common-mistakes->

الاحتيال

"التصيد"

الاحتيالي (Phishing) "، فالتصيد الاحتيالي هو محاولة لسرقة معلومات حساسة مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقات الائتمان (وأموال المستخدمين)، وذلك عن طريق التظاهر بكيان موثوق في اتصال إلكتروني بهدف تحقيق أهداف ضارة. حيث يقوم المحتالون بإرسال رسائل إلكترونية تدعي أنها من شركات أو مؤسسات معروفة مثل البنوك أو شركات التأمين، بهدف جمع معلومات شخصية ومالية³⁶ كما تشمل الأنواع الأخرى "الاحتيال عبر الهاتف" (Vishing)، حيث يتصل المحتالون بالضحايا ويتظاهرون بأنهم من مؤسسات معروفة، و"الاحتيال عبر الإنترنت (Scam)"، حيث يستخدم المحتالون مواقع وتطبيقات مزيفة لجمع المعلومات هذه الأساليب تعتمد بشكل أساسي على خداع الضحايا واستغلال ثقتهم، مما يقتضي ضرورة توعية المستهلكين لتحديد هذه المحاولات الاحتيالية.³⁷

في العراق، يمثل قانون العقوبات رقم 111 لسنة 1969 المعدل، والقوانين الأخرى ذات

الإلكتروني من أبرز التحديات التي تواجه المؤسسات التجارية في العصر الحديث، خاصة مع تزايد وتنوع أساليبه. إذ تتزايد التهديدات الأمنية في العصر الرقمي، حيث تشمل سرقة الهوية، القرصنة الإلكترونية، والاحتيال عبر الإنترنت. وفقاً لدراسة أجرتها Javelin Strategy & Research، فإنّ خسائر الاحتيال في الهوية وحدها وصلت إلى 56 مليار دولار في عام 2021، ممّا يعكس الحجم الكبير لهذه الجرائم الإلكترونية. كما أنّ الهجمات الإلكترونية تؤثر بشكل سلبي على ثقة العملاء في الشركات المستهدفة، ممّا يؤدي إلى تراجع في المبيعات والتعاملات التجارية. وتعتبر الأضرار المالية الناتجة عن هذه الهجمات ضارة جداً، حيث يمكن أن يكلف الهجوم الواحد الشركات ما يصل إلى 200,000 دولار.³⁵ فضلاً عن ذلك فإن مكافحة الاحتيال الإلكتروني تواجه تحديات تقنية كبيرة، حيث يتطلب الأمر استخدام تقنيات متقدمة مثل التشفير وتحسين البنية التحتية للإنترنت لضمان حماية فعّالة ضدّ هذه الجرائم. من بين الأنواع الشائعة للاحتيال الإلكتروني، يبرز

Attack Attack 'Winter International Symposium on Information and Communication Technologies 'Cape Town, January 2005.

³⁷ Getfocal.ai. (2024). الاحتيال في التجارة الإلكترونية: استراتيجيات الكشف والوقاية [online] Available at: <https://www.getfocal.ai/ar/blogs/ecommerce-fraud-detection-and-prevention> [Accessed 11 Mar. 2025].

³⁵ kaspersky.com. (2021). نصائح حول كيفية حماية نفسك من الجريمة الإلكترونية. [online] Available at: <https://me.kaspersky.com/resource-center/threats/what-is-cybercrime>.

³⁶ Van der Merwe 'AJ 'Looock 'M 'Dabrowski 'M. (2005) 'Character and Responsibilities included in a

الصلة،

جزءاً من

استراتيجية شاملة تهدف إلى الحفاظ على سمعة المؤسسة وثقة عملائها³⁹. على صعيد آخر، يتطلب منع الاحتيال الإلكتروني من المؤسسات التجارية استخدام مجموعة من الأدوات التقنية مثل المصادقة المعتمدة على المخاطر، وخدمات التحقق من العناوين، وتحليل بيانات العملاء للكشف عن الأنماط والسلوكيات غير العادية كما يجب على المؤسسات وضع سياسات داخلية لمكافحة الاحتيال، وتدريب الموظفين على كيفية التعامل مع المحاولات الاحتيالية، فضلاً عن توعية العملاء بمخاطر الاحتيال الإلكتروني⁴⁰

