

مخاطر الاقتصاد الرقمي: التحديات الأمنية والخصوصية

Risks of the Digital Economy: Security and Privacy Challenges

ادبوب سارة، أستاذ محاضر ب، جامعة الجزائر 3، الجزائر

eddeboub.sara@univ-alger3.dz

لسبيع مريم، أستاذ محاضر ب، جامعة 20 أوت 1955 - سكيكدة (الجزائر)،

m.lesbaa@univ-skikda.dz

تاريخ الاستلام: 2025/07/16 ؛ تاريخ القبول: 2025/12/01

مستخلص:

يهدف هذا البحث إلى تحليل شامل للتهديدات الأمنية وانتهاكات الخصوصية المتنامية في الاقتصاد الرقمي، حيث تكمن أهمية البحث في المساهمة في حماية نمو الاقتصاد الرقمي، صون خصوصية الأفراد، تقليل الخسائر المالية الناجمة عن الجرائم الإلكترونية، وبناء الثقة الرقمية، يقدم البحث في نهايته حلول وتوصيات شاملة تشمل الجوانب التقنية (مثل التشفير المتقدم والذكاء الاصطناعي في كشف التهديدات) والتشريعية والتوعوية (كالتعاون الدولي وزيادة الوعي الرقمي)، بهدف بناء بيئة رقمية أكثر أماناً ومرونة تدعم النمو المستدام.

الكلمات المفتاحية: اقتصاد رقمي؛ تشفير متقدم؛ جرائم إلكترونية؛

تصنيف JEL: L86 ؛ K24 ؛ O33

Abstract:

This research aims to comprehensively analyze the growing security threats and privacy violations within the digital economy. The study's significance lies in its contribution to protecting the growth of the digital economy, preserving individual privacy, reducing financial losses resulting from cybercrimes, and building digital trust. Ultimately, the research proposes comprehensive solutions and recommendations encompassing technical aspects (such as advanced encryption and AI in threat detection), as well as legislative and awareness-focused measures (like international cooperation and increased digital literacy), all with the goal of fostering a more secure and resilient digital environment that supports sustainable growth.

Keywords: Digital Economy; Advanced Encryption; Cybercrimes.**Jel Classification Codes :** L86 ; K24 ; O33

مقدمة

يشكل الاقتصاد الرقمي اليوم ركيزة أساسية للاقتصاد العالمي، حيث يساهم بشكل كبير في خلق القيمة المضافة، وعلى عكس الموارد التقليدية النادرة، يعتمد الاقتصاد الرقمي على المعرفة والابتكار، مما يجعله موردا متجددا وغير محدود.

يشهد العالم تحولا جذريا نحو الاقتصاد الرقمي، الذي يعد المحرك الأساسي للابتكار والنمو في عصرنا الحالي، هذا التحول يعني الاعتماد المتزايد على التقنيات الرقمية في كل جانب من جوانب الحياة اليومية والأعمال، من التجارة الإلكترونية والمعاملات المصرفية عبر الإنترنت، إلى الخدمات الحكومية والتواصل الاجتماعي، ومع أن هذا التوسع يجلب معه فرصا هائلة لتحسين الكفاءة، تسهيل الوصول إلى المعلومات، وفتح أسواق جديدة، إلا أنه يولد أيضا مجموعة كبيرة من التحديات الأمنية والسيبرانية.

إن الفهم العميق لهذه التحديات والمخاطر وتطوير استراتيجيات دفاعية فعالة أصبح ضرورة قصوى للحفاظ على ثقة المستخدمين وضمان استمرارية النمو المستدام للاقتصاد الرقمي.

الإشكالية: تتمثل إشكالية الدراسة في:

كيف تهدد المخاطر الأمنية والخصوصية استقرار الاقتصاد الرقمي؟

أهمية البحث:

تكمن أهمية هذا البحث في كونه يسعى إلى حماية نمو الاقتصاد الرقمي وتعزيز مرونته ضد الهجمات السيبرانية، مع التركيز على حماية خصوصية الأفراد وحقوقهم في بيئة رقمية متزايدة التعقيد، عن طريق تحديد أبرز التهديدات وتقديم حلول عملية. كما يهدف البحث إلى تقليل الخسائر المالية الناجمة عن الجرائم الإلكترونية، وبناء الثقة الرقمية الضرورية لتبني واسع للخدمات الرقمية.

الهدف من البحث :

يهدف هذا البحث إلى تحليل معمق للتهديدات الأمنية وانتهاكات الخصوصية المتزايدة التي تواجه الاقتصادات والمجتمعات في ظل التوسع المتسارع للاقتصاد الرقمي، سيركز البحث على فهم آليات عمل هذه المخاطر، من هجمات الفدية (Ransomware) والتصيد الاحتيالي (Phishing) إلى الاستغلال غير المشروع للبيانات الشخصية، وتحديد التكاليف الاقتصادية الباهظة لهذه

الجرائم، سواء كانت مباشرة كخسائر مالية أو غير مباشرة كفقدان الثقة وتدهور السمعة، بالإضافة إلى تقييم التداعيات على خصوصية الأفراد وأمن بياناتهم الحساسة.

