توظيف الاعلام الجديد في نشر الوعي بالتعامل الآمن مع وسائل التواصل الاجتماعي

Employing new media in spreading awareness of safe dealing with social media

نرجس حسنعلي آل حماده

مستخلص الدراسة

تعد الثورة الإلكترونية والتعامل الآمن موضوعاً حاسماً في العصر الحديث. واشارت اغلب النتائج بالدراسات خلال عامى 2021-2022 إلى أنه هناك تزايد فى عدد المستخدمين عبر الإنترنت بشكل ملحوظ، حيث بلغ عدد المستخدمين النشطين على الإنترنت أكثر من 4.8 مليار مستخدم. وتشير هذه النتائج إلى أن الثورة الإلكترونية قد أحدثت تغييرات هائلة في طريقة التواصل والتعامل. كما ان هناك زيادة فى التعاملات المالية عبر الإنترنت، ويعد التحدي الأساسي هو ضمان الأمان والحماية للمستخدمين. فقد أدى انتشار الاحتيال والتهديدات السيبرانية إلى تزايد الحاجة إلى حلول أمنية قوية. فقد تم تسجيل خلال العام الحالى أكثر من 155 مليون هجوم سيبراني في جميع أنحاء العالم، مما يؤكد أهمية الحماية الإلكترونية. وبالتالي، يجب أن يركز الجهود على تطوير نظم تكنولوجيا المعلومات والاتصالات القوية والمبتكرة لضمان تجربة تعامل آمنة عبر الإنترنت. كما ينبغي تعزيز الوعي والتثقيف فيما يتعلق بالمخاطر السيبرانية وأفضل الممارسات للحماية الإلكترونية.

Abstract

The electronic revolution and secure transactions are crucial topics in the modern era. The majority of research studies conducted in 2021-2022 indicated a significant increase in the number of internet users, with over 4.8 billion active users online. These results highlight the enormous changes brought about by the electronic revolution in communication and interaction. Additionally, there has been a rise in online financial transactions, with the primary challenge being the assurance of security and protection for users. The prevalence of fraud and cyber threats has led to an increasing need for robust security solutions. During the current year, over 155 million cyber attacks have been recorded worldwide, emphasizing the importance of electronic protection. Therefore, efforts should focus on developing strong and innovative information and communication technology systems to ensure a secure online experience. Furthermore, awareness and education regarding cyber risks and best practices for electronic security should be enhanced

مقدمة

أصبح العصر الإلكتروني يؤثر بشكل كبير على المجال التعليمي. ظهرت العديد من منصات التعلم عبر الإنترنت والتعليم عن بُعد، مما أتاح للأفراد فرصة الحصول على التعليم والتدريب على مدار الحياة وفقًا لاحتياجاتهم وجداولهم الزمنية. وظهر تحول للوسائط الإعلامية: شهدت وسائل الإعلام تحولًا جذريًا في عصر المعلومات الإلكتروني. انتشرت وسائل الإعلام الرقمية مثل المواقع الإلكترونية، والمدونات، والبودكاست، وقنوات اليوتيوب، وتطبيقات الجوال، مما سمح للأفراد بالوصول إلى المعلومات والمحتوى على نطاق واسع وبشكل فوري. ومع تزايد كمية المعلومات المخزنة والمشاركة عبر الشبكات الإلكترونية، أصبحت حماية البيانات الشخصية والخصوصية أمرًا هامًا. تطوير قوانين وسياسات لحماية البيانات والتعامل بشكل آمن مع المعلومات الشخصية أصبح أمرًا ضروريًا للحفاظ على سلامة الأفراد والمؤسسات.

ورغم الفوائد العديدة التي يوفرها عصر المعلومات الإلكتروني، فإنه يواجه أيضًا تحديات جديدة. من بين هذه التحديات، التعامل مع كميات ضخمة من المعلومات (البيانات الضخمة) وتحويلها إلى معلومات قيّمة، والتهديدات الأمنية مثل الاختراقات الإلكترونية والاحتيال عبر الإنترنت.ولقد يشهد عصر المعلومات العصر الإلكتروني تسارعًا في التطور التكنولوجي والابتكار. تُطوّر التقنيات الجديدة بشكل مستمر مثل الذكاء الاصطناعي، والواقع

الافتراضي، والواقع المعزز، والتحليلات الضخمة، مما يؤدي إلى تغييرات سريعة في العديد من الصناعات والقطاعات.

مع التطور السريع للتكنولوجيا الرقمية، أصبحت قضايا الأمان الإلكتروني والخصوصية أموراً حيوية وملحة. إذ يزداد الاعتماد على الشبكات الإلكترونية والأنظمة المعلوماتية في جميع جوانب الحياة اليومية، فمن الضروري أن نتعامل بطرق آمنة وموثوقة في العالم الرقمي. حيث يعد عصر المعلومات وما يسمى بالعصر الإلكتروني هو عصر تحولت فيه المعلومات إلى عملة قوية، وتكنولوجيا المعلومات والاتصالات أصبحت أحد أهم أركان التنمية والتقدم في العديد من المجالات. الثورة الالكترونية :تشير مصطلح "الثورة الالكترونية" إلى التحول الجذري الذي شهدته العالم في العقود الأخيرة في مجال التكنولوجيا الرقمية وتكنولوجيا المعلومات. يتعلق الأمر بتقدم كبير في الحوسبة والاتصالات والإنترنت والبرمجيات والأجهزة الإلكترونية، مما أدى إلى تغيير جذري في كيفية تفاعل البشر مع العالم وبعضهم مع بعض. وتشمل هذه الثورة تطبيقات مثل وسائل التواصل الاجتماعي، والتجارة الإلكترونية، والحوسبة السحابية، والذكاء الاصطناعي، والواقع الافتراضي، والواقع المعزز، وغيرها من التقنيات والابتكارات الرقمية.

مشكلة الدراسة

فى ضوء خبرة الباحثة اوضحت مشكلة الدراسة فى الاسئلة البحثية التالية

- ما هي تأثيرات الثورة الالكترونية على جوانب الأمان الرقمي والتعامل الآمن؟
- كيف يمكن تحليل التحولات التكنولوجية في الثورة الالكترونية لتحديد التهديدات الأمنية الحالية والمستقبلية؟
- ما هي أفضل الممارسات والاستراتيجيات للتعامل الآمن مع التحديات الأمنية المتصاعدة في الثورة الالكترونية؟
- هل هناك تطورات تكنولوجية محددة يمكن استخدامها لتعزيز الأمان الرقمي والتعامل الآمن في الثورة الالكترونية؟
- ما هي التدابير القانونية والتنظيمية التي يمكن اتخاذها لمكافحة الجرائم الإلكترونية وتعزيز التعامل الآمن؟

أهداف الدراسة

- تحليل تأثير الثورة الالكترونية على جوانب الأمان الرقمي: الهدف هنا هو فهم كيفية تأثير التطور التكنولوجي والثورة الالكترونية على مستوى الأمان الرقمي في مختلف المجالات مثل الأعمال التجارية والحكومة والتعليم والرعاية الصحية وغيرها.
- تحديد التهديدات الأمنية في العصر الرقمي: الهدف هنا هو تحديد وتصنيف التهديدات الأمنية المتعلقة بالثورة الالكترونية، مثل الاختراقات السيبرانية، وسرقة الهوية، والاحتيال الإلكتروني، والتجسس، والاختراق الهجين، وغيرها.

وسيساعد ذلك في تحديد الاحتياجات والتحضير لاستراتيجيات التعامل الآمن.

- تقييم استراتيجيات التعامل الآمن مع التحديات الأمنية: الهدف هنا هو دراسة وتقييم الاستراتيجيات والممارسات الحالية للتعامل الآمن مع التحديات الأمنية المرتبطة بالثورة الالكترونية. يمكن تضمين ذلك في قطاعات مختلفة مثل الأعمال التجارية والحكومة والمؤسسات التعليمية والصحية.
- توصيات لتعزيز التعامل الآمن: الهدف هنا هو تقديم توصيات وإرشادات عملية لتعزيز التعامل الآمن في ظل الثورة الالكترونية، مثل تطوير سياسات الأمان الرقمي، وتعزيز التدريب والتثقيف الأمني، واعتماد التقنيات الأمنية المتقدمة، وتعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية

أهمية الدراسة "الاهمية النظرية– الاهمية التطبيقية"

الأهمية النظرية:

- فهم التحولات الرقمية: تساهم الدراسة في فهم وتحليل التحولات الرقمية والتطورات التكنولوجية التي يشهدها العالم في الوقت الحاضر. توفر الدراسة الأساس النظري لفهم طبيعة وتأثيرات الثورة الالكترونية على المجتمع والأفراد.
- توضيح التحديات الأمنية: تسلط الدراسة الضوء على التحديات الأمنية المتصاعدة في العصر الرقمي، مما يساعد

على توعية الباحثين والمجتمع بأهمية تطوير استراتيجيات التعامل الآمن مع هذه التحديات.

- إثراء النقاش الأكاديمي: تعزز الدراسة النقاش الأكاديمي حول مفهوم الثورة الالكترونية وأهميتها في التغيير الاجتماعي والاقتصادي. يمكن أن تكون مصدراً للبحوث الأخرى والمقارنات والدراسات المستقبلية حول هذا الموضوع.

الأهمية التطبيقية:

- تعزيز الأمان الرقمي: تساهم الدراسة في توفير إطار فهم شامل للتحديات الأمنية في العصر الرقمي وتوجيه جهود تعزيز الأمان الرقمي في المجتمعات والمؤسسات. يمكن أن تساعد في تطوير وتبني استراتيجيات وأدوات وسياسات فعالة لمكافحة الجرائم الإلكترونية وحماية البيانات والمعلومات الحساسة.
- تحسين الممارسات والسلوكيات: تساهم الدراسة في توعية الأفراد والمؤسسات بأفضل الممارسات والسلوكيات للتعامل الآمن في العصر الرقمي. يمكن أن توجه التعليم والتثقيف الأمني وتعزز وعي الناس بحماية خصوصيتهم وأمان معلوماتهم الشخصية.
- تعزيز التعاون الدولي: تعزز الدراسة التعاون الدولي في مجال مكافحة الجرائم الإلكترونية وتعزيز التعامل الآمن،

حيث توفر إطاراً مشتركًا للتفاهم والتعاون بين الدول في مجال تبادل المعلومات الأمنية وتعزيز القدرات الأمنية.