تواجه المؤسسات التجارية في العراق تحديات متزايدة في مجال الاحتيال الإلكتروني، سواء بصفتها ضحية لهذه الجرائم أو كوسيلة تُستخدم لتنفيذها. فمن جهة، تصبح الشركات هدفاً للمحتالين الذين يسعون لاختراق بياناتها أو الاستيلاء على أموالها، ومن جهة أخرى، قد تلجأ بعض المؤسسات إلى ممارسات احتيالية في

الإطار القانوني الأساسي لمكافحة الاحتيال، بما في ذلك الاحتيال الإلكتروني. ومع ذلك، يرى بعض الخبراء أن هذه القوانين "لم تكن مواكبة لهذه الجرائم" بشكل كامل، خاصةً مع ظهور أساليب جديدة ومتطورة للاحتيال الإلكتروني. فالمادة 456 من قانون العقوبات العراقي تعاقب "بالحبس كل من توصل إلى تسلم أو نقل أو حيازة مال منقول مملوك للغير لنفسه أو إلى شخص آخر، من خلال استخدام طرائق احتيالية، أو اتخاذ اسم كاذب، أو صفة غير صحيحة، أو تقرير أمر كاذب عن واقعة معينة"³⁸

وفي هذا السياق، تبرز المسؤولية القانونية للمؤسسات التجارية في حماية عملائها من الاحتيال الإلكتروني. إذ تقع على عاتق هذه المؤسسات مسؤولية كبيرة في اتخاذ التدابير الأمنية لحماية البيانات الشخصية والمالية للزبائن، مثل توفير أنظمة دفع آمنة، وتحديث برامج الحماية من الفيروسات بشكل مستمر، وتدريب الموظفين على قضايا الأمان والخصوصية إضافة إلى ذلك، يجب على المؤسسات أن تكون مستعدة للإبلاغ عن أي حوادث احتيال إلى الجهات المختصة واتخاذ الإجراءات القانونية ضدّ الجناة هذه التدابير تمثل

⁴⁰ Federal Trade Commission (2018). Cyber Insurance. [online] Federal Trade Commission. Available at: <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance>.

³⁸ المادة 456 من قانون العقوبات العراقي رقم 111 لسنة 1969

³⁹ دليل مكافحة الإحتيال المالي، استراتيجية مكافحة الإحتيال المالي 2022، <https://rulebook.sama.gov.sa/ar>.

الهجمات

الإلكترونية، بما في ذلك تكاليف التحقيق، واستعادة البيانات، والدفاع القانوني تقدّم بعض شركات التأمين تغطية إضافية ضدّ الخسائر الناتجة عن توقف الأعمال أو الاحتيال في تحويل الأموال، ممّا يساعد المؤسسات التجارية على التعافي بسرعة من الأضرار.⁴³

المطلب الثاني: الجهود الدولية والعراقية في مكافحة الجرائم الإلكترونية الواقعة على الأعمال التجارية

تُعدّ الجرائم الإلكترونية ضدّ الشركات تهديداً جديداً في عصر الإنترنت، حيث أصبحت الشركات أكثر عرضة لأشكال مختلفة من الهجمات الإلكترونية، مثل سرقة البيانات والاحتيال وطلب الفدية. ومع تزايد الاعتماد على الإنترنت، قد تفقد معظم الشركات الثقة وتُعرّض سمعتها للخطر، مع احتمالية تكبد خسائر اقتصادية جسيمة.⁴⁴ وهذا يستدعي تعاوناً دولياً لمكافحة هذا النوع من الجرائم العابرة للحدود. ويتطلّب التصدي لهذه التحديات

الإعلانات أو المعاملات الإلكترونية، ممّا يضر بالمستهلكين ويسبب إلى سمعة السوق الرقمي.⁴¹

لذا، تتحمّل المؤسسات التجارية مسؤولية قانونية وأخلاقية لحماية عملائها وموظفيها من الاحتيال الإلكتروني، وذلك من خلال تطبيق تدابير أمنية صارمة لحماية البيانات، وتدريب الموظفين على اكتشاف أساليب الاحتيال وتجنبها، والالتزام بالشفافية في جميع التعاملات التجارية