أولاً: الاقتصاد الرقمي - خلفية نظرية-

يعد الاقتصاد الرقمي نظام اقتصادي متكامل يعتمد على التكنولوجيا الرقمية كمحرك رئيسي، حيث يركز هذا النظام على بنية تحتية متطورة من الأجهزة والبرمجيات والشبكات التي تمكن من إجراء المعاملات التجارية والاقتصادية عبر الإنترنت، من أبرز الأمثلة على هذه الآليات التجارة الإلكترونية والمعاملات الرقمية، مما يعكس بوضوح التطور الهائل لدور الإنترنت في إعادة تشكيل الاقتصاد العالمي وتغيير أنماط الحياة.

1. تعريف الاقتصاد الرقمي

الاقتصاد الرقمي هو نظام اقتصادي يعتمد بشكل أساسي على إنتاج المعرفة وتطبيقها، فهو يستثمر بكثافة في البحث والتطوير، ويستفيد من الكفاءات البشرية المؤهلة لابتكار حلول مبتكرة للتحديات الاقتصادية والاجتماعية والسياسية، يعتبر هذا النوع من الاقتصاد محركاً رئيسياً للنمو الاقتصادي المستدام، حيث يعتمد على المعرفة كأهم مورد.

كما يعرف الاقتصاد الرقمي بأنه نظام اقتصادي متكامل يعتمد على التكنولوجيا الرقمية والمعلومات، فهو يشمل مجموعة واسعة من الأنشطة الاقتصادية، مثل التجارة الإلكترونية، والخدمات الرقمية، المعلومات والمعرفة تلعب دور حاسم في هذا النظام، حيث تعتبر المحرك الرئيسي للابتكار والنمو. (الرزو، 2006، صفحة 13)

يمكن تعريف الاقتصاد الرقمي بأنه محرك رئيسي للابتكار، يعتمد بشكل أساسي على المعلومات والمعرفة، حيث تعتبر المعلومات هي المورد الأهم والأكثر قيمة، وتستخدم في اتخاذ القرارات وتحسين العمليات في جميع المجالات الاقتصادية.

2. خصائص الاقتصاد الرقمي

يمثل الاقتصاد الرقمي تحولا جذريا في النشاط الاقتصادي، حيث يعتمد على التكنولوجيا الرقمية مثل الإنترنت والبيانات الضخمة والتجارة الإلكترونية، وله عدة خصائص ممثلة في الجدول التالي:

الجدول رقم 01: خصائص الاقتصاد الرقمي

الخاصية	الشرح
الاعتماد على التكنولوجيا الرقمية	يعتمد الاقتصاد الرقمي بشكل كبير على تقنيات المعلومات و الثروة الفكرية والمعلوماتية كقوة دافعة رئيسية للاقتصاد
العمليات العالمية	يسمح الاقتصاد الرقمي بعمليات اقتصادية عالمية، حيث يمكن للشركات الوصول إلى أسواق جديدة عبر الإنترنت
أهمية البيانات	تعد البيانات مورد حيوي في الاقتصاد الرقمي، حيث تستخدم لاتخاذ القرارات الاستراتيجية وتحسين العمليات
الشخصنة	تصبح التجربة أكثر ارتباطاً باحتياجات العميل الفردية من خلال الشخصنة، كما يسمح لهم باستخدام المعرفة والمعلومات وإنتاجها وتطويرها كعامل رئيسي في القيمة الاقتصادية المنتجة، مع التركيز بشكل أساسي على أهمية المهارات البشرية الفكرية والإبداعية
الأمن السيبراني	تتطلب مفاوضات العقود الإلكترونية توافر الضمانات وبيئة أمنية تسمح للأشخاص بإجراء مختلف المعاملات التجارية وحماية البيانات والأنظمة من الهجمات السيبرانية

SOURCE : (Freijat, 2023, p. 7_8)

3. مؤشرات الاقتصاد الرقمي

تؤدي مؤشرات الاقتصاد الرقمي دوراً حاسماً في فهم مدى تقدم الدول في التحول الرقمي وتحديد السياسات اللازمة لدعم النمو الاقتصادي المستدام، فعن طريق تتبع هذه المؤشرات يمكن للحكومات والشركات والمستثمرون اتخاذ قرارات مدروسة لتعزيز مكانتهم في الاقتصاد العالمي الرقمي. هناك العديد من هذه المؤشرات منها:

- مؤشر التنافسية الرقمية العالمية (WDC): يصدره المنتدى الاقتصادي العالمي ويقيس قدرة الدول على تبني واستخدام التكنولوجيات الرقمية. (IMD, 2024)
- مؤشر تنمية الحكومة الإلكترونية (EGDI): الصادر عن الأمم المتحدة، يستند هذا المؤشر إلى مسح شامل لوجود الإنترنت في جميع الدول الأعضاء في الأمم المتحدة الـ 193، والذي يقيم مواقع الويب الوطنية وكيفية تطبيق سياسات واستراتيجيات الحكومة الإلكترونية بشكل عام وفي قطاعات محددة لتقديم الخدمات الأساسية. (EGOVKB, 2025)