بشكل عام، تتجلى الأهمية النظرية في فهم وتحليل الثورة الالكترونية وتأثيرها، في حين تساهم الأهمية التطبيقية في تحسين الأمان الرقمي وتعزيز التعامل الآمن في المجتمعات والمؤسسات.

محددات الدراسة " المحددات الموضوعية– المحددات البشرية– المحددات المكانية– المحددات الزمانية – الأساليب الاحصائية"

- **المحددات الموضوعية:** تتعلق بطبيعة ومحتوى الدراسة حيث يتضمن هنا مجموعة من المفاهيم الرئيسية شملت :

الثورة الالكترونية: تشير إلى التحول الشامل الذي يشهده العالم بسبب تقدم التكنولوجيا الرقمية والاتصالات. يمكن أن تتضمن دراسة الثورة الالكترونية تحليلاً لتطور التكنولوجيا الرقمية وتأثيراتها على المجتمع والاقتصاد والحياة الشخصية.(2)

التعامل الآمن: يشير إلى السلوك والممارسات الضرورية للحفاظ على الأمان والحماية في البيئة الرقمية. يمكن أن تشمل الدراسة تحليلًا للتهديدات الأمنية المحتملة مثل الاختراقات الإلكترونية والاحتيال الإلكتروني وسرقة الهوية، وكذلك تحليل السياسات والتقنيات التي تستخدم للتعامل الآمن مع هذه التهديدات.(8)

العلاقة بين الثورة الالكترونية والتعامل الآمن: يجب تحديد العلاقة بين الثورة الالكترونية وأهمية التعامل الآمن في العصر الرقمي. يمكن أن

تتضمن الدراسة تحليلًا لكيفية تأثير التطورات التكنولوجية والتحولات الرقمية على التهديدات الأمنية وضرورة تطبيق إجراءات وسياسات التعامل الآمن.

- **المحددات البشرية:** ترتبط بالعوامل البشرية المشاركة في الدراسة. يتضمن ذلك تحديد المجموعة المستهدفة للدراسة، وتمثلت فى الدراسة الحالية بمجموعة من الخبراء في مجال الأمن الرقمي، المتخصصين في التكنولوجيا الحديثة، و المستخدمين العاديين للتكنولوجيا. وقامت الباحثة باختيار نسبة المستخدمين العاديين للتكنولوجيا في المجتمع السعودى بشكل عشوائى بمراعاة الخبرة والتخصص: حيث تم التطبيق على ذوى الخبرة في مجال الأمن الرقمي، التكنولوجيا الحديثة، أو الاستخدام العام للتكنولوجيا. حيث يمكن أن تؤثر خبرة وتخصص المشاركين على نتائج الدراسة وتطبيقاتها المحتملة.
- **المحددات المكانية:** ركزت الباحثة على النطاق الجغرافي حيث تم مراعاة التطبيق للادوات البحثية فى البيئة المحلية لتعادل السياق الثقافي والاجتماعي بالمملكة العربية السعودية .
- **المحددات الزمانية:** تم تطبيق الدراسة الحالية خلال العام 2023-2022
- **الأساليب الإحصائية:** قامت الباحثة بتحليل البيانات الكمية للاستبانة بحساب المتوسطات والانحرافات

مصطلحات الدراسة

الثورة الالكترونية: تشير إلى التحول الجذري والسريع في المجال التكنولوجي واستخدام التقنية الرقمية في مختلف جوانب الحياة، بما في ذلك الاقتصاد والثقافة والتواصل والتجارة والتعليم وغيرها.(7)

التعامل الآمن: يشير إلى اتخاذ الإجراءات والسياسات والتقنيات الضرورية لحماية المعلومات والبيانات الرقمية من التهديدات والاختراقات واستخدامها غير القانوني أو غير المشروع.(12)

الأمان الرقمي: يشير إلى الحماية الشاملة للمعلومات والبيانات الرقمية من التهديدات المختلفة، بما في ذلك الاختراقات الإلكترونية والاحتيال والفيروسات والاعتداءات السيبرانية وغيرها.(18)

جرائم المعلوماتية: تشير إلى الأنشطة غير القانونية التي تتعلق بالتكنولوجيا الرقمية، مثل الاختراقات الإلكترونية، وسرقة المعلومات، والاحتيال الإلكتروني، والتجسس السيبراني، والتشويش على الشبكات والأنظمة الرقمية، وغيرها.(21)

تكنولوجيا المعلومات والاتصالات (تكنولوجيا الاتصالات الرقمية): تشمل المصطلحات المتعلقة بالتكنولوجيا والأجهزة والبرمجيات المستخدمة في نقل وتخزين ومعالجة وإدارة المعلومات والبيانات عبر الشبكات الرقمية، مثل الإنترنت والهواتف المحمولة والحواسيب والخوادم وغيرها.(11)

فروض الدراسة

- الثورة الالكترونية تشهد تطورات سريعة ومتسارعة في مجالات مختلفة، مما يفرض ضرورة التعامل الآمن مع التكنولوجيا الرقمية.
- التهديدات الأمنية المتعلقة بالثورة الالكترونية تشكل تحديات كبيرة على المستوى الشخصي والمؤسسي، وتتطلب اتخاذ إجراءات وقائية فعالة.
- التوعية والتثقيف حول مفهوم التعامل الآمن مع التكنولوجيا الرقمية تلعب دوراً حاسماً في حماية الأفراد والمؤسسات من التهديدات السيبرانية.
- تبني السلطات والجهات المعنية بالتكنولوجيا الرقمية للوائح والسياسات الفعّالة يسهم في تعزيز التعامل الآمن مع التكنولوجيا الرقمية.

منهج الدراسة

قامت الباحثة بتطبيق المنهج الوصفى التحليلى لاجراء الدراسة حيث قامت بالاجراءات التالية :

- **مرحلة البحث:** تم إجراء مراجعة شاملة للأدبيات المتاحة حول الثورة الالكترونية والتعامل الآمن. استخدم المصادر الأكاديمية، والدوريات العلمية، والكتب المتخصصة، والتقارير الحكومية والمنظمات الدولية ذات الصلة. ثم تجميع المفاهيم الأساسية والتحديات والمخاطر المتعلقة بالثورة الالكترونية والتعامل الآمن.
- **مرحلة تحديد الأهداف والأسئلة البحثية:** المرتبطة بالثورة الالكترونية وأهميتها، وتحليل التحديات الأمنية، وتقديم توصيات لتعزيز التعامل الآمن. ثم صياغة الأسئلة البحثية التي توجه الدراسة وتساعد على الحصول على الإجابات المطلوبة.
- **جمع البيانات:** حيث تم استخدام مجموعة متنوعة من المصادر ، بما في ذلك المقابلات مع الخبراء والمتخصصين، واستبيانات للمستخدمين والمؤسسات، وتحليل البيانات الاحصائية المتعلقة بالتحديات الأمنية، والحالات الفعلية للاختراقات السيبرانية، وسلوك المستخدمين والتوجهات المتعلقة بالتكنولوجيا الرقمية.
- **تحليل البيانات واستخراج النتائج الرئيسية.**
- تقديم التوصيات لتعزيز التعامل الآمن مع التكنولوجيا الرقمية.

مجتمع وعينة الدراسة

- قامت الباحثة بتحديد المجموعة المستهدفة للدراسة، وتمثلت فى مجموعة من الخبراء في مجال الأمن الرقمي، المتخصصين في التكنولوجيا الحديثة، وكذلك مجموعة عشوائية من المستخدمين العاديين للتكنولوجيا. كنسبة فى المجتمع المحلى

أدوات الدراسة

قامت الباحثة بتطبيق استبانة حول "(تأثير الأساليب اليومية لاستخدام وسائل التواصل الاجتماعي)" بنظام ديكارت الخماسي وقد شمل المقياس الجوانب التالية :

- ✓ **فاعلية** :(Effectiveness) تقييم مدى فاعلية استخدام وسائل التواصل الاجتماعي في تحقيق الأهداف المرجوة. مثلاً، "باستخدام وسائل التواصل الاجتماعي، يمكنني تحقيق أهدافي بشكل فعال".
- ✓ **كفاءة** :(Efficiency) تقييم مدى كفاءة استخدام وسائل التواصل الاجتماعي من حيث الوقت والجهد المستهلكين. مثلاً، "استخدام وسائل التواصل الاجتماعي يساعدني على توفير الوقت والجهد".
- ✓ **سهولة الاستخدام** :(Ease of use) تقييم مدى سهولة استخدام وسائل التواصل الاجتماعي والتفاعل معها. مثلاً، "أجد وسائل التواصل الاجتماعي سهلة الاستخدام ويمكنني التفاعل معها بسهولة".
- ✓ **متعة الاستخدام** :(Enjoyment) تقييم مدى متعة استخدام وسائل التواصل الاجتماعي والحصول على رضا وإشباع شخصي منها. مثلاً،

"أستمتع بالتفاعل مع وسائل التواصل الاجتماعي وأشعر بالرضا عند استخدامها".