وفضلاً عن هذه الإجراءات الأمنية يجب على المؤسسات التجارية التزام بالإبلاغ عن حوادث الاحتيال الإلكتروني إلى الجهات المختصة، ممّا يساعد في تتبع الأنشطة الإجرامية وتقديم الجناة للعدالة. هذه الإجراءات تساهم في تعزيز التعاون بين القطاعين العام والخاص للحد من خطر الاحتيال الإلكتروني.⁴²

من جانب آخر تلعب شركات التأمين دوراً مهماً في حماية المؤسسات التجارية من الخسائر الناجمة عن الاحتيال الإلكتروني. إذ تقدّم التأمينات السيبرانية تغطية مالية للخسائر الناتجة عن

<https://www.coalitioninc.com/topics/cyber-insurance-policy-coverages>.

⁴³ Fortinet (2024). What Is Cyber Insurance? Policies, Services, and Coverage. [online] Fortinet. Available at: <https://www.fortinet.com/resources/cyberglossary/cyber-insurance>.

⁴⁴ kaspersky.com. (2021). Ibid

⁴¹ م.د. تحسين علي زعلان، م.د. سامح صبري جاسم، المسؤولية القانونية للإعلانات التجارية الإلكترونية، مجلد 3 عدد 1 (2024): مجلة الفارابي للعلوم الإنسانية، ص36

⁴² Coalition (n.d.). What does a Cyber Insurance Policy Cover? [online] www.coalitioninc.com. Available at:

اتخاذ

تدابير متكاملة تشمل الجوانب القانونية والتقنية والتوعوية.⁴⁵

مديرية مكافحة

الجرائم الإلكترونية، بهدف التحقيق في الجرائم التي تتم عبر الانترنت⁴⁷

تتنوع الجرائم الإلكترونية ضد الشركات، بدءاً من عمليات الاختيال عبر البريد الإلكتروني والإنترنت، حيث يتم خداع العملاء والموظفين للكشف عن معلومات حساسة أو تحويل الأموال إلى حسابات وهمية. كما يشهد عالم الأعمال زيادة في حالات سرقة الهوية وسرقة البيانات المالية أو بيانات بطاقات الدفع، مما قد يؤدي إلى خسائر مالية فادحة. علاوة على ذلك، تتزايد تهديدات الابتزاز الإلكتروني، حيث تُهدد الشركات بتشفير بياناتها والاحتفاظ بها حتى يتم دفع فدية. تُبرز هذه الجرائم الحاجة إلى أنظمة أمنية متكاملة لحماية الشركات، كما تُبرز الحاجة إلى عمل دولي مُنسّق لمواجهة هذه التهديدات.⁴⁶

بالإضافة إلى ذلك، شارك العراق في أغسطس 2024 في اجتماعات اللجنة المعنية بوضع اتفاقية دولية لمكافحة استخدام تكنولوجيا المعلومات لأغراض إجرامية في نيويورك. أكد القائم بأعمال الممثلة الدائمة للعراق في الأمم المتحدة، الدكتور عباس كاظم عبيد على أهمية الاتفاقية المقترحة للتصدي للجريمة السيبرانية، مع التأكيد على ضرورة احترام الصكوك الدولية السابقة وضمن توافق بنود الاتفاقية مع القوانين الوطنية والقيم المجتمعية والدينية والثقافية للعراق.⁴⁸

للمؤسسات الدولية دورٌ رئيس في تنسيق الجهود لمكافحة الجرائم الإلكترونية. على سبيل المثال، تسعى الأمم المتحدة أيضاً إلى تعزيز تعاون الدول الأعضاء من خلال الدعم الفني، بالإضافة إلى وضع تشريعات تُسهّل بناء القدرات لمكافحة الجرائم الإلكترونية. كما أقرّت الجمعية العامة للأمم

حتى تاريخ مارس 2025، بذل العراق جهوداً متعدّدة لمكافحة الجرائم الإلكترونية التي تستهدف الأعمال التجارية. في فبراير 2025، أعلنت وزارة الداخلية العراقية عن استحداث

⁴⁷ محمد الباسم، العراق يستحدث وحدة أمنية خاصة لمكافحة الجرائم الإلكترونية، العربي الجديد مقال الكتروني بتاريخ 21 فبراير 2025 ، <https://www.alaraby.co.uk/society>

⁴⁸ وزارة الخارجية العراقية 2024 العراق يشارك في لجنة اعتماد اتفاقية دولية لمكافحة الجريمة السيبرانية ويؤكد موقفه منها – وزارة الخارجية العراقية : [online] Mofa.gov.iq. Available at: <https://mofa.gov.iq/2024/48798> [Accessed 23 Mar. 2025].