• مؤشر الجاهزية الشبكية (the network readiness index): هو مقياس لمدى استعداد دولة ما للاستفادة من التكنولوجيا الرقمية، ويعتمد على تقييم بنيتها التحتية الرقمية، واستخدام التكنولوجيا، وبيئة الأعمال الرقمية. (Escwa, 2025)

• المؤشر العربي للاقتصاد الرقمي (Arab Digital Economy Index): يهدف المؤشر إلى تقييم مدى تقدم الدول العربية في التحول الرقمي، وتوفير رؤية قيمة لصناع القرار لتعزيز النمو الاقتصادي المستدام من خلال الاستفادة من التقنيات الرقمية. (الاتحاد العربي للاقتصاد الرقمي، 2025)

ثانيا: التحديات الأمنية في الاقتصاد الرقمي

1. أنواع الهجمات الالكترونية:

تتطور أساليب الهجمات الالكترونية باستمرار، وتستهدف نقاط الضعف في الأنظمة والشبكات الرقمية، من أبرز هذه الأنواع:

1.1 الاختراقات والتهديدات السيبرانية: تتمثل في:

• هجمات برامج الفدية (Ransomware): تعتبر هذه الهجمات من أخطر التهديدات، حيث تتم بتشفير بيانات الضحايا والمطالبة بفدية مالية لإعادة الوصول إليها، من الأمثلة البارزة على ذلك هو هجوم WannaCry الذي انتشر في العالم في سنة 2017، مما أثر على مئات الآلاف من أجهزة الكمبيوتر في أكثر من 150 دولة، بما في ذلك البنى الأساسية كالمستشفيات والشركات الكبرى، وتسبب في خسائر كبيرة بمليارات الدولارات. (الجزيرة، 2017)

يطور مجرمو الانترنت أساليبهم باستمرار مستهدفين المؤسسات والشركات التي تعتمد بشكل كبير في أعمالها على البيانات الرقمية، حيث تعد برامج الفدية الضارة نوعا من البرامج الخبيثة التي يستخدمها مجرمو الإنترنت لمنع الوصول إلى البيانات الهامة، أو إتلافها، أو نشرها، ما لم تدفع فدية، بينما تستهدف برامج الفدية التقليدية الأفراد والشركات على حد سواء. ظهرت أنواع جديدة مثل برامج الفدية التي يديرها الإنسان وبرامج الفدية كخدمة، والتي تشكل تهديدا أكبر للمؤسسات الكبرى.

في برامج الفدية التي يديرها الإنسان، تستغل مجموعات من المهاجمين معرفتهم الجماعية لاختراق شبكات الشركات، قبل طلب الفدية، يدرسون الشركة لتحديد نقاط الضعف، وقد

يكشفون عن وثائق مالية لتحديد مبلغ الفدية، أما في نموذج برامج الفدية كخدمة، فيقوم مطورو برامج الفدية بإنشائها ثم يوظفون شركات تابعة أخرى لاختراق شبكات المؤسسات وتثبيت البرامج الضارة، ويقتسمون الأرباح المتفق عليها، وكمثال على ذلك نجد برامج الفدية الخبيثة Akira و هي برامج ضارة متطورة نشطة منذ بداية عام 2023، تستهدف أنظمة Windows و Linux على حد سواء، يستغل المهاجمون نقاط الضعف في خدمات VPN، خاصة تلك التي تفتقر إلى المصادقة متعددة العوامل، للوصول الأولي، منذ ظهورها أثرت Akira على أكثر من 250 مؤسسة وطالبت بحوالي 42 مليون دولار أمريكي كفدية.

تتسبب جميع أنواع برامج الفدية الضارة في أضرار جسيمة للأفراد والمؤسسات المستهدفة، قد تستغرق إعادة تشغيل الأنظمة المتأثرة أياما أو أسابيع أو حتى أشهر، مما يؤدي إلى خسارة في الإنتاجية والمبيعات، كما يمكن أن تتضرر سمعة المؤسسات لدى العملاء والمجتمع. (microsoft, 2025)

● **التصيد الاحتيالي (Phishing):** تتم هذه الهجمات عبر رسائل البريد الإلكتروني أو الرسائل النصية أو مواقع ويب مزيفة تبدو وكأنها شرعية، تعتمد هذه الهجمات على خداع المستخدمين للحصول على معلومات حساسة مثل كلمة المرور أو تفاصيل بطاقات الائتمان، ويؤدي هذا النوع من الهجمات إلى اختراقات للبيانات وسرقة الهوية، مما يكلف الشركات والأفراد مبالغ طائلة. تظهر الإحصائيات الأخيرة ارتفاعا مستمرا في تهديدات التصيد الاحتيالي، فمنذ سنة 2019، زادت هجمات التصيد الاحتيالي بنسبة 150% سنويا، وقد سجلت مجموعة عمل مكافحة التصيد الاحتيالي (APWG) رقما قياسيا في سنة 2022، حيث تجاوز عدد مواقع التصيد الاحتيالي المبلغ عنها 4.7 مليون موقع، كما تشير بيانات Proofpoint لعام 2022 إلى أن 84% من المؤسسات تعرضت لهجوم تصيد احتيالي ناجح واحد على الأقل. (Badman, 2023)

2.1 تزوير الهوية وسرقة البيانات

تعتبر سرقة الهوية وتزويرها من أخطر النتائج المترتبة على الهجمات السيبرانية التي تستهدف الأفراد والمؤسسات على حد سواء، يستغل المهاجمون المعلومات الشخصية والحساسة التي يتمكنون من الحصول عليها بطرق غير مشروعة من خلال اختراقات البيانات الواسعة أو هجمات التصيد الاحتيالي.