- ✓ **تأثير اجتماعي** :(Social influence) تقييم مدى تأثير وسائل التواصل الاجتماعي على العلاقات الاجتماعية والاتصالات الشخصية. مثلاً، "وسائل التواصل الاجتماعي له

ثبات وصدق المقياس

لحساب ثبات وصدق الاستبيان، قامت الباحثة بما يلى :

ثبات الاستبيان:(Reliability)

تم حساب معامل الاتساق الداخلي مثل معامل ألفا كرونباخ (Cronbach's alpha)، حيث يقيس العلاقة بين عناصر الاستبيان ويشير إلى مدى تجانس الأسئلة.

وقامت الباحثة باستخدام اختبار الاختبار–اختبار(test–retest) ، حيث تم اعادة إجراء الاستبيان على مجموعة من المشاركين بعد فترة زمنية وحساب الاتساق بين النتائج الأولية والنتائج المكررة.

صدق الاستبيان:(Validity)

قامت الباحثة باستخدام صدق المعيار الخارجيCriterion validity) من خلال تحليل علاقة نتائج الاستبيان مع المتغيرات الخارجية

الاطار النظرى للدراسة

مقدمة عن عصر المعلومات (العصر الالكتروني)

عصر المعلومات ما يسمى بالعصر الإلكتروني هو فترة زمنية تميزت بتطور التكنولوجيا واستخدام الحواسيب والشبكات الإلكترونية لتخزين ونقل المعلومات بشكل سريع وفعال. يعتبر هذا العصر مرحلة متقدمة من عصر الصناعة الثالثة ويشمل الفترة من الستينات وحتى الآن.

تمثلت الميزة الرئيسية لعصر المعلومات الإلكتروني في القدرة الكبيرة على جمع وتخزين المعلومات بشكل ضخم وتحويلها إلى صيغ رقمية يمكن معالجتها ونقلها عبر الشبكات الإلكترونية. يُعزز هذا العصر بواسطة تطور تقنيات الحوسبة والشبكات والإنترنت، والتي أنشأت منصة عالمية لتبادل المعرفة والمعلومات بين الأفراد والمؤسسات.(2)

وتأثرت جميع جوانب الحياة بسبب عصر المعلومات الإلكتروني. في المجال الاقتصادي، ساهم هذا العصر في تحول الاقتصاد من القائم على الصناعة إلى القائم على المعرفة، حيث أصبحت المعلومات والمعرفة همزة الوصل الأساسية بين الأفراد والشركات والحكومات.

من الناحية الاجتماعية، أصبحت الشبكات الاجتماعية ووسائل التواصل الاجتماعي تلعب دوراً مهماً في تبادل المعلومات والتواصل بين الناس حول العالم. وأصبحت الوصول إلى المعلومات والمحتوى متاحة بشكل واسع للجميع، مما سهّل عملية التعلم والتطوير الشخصي.

في المجال الحكومي، أصبحت الحكومات تعتمد بشكل كبير على تكنولوجيا المعلومات لتحسين خدماتها وتسهيل إجراءاتها الإدارية. وظهرت مفاهيم جديدة مثل الحكومة الإلكترونية والديمقراطية الإلكترونية.

علاوة على ذلك، تأثرت العديد من الصناعات بسبب عصر المعلومات الإلكتروني. ظهرت صناعات جديدة مثل تكنولوجيا المعلومات والاتصالات، والتجارة الإلكترونية، والتسويق الرقمي. كما تم تحسين العديد من العمليات والعمليات التجارية بفضل الحوسبة السحابية وتقنيات الذكاء الاصطناعي.(5)

باختصار، عصر المعلومات العصر الإلكتروني هو عصر تميز بتحول جذري في تخزين ونقل المعلومات بفضل التقدم التكنولوجي. يؤثر هذا العصر في جميع جوانب الحياة بما في ذلك الاقتصاد، والاجتماع، والحكومة، والصناعة، ويعزز التواصل وتبادل المعرفة بشكل كبير.

الثورة الرقمية وثورة المعرفة في العالم الرقمي

الثورة الرقمية وثورة المعرفة في العالم الرقمي تشيران إلى تطورات هائلة في مجال التكنولوجيا والمعلوماتية وكيفية استخدامها في جميع جوانب الحياة اليومية والأعمال التجارية والتفاعل الاجتماعي. يمكن تلخيص الثورة الرقمية وثورة المعرفة على النحو التالي:

الثورة الرقمية :تشمل الثورة الرقمية التقدم الهائل في التكنولوجيا الرقمية واستخدامها في الحياة اليومية والأعمال التجارية والحكومة. وتشمل هذه التطورات استخدام الحواسيب والهواتف الذكية والأجهزة اللوحية والإنترنت والشبكات الاجتماعية والتجارة الإلكترونية والحوسبة السحابية والواقع الافتراضي وغيرها من التقنيات الرقمية. وقد أحدثت هذه التكنولوجيات تغييراً جذرياً في كيفية التفاعل والتواصل والعمل والتعلم والترفيه.(8)

ثورة المعرفة في العالم الرقمي :مع زيادة الوصول إلى الإنترنت والمعلومات المتاحة على الشبكة، فإن ثورة المعرفة تشير إلى القدرة الهائلة للأفراد والمؤسسات على الوصول إلى المعرفة وتبادلها وتوليدها بشكل سريع وفعال. يتيح العالم الرقمي فرصاً هائلة للتعلم والتدريب والابتكار والتبادل الثقافي والعلمي، حيث يمكن للأفراد الوصول إلى المحتوى التعليمي والأبحاث والمعلومات المتخصصة من أي مكان في العالم وفي أي وقت.

تتعاون الثورة الرقمية وثورة المعرفة في خلق مجتمع يعتمد على التكنولوجيا والمعلوماتية، حيث يتم تعزيز التواصل والتعلم والابتكار والتنمية الشخصية والمؤسساتية. ومع ذلك، فإن هناك أيضاً تحديات ومسائل تتعلق بالأمان الرقمي والخصوصية والتوازن بين التكنولوجيا والإنسانية التي يجب معالجتها بعناية في هذا العصر الرقمي المتقدم.(10)

إيجابيات وسلبيات الثورة الالكترونية

الإيجابيات:

- **سهولة الوصول والتواصل:** أصبح بإمكان الأفراد التواصل والتفاعل مع بعضهم البعض بسهولة عبر الإنترنت ووسائل التواصل الاجتماعي. يمكن للأفراد من جميع أنحاء العالم التواصل وتبادل الأفكار والمعلومات والتجارب.
- **تسهيل الوصول إلى المعلومات:** يمكن للأفراد الحصول على المعلومات والبحوث والمصادر التعليمية بسهولة عبر الإنترنت، مما يعزز التعلم والتطور الشخصي.

- **التجارة الإلكترونية:** تمكن الثورة الالكترونية التجارة الإلكترونية والتسوق عبر الإنترنت، مما يتيح للأفراد والشركات الوصول إلى سلع وخدمات متنوعة وتسويق منتجاتهم بسهولة.
- **التطور التكنولوجي:** أدت الثورة الالكترونية إلى تقدم هائل في التكنولوجيا، مثل التطور في الحوسبة السحابية، والذكاء الاصطناعي، والواقع الافتراضي، والتكنولوجيا الحيوية، مما يفتح آفاقًا جديدة للابتكار والتطور في مختلف المجالات.(58)

السلبيات:

- **قضايا الأمان الرقمي:** تزايدت التهديدات الأمنية على الإنترنت، مثل الاختراقات الإلكترونية وسرقة البيانات الشخصية، مما يشكل تهديداً على خصوصية الأفراد والمؤسسات.
- **انعدام الخصوصية:** تتضمن الثورة الالكترونية جمع الكميات الهائلة من المعلومات الشخصية والبيانات، مما يثير قضايا الخصوصية واستخدام البيانات الشخصية بطرق غير مشروعة أو غير مرغوب فيها.
- **الاعتماد الزائد على التكنولوجيا:** قد يؤدي الاعتماد الكبير على التكنولوجيا إلى تقليل التفاعل الشخصي وتقليل المهارات الاجتماعية الحقيقية، وقد يؤثر على الصحة النفسية والعلاقات الإنسانية.

- **الفجوة الرقمية:** لا يمتلك الجميع نفس مستوى الوصول والفهم للتكنولوجيا، مما يؤدي إلى تفاقم الفجوة الرقمية بين الأفراد والمجتمعات، ويمكن أن يزيد من عدم المساواة في الفرص والمعرفة. (62)

نظام مكافحة جرائم المعلوماتية الالكترونية

نظام مكافحة جرائم المعلوماتية الالكترونية هو مجموعة من القوانين والسياسات والإجراءات التي تهدف إلى مكافحة الجرائم التي ترتكب باستخدام التكنولوجيا الرقمية والمعلوماتية. يهدف هذا النظام إلى حماية البيانات الشخصية والحفاظ على الأمان الرقمي ومكافحة أنشطة الاحتيال والاختراق والتلاعب بالمعلومات عبر الإنترنت.

يشمل نظام مكافحة جرائم المعلوماتية الالكترونية عدة جوانب وإجراءات، بما في ذلك:

- **قوانين وتشريعات:** وضع قوانين وتشريعات تنظم استخدام التكنولوجيا الرقمية وتعاقب على الجرائم المعلوماتية، مثل الاختراق الإلكتروني، وسرقة الهوية الرقمية، والاحتيال الإلكتروني.
- **إنشاء هيئات ووحدات تحقيق:** إنشاء هيئات ووحدات تحقيق مختصة في مكافحة جرائم المعلوماتية، تكون مجهزة بالمهارات والتقنيات اللازمة لجمع الأدلة الرقمية وتتبع المجرمين.