⁴⁵ United Nations (2021). United Nations Convention against Cybercrime. [online] United Nations : Office on Drugs and Crime. Available at: <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>.

⁴⁶ kaspersky.com. (2021). Ibid

المتحدة

وعلى

الرغم من هذه الجهود لا يزال التعاون الدولي يواجه تحديات جسيمة، مثل تناقض التشريعات واللوائح الوطنية، وصعوبات التنسيق بين الدول ذات النظم القانونية المختلفة.⁵¹ كما تعاني معظم الدول من نقص الموارد اللازمة لمكافحة الجرائم الإلكترونية، بالإضافة إلى صعوبات في تدريب الأفراد وسد فجوات الوعي بتعريفاتها. ولمواجهة هذه التحديات، ينبغي على الدول والمؤسسات الدولية العمل على وضع معايير دولية منسقة، وتطوير أطر للتعاون المثمر في تبادل المعلومات، ومساعدة الدول النامية على تطوير قدراتها على مكافحة هذه الجرائم.⁵²

وأخيرًا، مع تزايد إدراك حجم الجرائم الإلكترونية التي تطل القطاعات المختلفة، ويبدو أنّ التحركات العالمية ضدّ هذه الجرائم مستمرة، ولكن لا يزال هناك الكثير ممّا ينبغي عمله. وفي المستقبل، إذا تمّ التنسيق بين الدول والمنظمات المختلفة، وتم تحديث القوانين، وتم تطوير تقنيات

اتفاقيةً جديدةً لتكون بمثابة منصة لتبادل الأدلة الإلكترونية ودعم حقوق الإنسان على الإنترنت. وعلى نحوٍ مماثل، يُنسّق الإنتربول التحقيقات العابرة للحدود الوطنية ويقدم الدعم لمراقبة الهجمات الإلكترونية، ويبدل مجلس أوروبا جهودًا لتنسيق التشريعات الوطنية وتعزيز ممارسات التحقيق، مع مراعاة التعاون الدولي.⁴⁹

ومن أهمّ المساعي الدولية في هذا الاتجاه "الشراكة ضدّ الجرائم الإلكترونية"، التي أطلقها المنتدى الاقتصادي العالمي، بهدف رسم خريطة للجرائم الإلكترونية وتحليل المشهد الإجرامي العالمي. توجد "المبادرة الدولية لمكافحة برامج الفدية" التي تضم 68 دولة ومنظمة تهدف إلى مواجهة هجمات برامج الفدية. وتُعدّ اتفاقية بودابست بشأن الجرائم الإلكترونية معاهدة بارزة تهدف إلى مواءمة القوانين وتحسين التعاون بين الدول لمكافحة الجرائم الإلكترونية.⁵⁰

⁵¹ Unodc (2019). Cybercrime Module 7 Key Issues: Formal International Cooperation Mechanisms. [online] Unodc.org. Available at: <https://www.unodc.org/e4j/ar/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html> [Accessed 11 Mar. 2025].

⁵² National Association of Attorneys General (2020). Global Cooperative Efforts to Prevent Cybercrime. [online] National Association of Attorneys General. Available at: <https://www.naag.org/attorney-general-journal/global-cooperation-efforts-to-prevent-cybercrime/>

⁴⁹ United nation (2021). UN General Assembly adopts landmark convention on cybercrime. [online] United Nations : Office on Drugs and Crime. Available at: <https://www.unodc.org/unodc/en/press/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html>.

⁵⁰ UN General Assembly adopts landmark convention on cybercrime. (2024). <https://www.unodc.org/unodc/en/press/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html>

الأمن،

بل يمتد ليشمل ثقافة

الأمان الرقمي وتعزيز وعي الأفراد والشركات على حد سواء.