يعد اختراق بيانات فيسبوك (Meta حاليا) في عام 2021 مثالا واضحا على مدى خطورة هذه التهديدات، حيث تمّ تسريب بيانات أكثر من 530 مليون مستخدم حول العالم، شملت البيانات المسربة معلومات حساسة مثل أرقام الهواتف، عناوين البريد الإلكتروني، وتواريخ الميلاد، هذا الاختراق سلط الضوء على هشاشة المعلومات الشخصية على المنصات الكبرى.

كما أنّ تسريبات "كامبريدج أناليتيكا" مثّلت استخداما غير مشروع لبيانات مستخدمي فيسبوك بهدف التأثير على الانتخابات الأمريكية، حيث كشفت هذه الحادثة عن حجم المخاطر المتعلقة باستغلال البيانات الشخصية في التلاعب بالرأي العام والعمليات الديمقراطية.

وكمثال آخر نجد هجوم إلكتروني على هيئة التأمين الصحي الأسترالية (Medibank)، والذي أدّى إلى تسريب بيانات طبية لأكثر من 9.7 مليون شخص. تبرز هذه الواقعة مدى حساسية البيانات الصحية وحاجتها إلى أعلى مستويات الحماية لمنع استغلالها أو الإضرار بخصوصية الأفراد. (مخلف، 2025)

2. التكاليف الاقتصادية للجرائم الإلكترونية:

لا تقتصر تداعيات الجرائم الإلكترونية على فقدان البيانات وانتهاك الخصوصية، بل تتجاوز ذلك لتشمل تكاليف اقتصادية باهظة تتحملها الشركات والاقتصادات العالمية.

● متوسط تكلفة خرق البيانات: وفقا لتقرير IBM لسنة 2024، يبلغ متوسط تكلفة خرق البيانات 4.88 مليون دولار أمريكي بزيادة قدرها 10% مقارنة بسنة 2023، تشمل هذه التكاليف التحقيقات، استعادة البيانات، الإشعارات للعملاء المتأثرين، الغرامات التنظيمية، وفقدان الثقة في العلامة التجارية، كلما طال أمد اكتشاف الخرق واحتوائه، زادت التكاليف المرتبطة به. (ibm, 2025)

● الخسائر المتوقعة عالميا بحلول 2025: تشير تقديرات Cybersecurity Ventures إلى أن الخسائر العالمية الناجمة عن الجرائم الإلكترونية قد تصل إلى 10.5 تريليون دولار أمريكي بحلول عام 2025، حيث كانت تساوي 3 تريليون دولار أمريكي في عام 2015، يعكس هذا الرقم حجم المشكلة المتزايد ويؤكد على الحاجة الملحة للاستثمار في الأمن السيبراني، فهذه الخسائر تؤثر على جميع القطاعات الاقتصادية، من الشركات الصغيرة والمتوسطة إلى المؤسسات الحكومية والبنى التحتية الحيوية. (Morgan, 2020)

ثالثا: تحديات الخصوصية في الاقتصاد الرقمي

مع تزايد جمع البيانات الشخصية من قبل الشركات والمنصات الرقمية، تبرز تحديات كبيرة تتعلق بانتهاك الخصوصية وكيفية حماية هذه البيانات

1. انتهاكات الخصوصية

● جمع البيانات غير المصرح به: تقوم العديد من الشركات بجمع كميات هائلة من البيانات الشخصية دون موافقة صريحة أو وعي كامل من المستخدمين، هذا الجمع غير المصرح به للبيانات يثير مخاوف جدية بشأن كيفية استخدامها وتخزينها. تظهر دراسة استقصائية لـ PWC في نوفمبر 2024 أن المستهلكين في الشرق الأوسط لديهم مخاوف متزايدة بشأن خصوصية وأمن البيانات، خاصة مع تغلغل التقنيات الناشئة في حياتهم اليومية، يبحث 83% من المشاركين عن ضمانات تؤكد أن أجهزتهم تحمي معلوماتهم، مما يؤكد على الأهمية القصوى للثقة في التقنيات. تعكس هذه المخاوف أيضا رغبة 59% من المشاركين في عدم تلقي رسائل تسويقية أثناء تصفح الإنترنت، ما يشير إلى حرص المستهلكين على التحكم في معلوماتهم الشخصية. بالإضافة إلى ذلك، تعرض 31% من المستهلكين الإقليميين (مقارنة بـ 39% عالميا) لأنشطة مشبوهة عبر الإنترنت، بما في ذلك رسائل البريد الإلكتروني غير المرغوب فيها ومحاولات التصيد الإلكتروني، هذا يشير إلى أن المستهلكين في منطقة الشرق الأوسط يدركون تماما المخاطر التي تهدد خصوصيتهم على الإنترنت عند استخدام المنصات الرقمية، مما يعكس تزايد الوعي العام بهذه القضية، غالبا ما يتم استخدام هذه البيانات لتخصيص الإعلانات أو تحليل سلوك المستخدمين، ولكنها قد تستغل لأغراض أخرى غير مرغوبة. (pwc، 2024)