- **التعاون الدولي:** التعاون مع الجهات القضائية والأمنية في البلدان الأخرى لتبادل المعلومات والخبرات في مجال مكافحة جرائم المعلوماتية العابرة للحدود.
- **توعية الجمهور:** توعية الجمهور بمخاطر جرائم المعلوماتية وكيفية حماية أنفسهم، من خلال حملات توعوية وتثقيفية حول أمان الإنترنت وممارسات الأمان الرقمي.
- **تطوير التقنيات الأمنية:** تطوير تقنيات وأدوات أمنية متقدمة للكشف عن الاختراقات والتلاعب بالبيانات وحماية الأنظمة الرقمية من الهجمات.(67)

الجرائم الالكترونية مفهومها انواعها واهدافها واسبابها واساليب مكافحتها

الجرائم الإلكترونية هي أعمال غير قانونية تتم باستخدام التكنولوجيا الرقمية والمعلوماتية. يشمل ذلك الاختراق الإلكتروني، وسرقة الهوية الرقمية، والاحتيال الإلكتروني، والتلاعب بالمعلومات، والتجسس الإلكتروني، والتهديدات السيبرانية، والاعتداء على الخصوصية الرقمية، والتحريض على الكراهية عبر الإنترنت، والتجسس الصناعي، والتهديدات الإلكترونية الأخرى.

هناك عدة أهداف للجرائم الإلكترونية، بما في ذلك:

- **الربح المالي:** تشمل الجرائم الإلكترونية محاولة الحصول على المال بشكل غير قانوني، مثل الاحتيال الإلكتروني، وسرقة المعلومات المالية، والابتزاز المالي.

- **التخريب والتدمير:** قد يكون للجرائم الإلكترونية أهداف تخريبية، مثل الاختراق الهادف لتعطيل الأنظمة الحاسوبية أو تدمير البيانات.
- **التجسس الصناعي:** يمكن أن تستخدم الجرائم الإلكترونية لسرقة المعلومات التجارية والتكنولوجية من المنظمات لصالح المنافسين.
- **النشاط الإرهابي:** يستخدم بعض الأفراد والجماعات الإلكترونية وسائل التكنولوجيا الرقمية للتخطيط والتنفيذ لأعمال إرهابية.

هناك عدة أسباب لارتفاع حالات الجرائم الإلكترونية، بما في ذلك:

- **التطور التكنولوجي:** التقدم التكنولوجي السريع يوفر فرصاً جديدة لارتكاب الجرائم الإلكترونية ويسهل تنفيذها.
- **الربح المحتمل:** يعتبر الجانيون الإلكترونيون الحصول على المكاسب المالية من الجرائم الإلكترونية مغرياً.
- **الانتشار الواسع للإنترنت:** زيادة استخدام الإنترنت وتوفر الوصول السهل إلى التكنولوجيا الرقمية يزيد من فرص ارتكاب الجرائم الإلكترونية.

لمكافحة الجرائم الإلكترونية، تتبع الأساليب التالية:

- **قوانين وتشريعات قوية:** وضع قوانين صارمة لمكافحة الجرائم الإلكترونية وتعزيز العقوبات ضد المجرمين الإلكترونيين.
- **التعاون الدولي:** تعزيز التعاون وتبادل المعلومات بين الدول لمكافحة الجرائم الإلكترونية التي تعبر الحدود.
- **تعزيز الوعي والتثقيف:** توعية الجمهور بمخاطر الجرائم الإلكترونية وتعزيز الممارسات الأمنية الرقمية للحد من الاحتيال والاختراق.
- **التقنيات الأمنية:** استخدام التقنيات الأمنية المتقدمة لحماية البيانات والأنظمة الرقمية من الهجمات الإلكترونية.
- **تطوير الكوادر والخبرات:** تدريب الكوادر القانونية والتقنية على مكافحة الجرائم الإلكترونية وتطوير الخبرات في هذا المجال.

الفرق بين الجرائم المعلوماتية والجرائم الالكترونية

الجرائم المعلوماتية والجرائم الالكترونية عبارة عن مصطلحين يشيران إلى أنواع مختلفة من الجرائم التي تشمل استخدام التكنولوجيا والمعلومات. ومع ذلك، هناك بعض الاختلافات الدقيقة بينهما:

- **الجرائم المعلوماتية:(Cybercrimes)**

تشير إلى الجرائم التي ترتكب باستخدام التكنولوجيا المعلوماتية، سواء كانت تتعلق بالأجهزة المحمولة أو الشبكات الحاسوبية أو الأنظمة الإلكترونية.

قد تشمل جرائم مثل الاختراق الإلكتروني، وسرقة المعلومات، والتزوير الإلكتروني، والاحتيال الإلكتروني، والتجسس الإلكتروني، والتشويه الإلكتروني، والتهديد الإلكتروني، وغيرها.

- **الجرائم الالكترونية:(Electronic Crimes)**

تشير إلى الجرائم التي ترتكب باستخدام التكنولوجيا الإلكترونية، والتي تتعلق بالتحايل والاحتيال والتلاعب في المعاملات الإلكترونية.يمكن أن تشمل جرائم مثل الاحتيال الإلكتروني، والاستيلاء غير المشروع على الممتلكات الرقمية، والتلاعب في المعاملات المالية عبر الإنترنت، والتزوير الإلكتروني للمستندات.

بشكل عام، يمكن اعتبار الجرائم الالكترونية جزءاً من الجرائم المعلوماتية، حيث تندرج الجرائم الالكترونية تحت مظلة الجرائم المعلوماتية التي تتضمن أي نوع من أنواع الجرائم المرتبطة بالمعلومات واستخدام التكنولوجيا في ارتكابها.(73)

أركان الجريمة المعلوماتية في النظام السعودي

في النظام السعودي، لا يوجد تصنيف محدد لأركان الجريمة المعلوماتية، ولكن يمكن الاستناد إلى الأنظمة واللوائح المعمول بها لتحديد بعض العناصر الأساسية المشتركة التي يتم النظر فيها عند معالجة جرائم المعلوماتية. وفيما يلي بعض العناصر الأساسية التي قد تأخذ في الاعتبار في قضايا الجرائم المعلوماتية في النظام السعودي:

- **العمل الغير قانوني:** يشترط وجود عمل غير قانوني يتعلق بالمعلومات أو التكنولوجيا الحاسوبية، مثل الاختراق الإلكتروني أو التلاعب بالبيانات.
- **النية السيئة:** يشترط وجود نية سيئة أو غير قانونية في ارتكاب الجريمة المعلوماتية، مثل القصد في سرقة المعلومات أو التسبب في الضرر.
- **التأثير الضار:** يجب أن يكون هناك تأثير ضار ناتج عن الجريمة المعلوماتية، سواء كان ذلك في إتلاف المعلومات أو الإضرار بالأشخاص أو الكيانات.
- **العلاقة بالتكنولوجيا:** يشترط وجود عنصر التكنولوجيا الحاسوبية أو استخدام وسائل الاتصال الإلكترونية في ارتكاب الجريمة.
- **التوثيق والإثبات:** يجب توثيق وإثبات وقوع الجريمة المعلوماتية من خلال الأدلة والشواهد المناسبة.

السياسة الاجتماعية ومكافحة الجرائم الالكترونية في المجتمع السعودي في رؤية 2030

في رؤية المملكة العربية السعودية 2030، تُعتبر مكافحة الجرائم الإلكترونية وتعزيز السياسة الاجتماعية ذات أهمية كبيرة. تهدف الرؤية إلى بناء مجتمع متقدم رقمياً ومتصل، وتعزيز الأمن الإلكتروني والحماية من الجرائم الإلكترونية. في هذا السياق، تتمثل السياسة الاجتماعية ومكافحة الجرائم الالكترونية في المجتمع السعودي في عدة جوانب:

- **التوعية والتثقيف:** تعزيز الوعي والتثقيف بشأن أهمية الأمن الإلكتروني ومخاطر الجرائم الإلكترونية، وذلك من خلال حملات توعية وبرامج تثقيفية للمجتمع.
- **التشريعات والتنظيمات:** وضع تشريعات وقوانين فعالة تنظم استخدام التكنولوجيا والمعلومات الإلكترونية، وتحدد الجرائم الإلكترونية وتعاقب عليها.
- **التعاون الدولي:** تعزيز التعاون والتنسيق الدولي في مجال مكافحة الجرائم الإلكترونية، من خلال التبادل الإلكتروني للمعلومات والتجارب والخبرات.
- **التحقيق والملاحقة:** تعزيز قدرات الأجهزة الأمنية والقضائية في التحقيق وملاحقة المتورطين في الجرائم الإلكترونية، وتوفير التدريب والتحديث المستمر للكوادر العاملة في هذا المجال.

- **الحماية والأمان الإلكتروني:** تطوير البنية التحتية الرقمية وتعزيز الحماية الإلكترونية للأفراد والمؤسسات، بما في ذلك توفير الأدوات والتقنيات الضرورية للوقاية من الهجمات الإلكترونية.

دور المملكة في التصدي للجرائم الالكترونية " المنصة الوطنية الموحدة"

المملكة العربية السعودية تعتبر التصدي للجرائم الإلكترونية من أولوياتها، ولذلك قامت بإنشاء المنصة الوطنية الموحدة لمكافحة الجرائم الإلكترونية. تلعب هذه المنصة دوراً حيوياً في تعزيز الأمن الإلكتروني ومكافحة الجرائم الإلكترونية في المملكة، وذلك من خلال العديد من الأدوات والمبادرات التي توفرها، ومنها:

- **التبادل المشترك للمعلومات:** تقوم المنصة بتسهيل التبادل المشترك للمعلومات والبيانات المتعلقة بالجرائم الإلكترونية بين الجهات المختلفة في المملكة، مثل الجهات الأمنية والقضائية والحكومية.
- **التنسيق والتعاون:** تعزز المنصة التنسيق والتعاون بين الجهات المعنية في مكافحة الجرائم الإلكترونية، وتسهل تبادل الخبرات والمعرفة والتجارب المتعلقة بهذا المجال.
- **الإبلاغ والبلاغ:** توفر المنصة آليات وسبل للإبلاغ والبلاغ عن الجرائم الإلكترونية، سواء كان ذلك من خلال البلاغات الإلكترونية أو الهاتفية أو غيرها من وسائل الاتصال المتاحة.