فيمكننا أن نأمل في الحصول على فضاء إلكتروني آمن يعزّز الثقة في التكنولوجيا ويحمي الاستقرار الاقتصادي العالمي.⁵³

الخاتمة

وفي هذا السياق يظهر التعاون الدولي كعنصر أساسي في مواجهة الجرائم الإلكترونية العابرة للحدود، إذ يتطلب التصدي لهذه الجرائم تنسيقاً فعالاً بين الدول، وتبادل الخبرات والمعرفة القانونية، وهو ما يعزّز القدرة على الحد من مخاطر الأمن السيبراني ويحمي حقوق الأفراد والشركات في البيئة الرقمية.

وفي الختام يتّضح أنّ البيئة الرقمية قد أحدثت تحولاً جوهرياً في الطريقة التي يتم بها التعامل مع البيانات وحمايتها، ممّا يفرض تحديات قانونية جديدة تستوجب تطوير أطر تشريعية مرنة وقوية. لقد أبرزت التشريعات مثل "اللائحة العامة لحماية البيانات (GDPR)" دورها البارز في حماية حقوق الأفراد، وضمان الشفافية والأمان في التعامل مع البيانات الشخصية، ممّا يعزّز الثقة بين الشركات والمستهلكين ويشجع على الامتثال القانوني. بالإضافة إلى ذلك، فرضت الجرائم الإلكترونية تهديدات مستمرة على المؤسسات التجارية، ممّا يوجب عليها تعزيز التدابير الأمنية والاستجابة الفعالة لحماية بيانات عملائها وسمعتها.

ختاماً، إنّ بناء بيئة رقمية آمنة يتطلب من جميع الأطراف المعنية، من حكومات إلى مؤسسات تجارية وأفراد، تبني ممارسات وقوانين فعالة، وتحقيق التوازن بين حماية الحقوق الرقمية وتحقيق الابتكار والنمو في العالم الرقمي المتسارع.

النتائج

1- أثبتت التشريعات مثل اللائحة العامة لحماية البيانات (GDPR) دورها الحيوي في تعزيز الشفافية وحماية حقوق الأفراد في التعامل مع بياناتهم الشخصية، ممّا يعزّز الثقة بين الشركات والمستهلكين لكنه لا يوجد في العراق قانون محلي محدد لحماية البيانات الشخصية.

إنّ التحديات التي تطرأ في هذا المجال تتطلب جهداً جماعياً من الحكومات، الشركات، والمنظمات الدولية لتطوير استراتيجيات حماية متكاملة ومراقبة فعالة للحد من التهديدات الرقمية. هذا التوجه لا يقتصر فقط على الامتثال القانوني،

⁵³ United nation (2021). Ibid

-2

2- يجب على

الشركات والمؤسسات الاستثمار في تقنيات الأمان الحديثة مثل التشفير المتقدم وأنظمة الكشف عن التسلل، لضمان حماية البيانات الحساسة من أي تهديدات أو هجمات إلكترونية.

ضرورة الاستجابة الفعالة للتهديدات الإلكترونية
مع تزايد الجرائم الإلكترونية، تحتاج المؤسسات إلى تبني تدابير أمنية متقدمة لمواجهة هذه التهديدات وحماية بيانات عملائها بشكل مستمر

3- يجب أن تعمل الحكومات بالتعاون مع القطاع الخاص لتطوير تشريعات فعالة لمكافحة الجرائم الإلكترونية وحماية البيانات الشخصية. هذا التعاون يمكن أن يشمل تبادل المعلومات والتنسيق في الحالات العابرة للحدود.

3- التنسيق بين الدول في مجال مكافحة الجرائم الإلكترونية يُعدّ من الركائز الأساسية في الحد من الجرائم التي تتجاوز الحدود الجغرافية، ويحتاج إلى تبادل المعرفة القانونية والتقنية.

4- ما أن تهديدات الأمان الرقمي تتطور بشكل مستمر، يجب على الحكومات والمشرعين مراجعة وتحديث التشريعات المتعلقة بحماية البيانات الشخصية والأمن الرقمي بشكل دوري لمواكبة أحدث التطورات في هذا المجال.