● استغلال البيانات من قبل الشركات الكبرى: شهدنا أمثلة متعددة سابقا على استغلال الشركات الكبرى للبيانات الشخصية، من أبرزها فضيحة كامبريدج أناليتيكا مع فيسبوك، حيث تم جمع بيانات ملايين المستخدمين واستخدامها لأغراض سياسية دون علمهم أو موافقتهم، تسلط هذه الفضيحة الضوء على المخاطر الكبيرة المرتبطة بتركيز كميات هائلة من البيانات الشخصية في أيدي عدد قليل من الشركات العملاقة، ومدى تأثير ذلك على الديمقراطية والخصوصية الفردية.

2. القوانين واللوائح العالمية

لمواجهة هذه التحديات بدأت الحكومات والمنظمات الدولية في سن قوانين ولوائح تهدف إلى حماية البيانات الشخصية وتعزيز خصوصية المستخدمين:

- **اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي:** تعد GDPR من أقوى قوانين حماية البيانات في العالم، صدرت في 27 أبريل 2016 ودخلت حيز التنفيذ في 25 ماي 2018، (liberoassurance, 2025) وتفرض قواعد صارمة على الشركات فيما يتعلق بجمع وتخزين ومعالجة البيانات الشخصية للمواطنين الأوروبيين، كما تفرض عقوبات مالية كبيرة على الشركات المخالفة، قد تصل إلى 4% من إيراداتها السنوية العالمية أو 20 مليون يورو، أيهما أعلى، وقد أثرت هذه اللائحة بشكل كبير على ممارسات الشركات العالمية وأجبرتها على إعادة تقييم سياسات الخصوصية لديها. (uniview, 2018)

- **قانون حماية البيانات الشخصية في السعودية (PDPL):** تعتبر المملكة العربية السعودية من الدول الرائدة في المنطقة التي سنت تشريعات لحماية البيانات، صدر قانون "حماية البيانات الشخصية" في المملكة العربية السعودية بتاريخ 16 سبتمبر 2021، بعد موافقة مجلس الوزراء، ونشر في 24 سبتمبر 2022، يضع هذا القانون إطار شامل لحماية البيانات الشخصية، حيث يتضمن:

- شروط معالجة البيانات الشخصية: يحدد القانون القواعد التي يجب الالتزام بها عند جمع وتخزين ومعالجة البيانات.
- حقوق أصحاب البيانات الشخصية: يمنح الأفراد سلسلة من الحقوق المتعلقة ببياناتهم مما يعزز سيطرتهم عليها.
- معايير مفصلة لمعالجة البيانات: يوفر إطار واضح للمعايير التي يجب اتباعها لضمان التعامل الآمن والمسؤول مع البيانات.
- التزامات الجهات المعنية: يوضح القانون المسؤوليات الملقاة على عاتق الهيئات عند معالجتها للبيانات الشخصية.

- العقوبات المترتبة على عدم الامتثال: يحدد القانون العقوبات التي تواجه الشركات والهيئات العامة العاملة داخل المملكة في حال عدم التزامها بأحكامه، مما يؤكد على جدية تطبيق هذه اللوائح. (2025، daam)

دخل قانون حماية البيانات الشخصية حيز التنفيذ في 18 مارس 2023، ويهدف إلى تنظيم جمع ومعالجة وتخزين البيانات الشخصية لضمان حقوق الأفراد، يتماشى هذا القانون مع أفضل الممارسات العالمية ويسعى إلى تعزيز الثقة في الاقتصاد الرقمي بالمملكة. (2025، sdaia)

ثالثاً: الحلول والتوصيات

لمواجهة التحديات الأمنية والخاصة بالخصوصية في الاقتصاد الرقمي، يتطلب الأمر تبني نهج شامل يجمع بين الحلول التقنية والتشريعية، بالإضافة إلى زيادة الوعي.

1. حلول تقنية

● **التشفير المتقدم (End-to-End Encryption):** التشفير المتقدم من الأدوات الأساسية لحماية البيانات، يضمن هذا النوع من التشفير أن تظل مفاتيح التشفير سرية بين طرفي الاتصال فقط وبالتالي ضمان بقاء الرسائل والبيانات خاصة وأمنة من لحظة إرسالها إلى لحظة استقبالها، حيث لا يمكن لأي طرف ثالث - بما في ذلك مزود الخدمة- الوصول إلى محتواها مما يوفر خصوصية وأمان فائقين للبيانات، وهو ما يساهم في حماية خصوصية المستخدمين ومعلوماتهم الحساسة في العالم الرقمي المتزايد التعقيد.