- **التحقيق والتحليل:** تدعم المنصة الجهات المعنية في التحقيق والتحليل الجنائي للجرائم الإلكترونية، وتوفر الأدوات والتقنيات الضرورية لجمع الأدلة الرقمية وتحليلها.
- **التوعية والتثقيف:** تقدم المنصة برامج توعوية وتثقيفية للمجتمع بشأن أهمية الأمن الإلكتروني وكيفية الوقاية من الجرائم الإلكترونية، وذلك من خلال ورش العمل

نسبة الجرائم الالكترونية في المملكة العربية السعودية

بلغ عدد الجرائم الإلكترونية في المملكة خلال أعوام 1435 و 1436 و 1437 نحو 1513 جريمةً، في حين تصدرت المنطقة الشرقية القضايا بنحو 463، تلتها مكة المكرمة بـــ350 ثم المدينة المنورة بـــ153 قضية، وذلك وفقا لدراسة بحثية صادرة عن جامعة نايف العربية للعلوم الأمنية أجراها الباحث يزيد الصيقل لنيل درجة الدكتوراه.

تمثلت عوامل ارتكاب الجرائم الإلكترونية، على مستوى الفرد والمجتمع والعولمة، فى ضوء عناصر التعرف على أسباب وأساليب ارتكاب الجرائم الإلكترونية المتعلقة باختراق الحسابات أو الابتزاز أو التخريب، للحد من تفاقمها، والعمل على رصد طبيعة وأساليب مرتكبي الجرائم الإلكترونية المتعلقة بالإرهاب من خلال الخبرات الفنية والوطنية المختصة باعتبارها من أخطر أنواع الجرائم الإلكترونية على الفرد والمجتمع. ومن هذه العوامل توفر الفرصة

لارتكاب الجريمة، والزهو وحب الظهور، والتقدير الذاتي، والحياة الروتينية الرتيبة، والنسيج الحضري ونموه على حساب البادية والقرى والهجر، وضغوطات الحياة والمجتمع على أفراده من خلال عدم توفر فرص النجاح الحقيقية، وقلة مواكبة رقابة القوانين وإنفاذها في مجال الجرائم الإلكترونية، وتحول كثير من دول العالم إلى بيئة الحكومة الإلكترونية، وتزايد معدلات التسوق عبر المواقع الإلكترونية، وزيادة استخدام الأجهزة الرقمية التي غيرت العالم، وكثرة التعاطي مع مفاهيم العولمة والتعارف عبر الإنترنت.

حول طبيعة الجرائم الإلكترونية الشائعة في المملكة، بين الصيقل، أن الإحصاءات الرسمية لعام 1437 بينت أن طبيعة الجرائم الإلكترونية التي تمت مقاضاة مرتكبيها قد تنوعت بين سرقة معلومات، وبيانات، وتحرش، وتزوير، ومحاولات تسلل، وبين سطو على الحساب المصرفي للأفراد، إضافة إلى استهداف مواقع شخصية وحكومية بهدف التخريب، وتغيير معالمها، واتضح أن طبيعة هذه الجرائم قد ازدادت بين عامي 1435 و1437 بمعدل 400% حيث تضاعف الرقم من 164 جريمة إلى 776 جريمة إلكترونية.

بالنسبة لعدد ضبطيات الجرائم التقنية التي وردت لأقسام الشرطة بالمحافظات الإدارية لعام 1432 بلغت 246 قضية، كما بلغت في إحصائية عام 1433 نحو 294 قضية، وفي عام 1434 بلغت 303 قضايا، وفي عام 1435 بلغ مجموع الضبطيات 216 قضية، إلا أنه

في 1436 ازدادت الضبطيات لتصل إلى 341 قضية، وقد تنوعت نوعية الجرائم التقنية في أنواعها وأدواتها فبعض الجرائم تتعلق باختراق الحسابات وجرائم أخرى تتعلق بالابتزاز الجنسي عبر برامج التواصل الاجتماعي، ويتضح من الإحصاءات السابقة أن هناك تزايدا في معدلات الجرائم الإلكترونية في السعودية.

أبرز الجرائم التي تقع باستخدام النظام المعلوماتي

- جرائم متعلقة بالبيانات المتصلة بالحياة الخاصة
- جرائم متعلقة بالتجارة الإلكترونية
- المخدرات عبر الإنترنت
- غسيل الأموال
- الإرهاب عبر الإنترنت
- الجرائم الإلكترونية التي تستهدف الجهات الرسمية وغير الرسمية

الجرائم الإلكترونية خلال أعوام 1435 – 1436 – 1437

- ✓ المنطقة الشرقية: 463
- ✓ مكة المكرمة: 350
- ✓ المدينة المنورة: 153
- ✓ الرياض: 152
- ✓ عسير: 131
- ✓ القصيم: 70

- ✓ حائل: 50
- ✓ جازان: 45
- ✓ تبوك: 24
- ✓ الجوف: 21
- ✓ الحدود الشمالية: 20
- ✓ الباحة: 19
- ✓ نجران: 15

اللائحة التنفيذية لنظام الجرائم الالكترونية

نظام الجرائم الإلكترونية في المملكة العربية السعودية يتم تنظيمه وتنفيذه من خلال العديد من اللوائح والأنظمة. واحدة من هذه اللوائح هي اللائحة التنفيذية لنظام الجرائم الإلكترونية، والتي تحدد الإجراءات والضوابط المتعلقة بتطبيق النظام وتنفيذه. ومن بين الجوانب التي تغطيها اللائحة التنفيذية:

تحديد أنواع الجرائم الإلكترونية: تحدد اللائحة التنفيذية أنواع الأفعال التي تعتبر جرائم إلكترونية، مثل الاحتيال الإلكتروني، والاختراق السيبراني، وانتحال الهوية الرقمية، ونشر المعلومات الكاذبة عبر الشبكة العنكبوتية، وغيرها.

التحقيق والمحاكمة: تنص اللائحة التنفيذية على الإجراءات المتعلقة بالتحقيق في جرائم الإنترنت وجمع الأدلة الرقمية، وتوضح

الإجراءات القانونية المطبقة على المشتبه بهم والمتهمين بارتكاب جرائم إلكترونية، بما في ذلك إجراءات المحاكمة وتطبيق العقوبات.

الجهات المختصة: تحدد اللائحة التنفيذية الجهات المسؤولة عن تنفيذ النظام ومكافحة الجرائم الإلكترونية في المملكة، مثل الهيئة الوطنية لمكافحة الجرائم الإلكترونية والجهات الأمنية المعنية.

العقوبات: تنص اللائحة التنفيذية على العقوبات المقررة

المسؤولية الاجتماعية للحد من الجرائم المعلوماتية

تعني المسؤولية التي يتحملها المجتمع والأفراد في الوقاية من ومكافحة الجرائم المعلوماتية والحماية منها. من خلال ما يلى :

التوعية والتعليم: ينبغي أن يتم توعية الأفراد والمجتمع بأنواع الجرائم المعلوماتية وأساليبها، وتعريفهم بالمخاطر والتدابير الوقائية. يمكن ذلك من خلال حملات توعية ومبادرات تثقيفية للأفراد والمؤسسات.

تعزيز الأمن الرقمي: يتطلب الأمر من المجتمع تبني إجراءات وسلوكيات آمنة في استخدام التكنولوجيا والمعلومات، مثل استخدام كلمات مرور قوية وتحديث البرامج والأنظمة الأمنية بشكل منتظم.

التبليغ عن الجرائم: يجب على الأفراد والمؤسسات الإبلاغ عن أي جرائم معلوماتية يشتبه في وقوعها، سواءً بالتوجه إلى الجهات الأمنية المختصة أو الهيئات المعنية بمكافحة الجرائم المعلوماتية.

التعاون والشراكة: يتعين على المجتمع والقطاعين العام والخاص التعاون في مجال مكافحة الجرائم المعلوماتية، وتبادل المعلومات والخبرات والتجارب لتعزيز القدرة على التصدي لهذه الجرائم.

القوانين والتشريعات: يجب أن يتم وضع وتنفيذ قوانين وتشريعات فعالة لمكافحة الجرائم المعلوماتية ومعاقبة المرتكبين. ينبغي أن تكون هذه القوانين متجددة وملائمة للتطورات التكنولوجية المستمرة.(23-24)

العوامل الاجتماعية المؤدية لارتكاب الجرائم الالكترونية

هناك عدة عوامل اجتماعية يمكن أن تسهم في ارتكاب الجرائم الإلكترونية. ومن بين هذه العوامل:

- **التكنولوجيا والوصول إلى الإنترنت:** توفر التكنولوجيا الحديثة والوصول السهل إلى الإنترنت فرصاً وأدوات للأفراد لارتكاب الجرائم الإلكترونية. يمكن للأشخاص الذين لديهم مهارات تقنية ووصول إلى الإنترنت الارتكاب بسهولة لأنهم يمتلكون المعرفة والأدوات اللازمة.
- **الفقر والظروف الاقتصادية الصعبة:** قد يجد بعض الأفراد في الظروف الاقتصادية الصعبة في الحاجة الماسة إلى المال، وبالتالي يلجؤون إلى الجرائم الإلكترونية كوسيلة للحصول على المال بطرق غير قانونية.

- **الانعزال الاجتماعي وعدم وجود فرص:** في بعض الحالات، يمكن أن يلجأ الأفراد الذين يشعرون بالانعزال الاجتماعي أو الذين يواجهون صعوبات في الحصول على فرص اجتماعية واقتصادية إلى الجرائم الإلكترونية كوسيلة للتعبير عن أنفسهم أو لتحقيق رغباتهم.
- **الضغوط الاجتماعية والثقافية:** قد يكون هناك ضغوط اجتماعية وثقافية على الأفراد لتحقيق النجاح والثراء بأي طريقة ممكنة. في بعض الثقافات، قد يعتبر النجاح المادي السريع والحصول على المال بأي وسيلة ضرورة للتمتع بالاحترام والتقدير الاجتماعي.
- **القلة في وعي الأفراد بالقوانين الرقمية:** قد ينتج عن قلة وعي الأفراد بالقوانين والتدابير الأمنية المتعلقة بالعالم الرقمي ارتكاب الجرائم الإلكترونية بشكل غير مدرك. بعض الأفراد قد يجربون سلوكًا غير قانونيًا دون أن يدركوا تمامًا العواقب القانونية لتلك الأفعال.