4- إيجاد توازن بين حماية الأفراد والشركات من المخاطر الرقمية وبين تشجيع الابتكار والنمو في مجال التكنولوجيا، حيث يمكن للأمن الرقمي أن يعزّز البيئة الرقمية ويسهم في الاستقرار والنمو.

5- ينبغي تحفيز الابتكار في مجال الأمان الرقمي، سواء عبر دعم البحث والتطوير في تقنيات الأمان أو من خلال تشجيع الشركات على تبني حلول جديدة ومتطورة لحماية بيانات المستخدمين من المخاطر المتزايدة.

5- تعزيز الوعي بأهمية الأمان الرقمي من أهم الخطوات للحفاظ على بيئة رقمية آمنة، إذ يتعين على الأفراد والشركات فهم المخاطر التي قد تواجهها بياناتهم وكيفية الحماية منها.

التوصيات

1- من الضروري زيادة برامج التدريب والتوعية حول أهمية حماية البيانات الشخصية للأفراد والشركات، وذلك من خلال ورش عمل ومؤتمرات لتوضيح المخاطر الرقمية وأفضل الممارسات للحماية.

المصادر والمراجع
أولاً: القوانين:

1. قانون حماية البيانات الشخصية في مصر، قانون رقم ١٥١ لسنة ٢٠٢٠.

4. فاطمة الزهراء

فرحات، دور التحول الرقمي في تحسين أداء وظائف العلاقات العامة في المؤسسات ٢ العمومية الجزائرية، دراسة تحليلية لصفحة فيسبوك مديرية الصحة والسكان لولاية أم البواقي، رسالة ماجستير، كلية العلوم الاجتماعية والإنسانية، جامعة العربي بن مهيدي- أم البواقي، الجزائر، ٢٠٢٠

5. ماجدة عبد الشافي محمد الهادي خالد منصور، الحماية الدستورية للأمن السيبراني وأثره على النظام العام، جامعة بنها،

6. محمود، لبنى (2023) مخاطر التحول الرقمي في عام ٢٠٢٣ للمؤسسات [online]. مجموعة ريناد المجد لتقنية المعلومات RMG.

Available at: <https://www.rmg-sa.com>.

7. د/ مصطفى أحمد أمين، التحول الرقمي في الجامعات المصرية كمتطلب لتحقيق مجتمع المعرفة، مجلة ٤ الإدارة التربوية، العدد التاسع عشر، ٢٠١٨

8. د. وائل مجدي رزق، دور التحول الرقمي في دعم بيئة الأعمال وجذب الاستثمارات في مصر في ضوء رؤية 2030، أكاديمية السادات للعلوم الإدارية مركز الاستشارات والبحوث والتطوير، مجلة البحوث الإدارية المجلد الأربعون، العدد الرابع، أكتوبر 2022

9. وزارة الخارجية العراقية 2024 العراق يشارك في لجنة اعتماد اتفاقية دولية لمكافحة الجريمة السيبرانية ويؤكد موقفه منها – وزارة الخارجية العراقية. Mofa.gov.iq [online].

Available at:

2. قانون العقوبات العراقي رقم 111 لسنة 1969

ثانياً: الكتب:

1. د/ خالد ممدوح ابراهيم، ابرام العقد الالكتروني، در الفكر الجامعي، 2007. الشكلية القانونية في عقود الإنترنت والتجارة الإلكترونية -

<https://kenanaonline.com/users/KhaledMamdouh/posts/77862>

2. الشوابكة، محمد امين. (2004). جرائم الحاسوب والانترنت، عمان، دار الثقافة للنشر والتوزيع، الأردن، ط1
3. محمد عبد الحميد، نظريات الاعلام واتجاهات التأثير، ط3، عالم الكتب، القاهرة، ٢٠٠٤ ص ١١٠-١١١

ثالثاً: المجلات والدراسات:

1. أحمد فرج أحمد، الرقمنة داخل مؤسسات المعلومات أم خارجها؟ دراسة في الإشكالات ومعايير الاختيار، مجلة دراسات المعلومات، تصدر عن جمعية المكتبات والمعلومات السعودية بالتعاون مع معهد الملك سلمان للدراسات والخدمات الاستشارية، العدد الرابع، يناير، ٢٠٠٩