ينصح بتطبيق التشفير من طرف إلى طرف (E2EE) في جميع الاتصالات الحساسة والمعاملات المالية لضمان أقصى درجات الأمان، ذلك أنه يستخدم عدة تقنيات لتبادل المفاتيح وتشفير البيانات، أبرزها:

- الخصوصية الجيدة جداً (PGP - Pretty Good Privacy): برنامج تشفير وفك تشفير يوفر الخصوصية والمصادقة للرسائل النصية والبريد الإلكتروني، باستخدام تشفير قوي.

- المفتاح الفريد المشتق لكل معاملة (DUKPT - Derived Unique Key Per Transaction): طريقة لإدارة مفاتيح التشفير، حيث يتم إنشاء مفتاح فريد لكل عملية إرسال من قيمة

ثابتة، هذا يعني أنه حتى لو تم اختراق مفتاح عملية واحدة، فإن البيانات السابقة واللاحقة تظل آمنة.

- تبادل مفاتيح ديفي-هيلمان (D-H - Diffie–Hellman key exchange) بروتوكول آمن لتبادل مفاتيح التشفير عبر قناة اتصال عامة، مما يتيح للطرفين إنشاء مفتاح سري مشترك دون الحاجة لتبادله بشكل مباشر. يطبق تشفير E2EE على نطاق واسع في العديد من التطبيقات والخدمات التي تتطلب أمانا عاليا للبيانات مثل:

- برامج المراسلة الآمنة والبريد الإلكتروني: مثل PGP و S/MIME ملحقات بريد الإنترنت الآمنة متعددة الأغراض.
 - تطبيقات المحادثة الفورية: مثل iMessage ، OTR (Off-the-Record Messaging) ، وتلغرام.
 - خدمات التخزين السحابي: مثل Tresorit و MEGA.
 - تقنيات الاتصال اللاسلكي: مثل TETRA الشبكة الأرضية اللاسلكية المحسنة .
- (<https://academy.binance.com>, 2023)

● **الذكاء الاصطناعي لاكتشاف التهديدات:** يشير الذكاء الاصطناعي (AI) والتعلم الآلي (ML) في سياق الأمن السيبراني إلى استخدام هذه التقنيات لتعزيز قدرة الأنظمة والشبكات على اكتشاف التهديدات السيبرانية ومكافحتها، يوظف الذكاء الاصطناعي لتحليل كميات هائلة من البيانات، بهدف تحديد الأنماط والسلوكيات غير العادية التي قد تشير إلى هجمات محتملة، من خلال هذا التحليل المتقدم، يمكن للمنظمات تعزيز قدرتها على مواجهة التهديدات السيبرانية وحماية بياناتها ومعلوماتها الحساسة، حيث يمكن للأنظمة المدعومة بالذكاء الاصطناعي تحليل كميات هائلة من البيانات لتحديد الأنماط المشبوهة، اكتشاف التهديدات الجديدة، والاستجابة للهجمات بشكل أسرع وأكثر فعالية من الأنظمة التقليدية، على سبيل المثال يمكن للذكاء الاصطناعي كشف هجمات التصيد الاحتيالي المتطورة أو تحديد سلوكيات البرامج الضارة قبل أن تتسبب في أضرار جسيمة. (دحمان، 2023، صفحة 607)

2. حلول تشريعية وتوعوية

• تعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية: تعتبر اتفاقية الجريمة الإلكترونية (تعزيز التعاون الدولي لمكافحة الجرائم المرتكبة عبر أنظمة تكنولوجيا المعلومات والاتصالات) هي أول معاهدة للعدالة الجنائية الدولية يتم التفاوض بشأنها منذ أكثر من 20 سنة، تنشئ الاتفاقية إطارا عالميا غير مسبوق ومنصة للتعاون لمكافحة الجريمة الإلكترونية، مع ضمان حماية حقوق الإنسان والتأكد من أن الفضاءات الرقمية العالمية محمية وشاملة وقادرة على التكيف مع التهديدات الناشئة.

إلى جانب أبعادها القانونية تعطي الاتفاقية أولوية للشمولية والإنصاف، حيث تقدم دعما حيويا لبناء القدرات للدول ذات الموارد المحدودة، كما تقر بأن الأمن السيبراني ليس مجرد قضية تقنية، بل ضرورة لحقوق الإنسان، مما يضمن حماية المجتمعات المهمشة و الحريات الأساسية في العصر الرقمي، فنظرا للطبيعة العابرة للحدود للجرائم الإلكترونية، فإن التعاون الدولي أمر حاسم لمكافحتها، حيث يشمل ذلك تبادل المعلومات، تنسيق الجهود الأمنية، وملاحقة المجرمين السيبرانيين عبر الحدود، توقيع الاتفاقيات الدولية وتوحيد التشريعات يمكن أن يسهل هذا التعاون ويعزز القدرة على الرد على التهديدات العالمية. (United Nations, 2025)

• زيادة الوعي الرقمي للمستخدمين والشركات: يعتبر العامل البشري حلقة وصل ضعيفة في سلسلة الأمن السيبراني، لذلك فإن التوعية الأمنية نعد عنصرا أساسيا في سياسة الأمن المتبعة في الشركات، وتشمل تدريب الموظفين واختبارهم بهدف حمايتهم من الجرائم الإلكترونية، مثل التصيد الاحتيالي والهجمات الأخرى.