يجب الأخذ في الاعتبار أنه لا يمكن تحميل العوامل الاجتماعية فقط مسؤولية ارتكاب الجرائم الإلكترونية، فالقرار النهائي لارتكاب الجريمة يعتمد على خيارات الفرد وقراراته الشخصية. ومع ذلك، فهذه العوامل الاجتماعية قد تلعب دوراً في تشجيع بعض الأفراد على الانخراط في الجرائم الإلكترونية.(22)

المشكلات العملية والقانونية للجرائم الالكترونية

الجرائم الإلكترونية تثير العديد من المشكلات العملية والقانونية، ومن بين هذه المشكلات:

- **التحقيق وجمع الأدلة:** يمكن أن تكون التحقيقات في الجرائم الإلكترونية تحدياً صعباً. فعندما يتم ارتكاب جريمة إلكترونية، فإن الأدلة عادةً ما تكون رقمية وتختفي بسهولة. قد يكون من الصعب تحديد هوية الجاني وتتبعه وتوثيق أدلة قوية لتقديمها للمحاكم.
- **القضايا الحدودية والدولية:** يعد التعاون القانوني والتحقيق في الجرائم الإلكترونية قضية دولية، حيث يمكن للجرائم الإلكترونية أن تتم عبر الحدود الوطنية. يجب التعاون بين الدول في مجال تبادل المعلومات والأدلة وتقديم المساعدة القانونية المتبادلة لمكافحة هذه الجرائم بشكل فعال.
- **التشريعات والقوانين المتطورة:** تحديث التشريعات والقوانين لمواجهة التهديدات الجديدة المتعلقة بالجرائم الإلكترونية يمثل تحدياً. يجب أن تكون القوانين قادرة على التعامل مع تقنيات جديدة وأنماط جرائم جديدة بشكل فعال، مما يتطلب مرونة وسرعة في التعديلات القانونية.
- **حماية البيانات والخصوصية:** تتعلق الجرائم الإلكترونية في كثير من الأحيان بانتهاك الخصوصية وسرقة البيانات

الشخصية. يجب أن تكون هناك تشريعات وإجراءات فعالة لحماية البيانات والخصوصية وتعزيز الأمان الإلكتروني.

- **التهديدات الجماعية والتنظيمات الإجرامية:** بعض الجرائم الإلكترونية ترتبط بتنظيمات إجرامية متنظمة وشبكات جرائم دولية. قد تمثل هذه التنظيمات تهديداً كبيراً للأمن السيبراني والاقتصاد الرقمي، وتتطلب جهوداً تعاونية بين الدول والوكالات الأمنية لمواجهة هذه التهديدات.(84)

المبادرات التقنية لحماية النشء من الجرائم الالكترونية

هناك العديد من المبادرات التقنية التي تهدف إلى حماية النشء من الجرائم الإلكترونية. ومن بين هذه المبادرات:

- **برامج التوعية والتثقيف الرقمي:** تتضمن هذه المبادرات تطوير برامج وحملات توعوية تهدف إلى تعليم النشء حول المخاطر الإلكترونية وأساليب الوقاية منها. تتضمن هذه البرامج توفير المعلومات حول الخصوصية والأمان عبر الإنترنت، ومفاهيم مثل الاحتيال الإلكتروني والتنمر عبر الإنترنت.
- **برامج التحكم الأبوي في الإنترنت:** توفر هذه البرامج أدوات للآباء والأوصياء لمراقبة وتحكم نشاطات النشء عبر الإنترنت. يمكن لهذه البرامج تتبع أنشطة الأطفال عبر الشبكة ومنعهم من الوصول إلى محتوى غير مناسب أو خطير.

- **أدوات تصفية وتصنيف المحتوى:** تقدم بعض الأدوات والتطبيقات خيارات لتصفية وتصنيف المحتوى على الإنترنت، مما يساعد النشء على تجنب الوصول إلى محتوى غير مناسب أو ضار. تتضمن هذه الأدوات تصنيف الروابط والمواقع والتطبيقات حسب العمر والمحتوى.
- **أمن البيانات والتشفير:** يُعتبر توفير أمن البيانات والتشفير من الأساسيات لحماية النشء من الجرائم الإلكترونية. تشمل هذه المبادرات استخدام تقنيات التشفير لحماية البيانات الشخصية والمعلومات الحساسة.
- **تطوير تقنيات الكشف عن التهديدات:** يعمل الخبراء في مجال أمن المعلومات والشركات التقنية على تطوير تقنيات الكشف عن التهديدات الإلكترونية والهجمات السيبرانية. تتضمن هذه التقنيات استخدام الذكاء الاصطناعي وتحليل السلوك للكشف المبكر عن الأنشطة الخبيثة والتهديدات المحتملة.(58)

الدراسات السابقة العربية والاجنبية

قامت الباحثة بالاطلاع على الدراسات السابقة والبحوث المتعلقة بمحاور البحث النظرية وحللتها وفيما يلى استعراض للادبيات:

دراسة (المطرف، 2020) هدفت هذه الدراسة إلى استقصاء مدى إمكانية التحول الرقمي في الجامعات الحكومية والخاصة في

المملكة العربية السعودية، بالإضافة إلى رصد واقع التحول الرقمي بينهما في ظل الأزمات العالمية والكوارث. وقد توصلت الدراسة إلى وجود فروق ذات دلاله إحصائية بين الجامعات الحكومية والجامعات الخاصة في مدى توافر العناصر المادية اللازمة للتحول الرقمي لصالح الجامعات الحكومية، وجود فروق ذات دلالة إحصائية بين الجامعات الحكومية والجامعات الخاصة في مدى توافر الكفاءات الرقمية لدى أعضاء هيئة التدريس لصالح العاملين في القطاع الخاص، وجود فروق ذات دلالة إحصائية بين الجامعات الحكومية والجامعات الخاصة في إمكانية التحول الرقمي للتعليم في ظل الأزمات لصالح الجامعات الخاصة، ويتضح من ذلك أنه يوجد تأثير معنوى لاختلاف قطاع التعليم الجامعي على مدى إمكانية التحول الرقمي للتعليم في ظل الأزمات الحالية.

دراسة (البلوشية وآخرون، 2020) تناقش الدراسة واقع التحول الرقمي في دولة عمان، من خلال معرفة حجم التحول الرقمي داخل المؤسسات العامة وتقييمه، واعتمدت الدراسة على المنهج الوصفي والمقابلات لمعرفة البيانات وتوصلت الدراسة إلى الجهد الكبير الذي تبذله تلك المؤسسات في نشر ثقافة التحول بين المستفيدين لزيادة الاستخدام.

دراسة (دربالة، 2020) هدفت الدراسة إلى تقديم نموذج موحد كامل لعملية التحول الرقمي بهدف دعم الجهود الحكومية المصرية في

التحول الرقمي، وبناء معيار موحد مشترك بين جميع الهيئات والجمعيات الحكومية المسئولة عن التحول الرقمي، وبالتالي توحيد المفاهيم المشتركة والمستخدمة في عملية التحول الرقمي، وتوحيد منهج دراسة وتخطيط وتنفيذ هذه المبادرات لضمان تحقيقها للأهداف الموضوعة من أجلها.

دراسة (محمد ،2019) تقيس الدراسة دور التقنيات الرقمية في تنشيط قطاع السياحة، واتبعت الدراسة المنهج الوصفي التحليلى للتوصل إلى أن التقنيات الرقمية لها دور فعال في دولة الجزائر لتقدم قطاع السياحة.

دراسة (أمين، 2018) تجيب الدراسة عن تساؤل كيفية إسهام التحول الرقمي في الجماعات لتحقيق مجتمع المعرفة؟ واستخدمت الدراسة المنهج الوصفي لدراسة المشكلة ووصفها وصفاً دقيقاً، وصاغت في نهايتها تصوراً مقترحاً حول عملية التحول الرقمي من خلال استراتيجية لنشر ثقافة التحول الرقمي، وكيفية تمويله، بالإضافة إلى تصميم برامج تعليمية للمستفيدين حول كيفة الاستفادة من التحول الرقمي.

دراسة (Lathinen, M. and Weaver, B., 2015) عرضت الدراسة تحديات عملية التحول الرقمي للتعليم الجامعي، وقد أشارت الدراسة إلى وجود ثلاثة طرق موازية لتصميم محتوى التعليم الجامعي لمواجهة تحدي التحول الرقمي سيستفيد منها مصممو البرامج ـــــ

وأعضاء هيئة التدريس ـــــــ وهي الأنشطة التعليمية غير الرقمية التي تعمل على محو الأمية الرقمية وتوفير الفرص الرقمية التي تعزز الممارسات في الفصول الدراسية التقليدية، والتحول الرقمي للجامعة يسير إلى فرصة نقل التعليم الجامعي نحو الوسائل الرقمية بشكل كامل.

دراسة (درة، 2018) تُقيم الدراسة مستوى أداءالخدمات في المنظمات الصحية، وذلك من خلال المقارنة بين الخدمات المقدمة في المستشفيات الخاصة والحكومية، واستخدم البحث المنهج الوصفي التحليلى لإظهار نتائج توضح عدم وجود اختلافات معنوية في مستوى إدراك أداء الخدمات للمنظمات الصحية بدولة عمان، وأوصت الدراسة بوجوب العمل على تحسين مستوى أداء الخدمات المقدمة من قطاع الصحة .