2. ايمن مظهر بدر، تحقيق التوازن بين الفوائد والمخاطر: التحول الرقمي وحماية الحقوق والخصوصية في العراق، جامعة ديالى كلية العلوم السياسية،

<https://law.uodiyala.edu.iq>

3. الحداد، محرم صالح: محمد، محمد إبراهيم 2021، " الثورة الصناعية الرابعة (الذكاء الاصطناعي – التحول الرقمي) تحديات وفرص الاستحواذ علي القوة الرقمية الجديدة"، سلسلة أوراق السياسات في التخطيط والتنمية المستدامة، الإصدار رقم 8، يناير 2021 معهد التخطيط القومي، مصر.

5. Van der Merwe 'AJ 'Loock 'M ' Dabrowski 'M. (2005) 'Character and Responsibilities included in a Attack Attack 'Winter International Symposium on Information and Communication Technologies 'Cape Town 'January 2005.

6. Getfocal.ai. (2024). الاحتيال في التجارة الإلكترونية: استراتيجيات الكشف والوقاية [online] Available at: <https://www.getfocal.ai/ar/blogs/e-commerce-fraud-detection-and-prevention> [Accessed 11 Mar. 2025].
7. Federal Trade Commission (2018). Cyber Insurance. [online] Federal Trade Commission. Available at: <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance>.
8. Coalition (n.d.). What does a Cyber Insurance Policy Cover? [online] www.coalitioninc.com. Available at: <https://www.coalitioninc.com/topics/cyber-insurance-policy-coverages>.
9. Fortinet (2024). What Is Cyber Insurance? Policies, Services, and Coverage. [online] Fortinet. Available at:

<https://mofa.gov.iq/2024/48798>

[Accessed 23 Mar. 2025].

10. يحيى يوسف فلاح حسن، التنظيم القانوني للعقود الإلكترونية، جامعة النجاح الوطنية، الأطروحة استكمالاً لنيل درجة الماجستير في القانون الخاص بكلية الدراسات العليا في جامعة النجاح الوطنية في نابلس، فلسطين 2007.

رابعاً: المراجع الأجنبية:

1. OECD, (2020), " A Roadmap Toward A Common Framework for Measuring the Digital Economy ", Report for the G20 Digital Economy Task Force Saudi Arabia, 2020.
2. Muehlburger, M., Rueckel, D., & Koch, S. (2019), "A framework of factors enabling digital transformation"
3. Maye, Terry & Others, Transforming Higher Education Through Technology Enhanced Learning, The Higher Education Academy, York Science Park, Heslington, 2009,p11.
4. World Economic Forum , Digital Transformation Initiative Professional Services Industry, White Paper, Committed To Improving The State Of The World, January 2017, p2.

ss/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html.

15. *UN General Assembly adopts landmark convention on cybercrime.* (2024).

<https://www.unodc.org/unodc/en/press/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.htm>.

<https://www.fortinet.com/resources/cyberglossary/cyber-insurance>.

10. **United Nations (2021). United Nations Convention against Cybercrime.** [online] United Nations : Office on Drugs and Crime. Available at: <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>.

11. **UN General Assembly adopts landmark convention on cybercrime.** (2024). <https://www.unodc.org/unodc/en/press/releases/2024/December/un-general-assembly-adopts-landmark-convention-on-cybercrime.html>

12. **Unodc (2019). Cybercrime Module 7 Key Issues: Formal International Cooperation Mechanisms.** [online] Unodc.org. Available at: <https://www.unodc.org/e4j/ar/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html> [Accessed 11 Mar. 2025].

13. **National Association of Attorneys General (2020). Global Cooperative Efforts to Prevent Cybercrime.** [online] National Association of Attorneys General. Available at: <https://www.naag.org/attorney-general-journal/global-cooperation-efforts-to-prevent-cybercrime/>

14. **United nation (2021). UN General Assembly adopts landmark convention on cybercrime.** [online] United Nations : Office on Drugs and Crime. Available at: <https://www.unodc.org/unodc/en/pre>