تساعد دورات التوعية الأمنية الموظفين على التعرف على التهديدات التي قد تعرض البيانات والأنظمة الحساسة للخطر، وتجنبها والإبلاغ عنها، وتشمل هذه التهديدات التصيد الاحتيالي (Phishing)، والبرامج الضارة (Malware)، وبرامج الفدية (Ransomware)، وبرامج التجسس (Spyware)، وكجزء من هذه الدورات، تجرى محاكاة للهجمات (سواء التصيد الاحتيالي أو غيره) بهدف اختبار سلوك الموظفين وغرس الممارسات الصحيحة لديهم. (Barracuda, 2025)

بتطبيق هذه الحلول المتكاملة يمكن للأعمال الرقمية بناء بيئة أكثر أمان ومرونة، مما يدعم النمو المستدام للاقتصاد الرقمي مع حماية حقوق وخصوصية الأفراد.

الخلاصة:

في ظل التحول الرقمي المتسارع الذي يشهده العالم، تبرز التحديات الأمنية والتهديدات السيبرانية كعقبة رئيسية تعترض طريق التقدم التكنولوجي والاقتصادي، وقد كشفت هذه الدراسة عن حجم المخاطر المتنامية التي تواجه الأفراد والشركات على حد سواء، بداية من هجمات برامج الفدية والتصيد الاحتيالي، مروراً بتكاليفها الاقتصادية الباهظة، ووصولاً إلى انتهاكات الخصوصية واستغلال البيانات.

نتائج الدراسة:

- تزايد وتطور الهجمات السيبرانية: أكدت الدراسة أن الهجمات الإلكترونية ليست مجرد حوادث عابرة، بل هي تهديدات متطورة ومتنامية تستغل الثغرات التقنية والبشرية، مما يتطلب يقظة مستمرة واستراتيجيات دفاعية مرنة.
 - التكاليف الباهظة للانتهاكات: أظهرت الدراسة أن التداعيات المالية للجرائم الإلكترونية ضخمة، وتشمل تكاليف مباشرة لاستعادة الأنظمة وتعويض الأضرار، بالإضافة إلى خسائر غير ملموسة مثل فقدان الثقة والإضرار بالسمعة.
 - تحديات الخصوصية: أبرزت الدراسة أن جمع البيانات الشخصية بكميات هائلة يثير مخاوف جدية بشأن الخصوصية، وأن استغلال هذه البيانات من قبل الشركات الكبرى يمكن أن تكون له عواقب وخيمة على الأفراد والمجتمعات.
 - أهمية الأطر القانونية: أهمية وفاعلية اللوائح والقوانين العالمية، مثل اللائحة العامة لحماية البيانات (GDPR) وقانون حماية البيانات الشخصية السعودي (PDPL)، في فرض معايير صارمة لحماية البيانات وتعزيز المساءلة.
- توصيات الدراسة:

بناءً على النتائج والتحديات المطروحة نقدم التوصيات التالية لتعزيز الأمن الرقمي والخصوصية في الاقتصاد الرقمي:

- الاستثمار في الحلول التقنية المتقدمة: يجب على الشركات والحكومات تكثيف الاستثمار في التشفير المتقدم (End-to-End Encryption) وتطوير أنظمة الذكاء الاصطناعي (AI) والتعلم الآلي (Machine Learning) لاكتشاف التهديدات والاستجابة لها بشكل استباقي وفعال.
- تطوير الإطار التشريعي والتنظيمي: من الضروري مراجعة وتحديث القوانين واللوائح الوطنية باستمرار لتواكب التطور السريع في التهديدات السيبرانية، مع التركيز على حماية البيانات الشخصية وضمان حقوق المستخدمين.
- تعزيز الوعي الرقمي وبناء القدرات البشرية: يجب أن يكون هناك تركيز مكثف على تدريب الأفراد والموظفين على أفضل ممارسات الأمن السيبراني، وكيفية التعرف على الهجمات، وكيفية الإبلاغ عنها، لأن العنصر البشري يظل خط الدفاع الأول.
- تكثيف التعاون الدولي: لا بد من تعزيز التعاون الدولي وتبادل المعلومات بين الدول والمنظمات لمكافحة هذه التهديدات بفاعلية أكبر.