دراسة (بوفاس، 2018) تهدف الدراسة إلى تسليط الضوء على نموذج الفجوات الخمس باعتباره سلسلة من المقاييس المتكاملة والمترابطة لمعرفة رأس المستهلك بما يتوقعه من أداء في الخدمة المقدمة له من منتجها وفقاَ لعدد من الخصائص، وتوصلت الدراسة إلى أن قياس مدى توافر أبعاد مستوي أداء الخدمات الصحية من وجهات نظر مختلف المتعاملين يسمح بالإجابة عن التساؤلات المتعلقة بمدى توافر المستويات المطلوبة لجودة الخدمات الصحية في مؤسسات الصحة الجزائرية.

دراسة (أسو، بطرس 2018) تهدف الدراسة إلى التعرف على مستوى أداء جودة الخدمات المصرفية التي تقدمها المصارف في مدينة دهوك من وجه نظر العملاء، تكونت عينة الدراسة من 300 من العملاء المتعاملين مع بنك الرشيد والرافدين تم اختيارها بشكل عشوائي وتوصلت إلى مجموعة من النتائج بالتقييم الإيجابي لمستوي أداء الخدمة المصرفية الفعلية والمتوقعه، فضلاً عن وجود تباين في الأهمية النسبية التي يوليها العملاء عند تقييمهم لمستوى جودة الخدمات المصرفية، وخلصت الدراسة إلى ضرورة قيام الإدارة المصرفية بإعداد برامج عملية لتطوير خبرات ومهارات الموظفين من أجل تقديم أفضل الخدمات إلى العملاء.

دراسة (آمنة، 2018) تهدف الدراسة إلى إبراز مدى حاجة المؤسسات الصحية لتبني مدخل الجودة في خدماتها وتبيان القيمة المضافة من ذلك، بالإضافة إلى الوقوف على مستوى الرضا المتحقق لدى عينة من مرضى المستشفيات مع البرهنة على أن لجودة الخدمات الصحية أهمية كبيرة لتحقيق رضا المرضى، وتتناول الدراسة تحديد أثر جودة الخدمات الصحية على رضا المريض في المؤسسة محل الدراسة، وتقترح الدراسة في نهايتها إلى ضرورة رفع مستوى أداء العاملين من خلال تكثيف الدورات التكوينية، مع إقامة برامج تدريبية تركز على تنمية مهاراتهم السلوكية في التعامل مع المريض.

دراسة (أحمد، 2016) تناولت الدراسة مستوى أداء الخدمات وأثرها على رضا العملاء، وقد تمثلت مشكلة الدراسة في الإجابة عن التساؤل التالي: ما هو تأثير جودة الخدمات على رضا العملاء؟ وقد هدفت الدراسة بشكل رئيسي إلى التعرف على مستوي أداء الخدمات بالمؤسسات الخدمية في تحقيق رضا المستفيدين، وتوصلت الدراسة إلى نتائج من أهمها أن جودة الخدمات تؤثر إيجابياً على رضا العملاء كما توجد علاقة إيجابية بين أبعاد جودة الخدمات (الاستجابة، الملموسية، الضمان)، وقد خلصت الدراسة إلى مجموعة من التوصيات أهمها أن تقدم المؤسسة خدمات أكثر دقة ووضوحاً مع التطوير المستمر للخدمة وعمل برامج تدريبية للموظفين.

دراسة (Jun, 2010) تهدف الدراسة إلى اختبار العلاقة بين مستوي أداء الخدمة بأبعادها وبين رضا العمل الداخلي، وتوصلت الدراسة إلى مجموعة من النتائج من أهمها أن رضا العميل الداخلي دافع لإرضاء العميل الخارجي، وأن عامل التعاطف هو العامل الأكثر تأثيراً في تحقيق مستوي أداء الخدمات الداخلية وفي رضا العميل الداخلي، بالإضافة إلى التعامل الودي والتحسين المستمر لعمل الفريق.

دراسة (Bello, 2008) هدفت الدراسة إلى التعرف على أثر مستوى أداء الخدمات الداخلية على سلوك مقدمي الخدمة للعملاء، وقد أجريت على العاملين من موظفي الصف الأول في البنوك داخل اليونان، وتوصلت الدراسة إلى أن العاملين في تلك البنوك يفضلون

تحسين كفاءتهم وسلوكهم العام بشكل أكبر من أجل تحقيق مزيد من تحسين مستوي الخدمات الداخلية، وأنه عند زيادة مستوى أداء الخدمات الداخلية فإن العاملين يحسنون من أدائهم العام مما يساعد المنظمة على تحقيق الجودة الخارجية للخدمات، وتحقيق رضا العميل الخارجي.

فى ضوء ما سبق يركز التعقيب على الدراسات السابقة على ما يلى :

- **تحول العالم الرقمي:** تؤكد الدراسات على أن الثورة الإلكترونية أدت إلى تحول جذري في طريقة تفكيرنا وتصرفنا في التعامل مع التكنولوجيا والمعلومات. تمتد هذه التحولات إلى مجموعة متنوعة من المجالات بما في ذلك التجارة الإلكترونية والتواصل الاجتماعي والخدمات الحكومية الرقمية.
- **التحديات الأمنية:** تشير الدراسات إلى أن الثورة الإلكترونية أحدثت تحديات أمنية كبيرة. تزايدت جرائم القرصنة الإلكترونية وسرقة الهوية والاختراقات السيبرانية. توضح الدراسات أيضاً ضرورة التعامل مع هذه التحديات واتخاذ تدابير أمنية فعالة للحفاظ على البيانات والمعلومات الحساسة.
- **أهمية التوعية والتثقيف:** يُؤكد الباحثون أن التوعية والتثقيف السليم بشأن أمان البيانات والتصرف الآمن على الإنترنت

يلعبان دوراً حاسماً في التصدي للجرائم الإلكترونية. يوصون بتعزيز الوعي وتعليم المجتمع بأفضل الممارسات وسلوكيات الأمان الرقمي.

- **التعاون الدولي والقوانين:** تشدد الدراسات على أهمية التعاون الدولي وتبادل المعلومات والخبرات في مجال مكافحة الجرائم الإلكترونية. يُشدد أيضًا على أهمية وضع قوانين تتعلق بذلك
- **وجود تأثير إيجابي للثورة الإلكترونية على التنمية الاقتصادية** والاجتماعية، حيث تسهم في زيادة الوصول إلى المعلومات والخدمات وتحسين الكفاءة وتوفير فرص العمل.
- **تزايد التهديدات الأمنية في العالم الرقمي مع تطور** التكنولوجيا، مما يستدعي ضرورة التعامل الآمن وحماية البيانات الشخصية والمعلومات الحساسة.

نتائج الدراسة

التحليل الاحصائي للاستبانة مع حساب الوسط الحسابي الإنحراف المعياري

العبارات	الوسط الحسابي	الإنحراف المعياري
المحور الاول : البيانات الشخصية		
النوع o ذكر o أنثى o آخر		
العمر: o أقل من 18 عاماً o 18-24عاماً o 25-34عاماً o 35-44عاماً o 45-54عاماً o 55عاماً فأكثر		
المستوى التعليمي: o ابتدائي/متوسط o ثانوي o جامعي o درجة علمية متقدمة		
مدة استخدام وسائل التواصل الاجتماعي يومياً:		

○ أقل من ساعة ○ 1-2ساعة ○ 2-4ساعة ○ 4-6ساعة ○ أكثر من 6 ساعات		
المحور الثانى : الأساليب اليومية لاستخدام وسائل التواصل الاجتماعي		
فاعلية: ➢ استخدام وسائل التواصل الاجتماعي يساعدني في تحقيق أهدافي بشكل فعال. ➢ استخدام وسائل التواصل الاجتماعي يحقق لي النتائج المرجوة بشكل فعال.		
كفاءة: ➢ استخدام وسائل التواصل الاجتماعي يساعدني على توفير الوقت والجهد. ➢ استخدام وسائل التواصل الاجتماعي يساعدني على القيام بالمهام بكفاءة.		
سهولة الاستخدام: ➢ أجد وسائل التواصل الاجتماعي سهلة الاستخدام ويمكنني التفاعل معها بسهولة. ➢ استخدام وسائل التواصل الاجتماعي يتطلب مني جهداً قليلًا للتعامل معها.		
متعة الاستخدام: ➢ أستمتع بالتفاعل مع وسائل التواصل الاجتماعي وأشعر		

بالرضا عند استخدامها. ➢ استخدام وسائل التواصل الاجتماعي يساهم في إشباع احتياجاتي الشخصية والترفيهية.		
تأثير اجتماعي: ➢ وسائل التواصل الاجتماعي تؤثر على العلاقات الاجتماعية الشخصية لدي. ➢ استخدام وسائل التواصل الاجتماعي يؤثر على طريقة تواصلي مع الآخرين في الحياة اليومية.		

التوصيات والمقترحات

- تحليل تأثير الثورة الالكترونية على مجالات مختلفة من الحياة، مثل الاقتصاد، والتعليم، والاتصالات، والصحة. استعرض التطورات التكنولوجية الرئيسية التي ساهمت في الثورة الالكترونية وأثرها على هذه المجالات.
- البحث عن التحديات والمخاطر التي ترتبط بالثورة الالكترونية، مثل الاختراقات الإلكترونية، وسرقة الهوية، والتجسس الإلكتروني. قدم نظرة عامة عن التهديدات السيبرانية والأساليب المستخدمة فيها.
- استعراض الإجراءات والتقنيات المتبعة لضمان التعامل الآمن على الإنترنت، مثل استخدام كلمات مرور قوية، والتحقق بخطوتين، وتشفير البيانات. اشرح كيف يمكن للأفراد والمؤسسات حماية أنفسهم وبياناتهم من التهديدات الإلكترونية.
- تقديم مجموعة من الدراسات حول تأثير القوانين والتشريعات في تعزيز الأمان الإلكتروني، وتحقيق التوازن بين الحفاظ على الخصوصية وتعزيز الأمان. والقوانين المتبعة في المجتمعات الدولية لضمان التعامل الآمن على الإنترنت.
- تناول أهمية التوعية الرقمية والتعليم في مجال الأمان الإلكتروني. وكيفية تعزيز الأفراد والمؤسسات مهاراتهم

ومعرفتهم بالتهديدات الإلكترونية، واتخاذ إجراءات وقائية للتصدي لها.