قائمة المراجع:

- Annie Badman (2023, 08 09). **ما هي محاكاة التصيد الاحتيالي؟** تاريخ الاسترداد 23 06 2025، من <https://www.ibm.com/sa-ar/think/topics/phishing-simulation>
- Barracuda. (2025). **Sensibilisation des utilisateurs à la sécurité.** Consulté le 05 13, 2025, sur [fr.barracuda.com](https://fr.barracuda.com/support/glossary/user-security-awareness): <https://fr.barracuda.com/support/glossary/user-security-awareness>
- daam. (2025). **قانون حماية البيانات الشخصية السعودية PDPL.** تاريخ الاسترداد 06 06 2025، من [daam.com](https://daam.com.sa/blog/security/البيانات-الشخصية-السعودية/): <https://daam.com.sa/blog/security/البيانات-الشخصية-السعودية/>
- EGOVKB. (2025). **E-Government Development Index (EGDI).** Retrieved 01 01, 2025, from <https://publicadministration.un.org/https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index>
- Escwa. (2025). **Network readiness index.** Retrieved 01 07, 2025, from [unescwa.org](https://www.unescwa.org/sd-glossary/network-readiness-index-issued-world-economic-forum): <https://www.unescwa.org/sd-glossary/network-readiness-index-issued-world-economic-forum>
- Freijat, S. (2023). **Digital economy. (its characteristics, advantages, applications).** Jordan, Business Faculty, Department of Business Economics.
- ibm. (2025). **تقرير تكلفة خرق البيانات لعام 2024.** تاريخ الاسترداد 05 06 2025، من [ibm.com](https://www.ibm.com): [ibm.com](https://www.ibm.com)

<https://www.ibm.com/sa-ar/reports/data-breach>

• IMD. (2024). **World Digital Competitiveness Ranking**. Retrieved 12 26, 2024, from imd.org: <https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/>

• liberoassurance. (2025). **شهادة اللانحة العامة لحماية البيانات**. تاريخ الاسترداد 12 06, 2025, من liberoassurance.org:

<https://liberoassurance.org/ar/شهادة/gdpr/>

• microsoft. (2025). **ما هي برامج الفدية الضارة؟** تاريخ الاسترداد 04 07, 2025, من [microsoft.com](https://www.microsoft.com/ar/security/business/security-101/what-is-ransomware):

<https://www.microsoft.com/ar/security/business/security-101/what-is-ransomware>

• Morgan, S. (2020, 11 13). **Cybercrime To Cost The World \$10.5 Trillion Annually By 2025**. Retrieved 07 02, 2025, from [cybersecurityventures.com](https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/): <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>

• pwc. (2024, 11 12). **تقرير صوت المستهلكين الملمين بالتكنولوجيا**. تاريخ الاسترداد 12 06, 2025, من [pwc.com](https://www.pwc.com/m1/en/publications/voice-of-the-consumer-2024-regional-findings-ar/voice-of-the-tech-savvy-consumer-ar.html):

<https://www.pwc.com/m1/en/publications/voice-of-the-consumer-2024-regional-findings-ar/voice-of-the-tech-savvy-consumer-ar.html>

• sdaia. (2025, 06 12). **حماية البيانات**. تم الاسترداد من [sdaia.gov](https://sdaia.gov.sa/ar/Research/Pages/DataProtection.aspx): <https://sdaia.gov.sa/ar/Research/Pages/DataProtection.aspx>

• United Nations. (2025). **Peace and Security**. Retrieved 06 26, 2025, from [un.org](https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty#:~:text=The%20newly%20adopted%20Cybercrime%20Convention,negotiated%20in%20over%2020%20years.): <https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty#:~:text=The%20newly%20adopted%20Cybercrime%20Convention,negotiated%20in%20over%2020%20years.>

• uniview. (2018, 05 23). **اللائحة العامة لحماية البيانات (GDPR)**. تاريخ الاسترداد 23 06, 2025, من [uniview.com](https://www.uniview.com/arab/News/News/201805/834829_284784_0.htm):

https://www.uniview.com/arab/News/News/201805/834829_284784_0.htm

• الاتحاد العربي للاقتصاد الرقمي. (2025). **المؤشر العربي للاقتصاد الرقمي**. تاريخ الاسترداد 07 01, 2025, من arab-digital-economy.org:

https://arab-digital-economy.org/?page_id=3954

• الجزيرة. (2017, 05 16). **كيف وقع هجوم "طلب الفدية" الإلكتروني؟** تاريخ الاسترداد 25 06, 2025, من [aljazeera.net](https://www.aljazeera.net/encyclopedia/2017/5/16-كيف-وقع-هجوم-طلب-الفدية-الإلكتروني):

<https://www.aljazeera.net/encyclopedia/2017/5/16-كيف-وقع-هجوم-طلب-الفدية-الإلكتروني>

- حسن مظفر الرزو. (2006). مقومات الاقتصاد الرقمي ومدخل الى اقتصاديات الانترنت. الرياض، المملكة العربية السعودية: مركز البحوث.
- محمد دحماني. (2023). الذكاء الاصطناعي كألية لتعزيز الامن السيبراني. مجلة الفكر القانوني والسياسي، 7(2)، 607.
- محمد مخلوف. (2025, 06 28). تسريب البيانات قنبلة تهدد الأفراد والدول.. كيف نواجهه؟ تاريخ الاسترداد 2025, 07 07 من: alarabiya.net: <https://www.alarabiya.net/science/2025/06/28/تسريب-البيانات-قنبلة-تهدد-الافراد-الدول-كيف-يمكن-مواجهتها->