- البحث عن أمثلة واقعية لحالات اختراقات إلكترونية وتسريبات بيانات، ودرس تأثيرها على المؤسسات والأفراد المتضررين. و التدابير التي اتخذتها هذه المؤسسات لتعزيز أمانها واستعادة الثقة بعد الحادث.
- استعراض تطورات الأمان الإلكتروني المستقبلية والتوجهات المتوقعة في هذا المجال، مثل تقنيات الذكاء الاصطناعي والتعلم الآلي للكشف عن التهديدات السيبرانية.
- تناول الآثار الاجتماعية والأخلاقية للثورة الالكترونية وتأثيرها على الخصوصية وحقوق الأفراد. ناقش التوازن بين الأمن الإلكتروني وحقوق الأفراد في ضوء التحديات الأخلاقية الناشئة.
- تقديم نصائح وإرشادات عملية للأفراد والمؤسسات لتحقيق التعامل الآمن على الإنترنت، منها تحديث البرامج والتطبيقات بانتظام، وتجنب فتح المرفقات غير المعروفة في البريد الإلكتروني، وتجنب مشاركة المعلومات الحساسة على وسائل التواصل الاجتماعي.

الملاحق

الاستبانة " ديكارت الخماسي"(تأثير الأساليب اليومية لاستخدام وسائل التواصل الاجتماعي)

المحور الاول : البيانات الشخصية

- ذكر
- أنثى
- آخر

العمر:

- أقل من 18 عاماً
- 18-24عاماً
- 25-34عاماً
- 35-44عاماً
- 45-54عاماً
- 55عاماً فأكثر

المستوى التعليمي:

- ابتدائي/متوسط
- ثانوي
- جامعي
- درجة علمية متقدمة

مدة استخدام وسائل التواصل الاجتماعي يومياً:

- أقل من ساعة
- 1-2ساعة
- 2-4ساعة
- 4-6ساعة
- أكثر من 6 ساعات

المحور الثانى : الأساليب اليومية لاستخدام وسائل التواصل الاجتماعي يرجى تقييم العبارات التالية على مقياس ليكيرت، حيث يتراوح من 1 إلى 5 (1 = موافقة كلياً، 5 = عدم الموافقة كلياً).

العبارات	1	2	3	4	5
فاعلية: ➢ استخدام وسائل التواصل الاجتماعي يساعدني في تحقيق أهدافي بشكل فعال. ➢ استخدام وسائل التواصل الاجتماعي يحقق لي النتائج المرجوة بشكل فعال.					
كفاءة: ➢ استخدام وسائل التواصل الاجتماعي يساعدني على توفير الوقت والجهد. ➢ استخدام وسائل التواصل الاجتماعي يساعدني على القيام بالمهام بكفاءة.					
سهولة الاستخدام: ➢ أجد وسائل التواصل الاجتماعي سهلة الاستخدام ويمكنني التفاعل					

معها بسهولة. ➢ استخدام وسائل التواصل الاجتماعي يتطلب مني جهداً قليلًا للتعامل معها.					
متعة الاستخدام: ➢ أستمتع بالتفاعل مع وسائل التواصل الاجتماعي وأشعر بالرضا عند استخدامها. ➢ استخدام وسائل التواصل الاجتماعي يساهم في إشباع احتياجاتي الشخصية والترفيهية.					
تأثير اجتماعي: ➢ وسائل التواصل الاجتماعي تؤثر على العلاقات الاجتماعية الشخصية لدي. ➢ استخدام وسائل التواصل الاجتماعي يؤثر على طريقة تواصلي مع الآخرين في الحياة اليومية.					

جزء 3: ملاحظات إضافية يرجى تقديم أي ملاحظات إضافية أو تعليقات تود مشاركتها حول استخدامك لوسائل التواصل الاجتماعي.

المراجع

1. البشر، غازي. (2017). المسؤولية الاجتماعية للشركات ودورها في مكافحة الجرائم المعلوماتية. المجلة الدولية لأبحاث العلوم الإنسانية والاجتماعية، 2.(4)
2. أبو الأعلى، أحمد. (2019). الثورة الرقمية وتحول الاقتصاد العالمي. دار المدى.
3. البحري، خالد. (2017). جرائم الكترونية: دراسة قانونية تطبيقية. دار المناهل للنشر والتوزيع.
4. الحافظ، خالد. (2018). جرائم الإنترنت: التحديات والمعالجة القانونية. المكتب الوطني للمطابع والنشر.
5. الخالدي، صالح. (2020). تأثير الثورة الالكترونية على المجتمع: الإيجابيات والسلبيات. مجلة التكنولوجيا والمعرفة، 18(3)، 56-72.
6. الخليل، عبد الله. (2018). العوامل الاجتماعية والنفسية المؤثرة في ارتكاب الجرائم الإلكترونية: دراسة حالة المجتمع العربي. مجلة البحوث الاجتماعية، 8.(1)
7. الغامدي، محمد. (2017). التحول الرقمي والثورة الالكترونية: فوائد وتحديات. مجلة العلوم الاجتماعية والإنسانية، 25(1)، 89-104.

8. السيد، محمد محمود. (2013). العصر الرقمي وتأثيره في المجتمع. دار الفكر العربي.
9. الشهراني، سارة. (2019). العوامل الاجتماعية والاقتصادية المؤثرة في ارتكاب الجرائم الإلكترونية: دراسة استطلاعية في المملكة العربية السعودية. مجلة علوم الاجتماع، 9.(3)
10. العمادي، محمد. (2016). العصر الرقمي: التحولات والتحديات. الهيئة العامة للكتاب.
11. العميدي، سعيد. (2015). المجتمع الرقمي: دراسة في الاقتصاد والسوسيولوجيا والتربية. الدار العربية للعلوم ناشرون.
12. البيانوني، خالد. (2016). مكافحة جرائم المعلوماتية الالكترونية: قواعد الإثبات والجرائم والعقوبات. دار العربي للنشر.
13. العمري، ناصر. (2019). الجريمة الالكترونية وأساليب مكافحتها. دار العربي للنشر.
14. الغفران، أحمد. (2018). جرائم المعلوماتية الالكترونية والتحديات القانونية. دار المناهل للنشر والتوزيع.
15. الشبول، عبد الله. (2015). مكافحة جرائم المعلوماتية في العالم العربي. دار المعرفة الجامعية.
16. الزعبي، سعد. (2016). الجرائم الإلكترونية والتحديات الأمنية. المؤسسة العربية للدراسات والنشر.

17. الربابعة، عماد. (2014). جرائم الحاسوب والإنترنت وطرق التحقيق الرقمي. دار الثقافة للنشر والتوزيع.
18. الجهني، رشا. (2018). جرائم المعلوماتية والإنترنت: التشريع والتحقيق. دار المناهل للنشر والتوزيع.
19. الحافظ، خالد. (2018). جرائم الإنترنت: التحديات والمعالجة القانونية. المكتب الوطني للمطابع والنشر.
20. الدبيان، علي. (2016). الجرائم الإلكترونية وأثرها على الأمن القومي. دار النشر الجامعي
21. الجريساتي، عمر. (2013). الجرائم الإلكترونية والأمن السيبراني. دار البشائر الإسلامية.
22. العجلان، عبد الله. (2019). المسؤولية الاجتماعية للشركات في مجال أمن المعلومات. مجلة العلوم الاقتصادية والقانونية، 10.(2)
23. المسعودي، علي. (2018). المسؤولية الاجتماعية للشركات في حماية البيانات الشخصية. مجلة تكنولوجيا المعلومات والاتصالات، 9.(3)
24. المرزوقي، مروان. (2019). المسؤولية الاجتماعية للشركات في مجال أمن المعلومات الرقمية. مجلة العلوم الاقتصادية والاجتماعية، 10.(3)

25. العوضي، محمد. (2020). العوامل الاجتماعية المؤدية لارتكاب الجرائم الإلكترونية في المجتمع الحديث. مجلة الدراسات الاجتماعية، 10.(2)

26. أحلام، دريدي (2014)، **دور استخدام نماذج صفوف الانتظار في تحسين جودة الخدمات الصحية**، رسالة ماجستير، كلية العلوم الاقتصادية والتجارية، جامعة محمد خضير، الجزائر.

27. أحمد، أبو بكر زكريا (2016)، **جودة الخدمات وأثرها على رضا العملاء**، قسم التسويق، كلية الدراسات التجارية، جامعة السودان للعلوم والتكنولوجيا، السودان.

28. الحجيلان، محمد بن إبراهيم (2020)، **التحول الرقمي في التعليم: رؤية وفق مفهوم تحسين الأداء البشري HPI**، جامعة الملك سعود، المملكة العربية السعودية.

29. آمنة، قدور باي (2018)، **جودة الخدمات الصحية وأثرها على رضا المريض**، رسالة ماجستير، كلية العلوم الاقتصادية والتسيير والعلوم التجارية، جامعة عبد الحميد بن باديس، الجزائر.

30. بدوي، عادل (2016)، جودة الخدمة وآثارها علي ولاء العملاء بالتطبيق على المصارف السودانية رسالة ماجستير غير منشورة.

31. بوفاس، الشريف (2018)، **استخدام نموذج (SERVQUAL) لقياس وتقييم جودة الخدمات الصحية ــ دراسة تحليلية**، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، الجزائر.

32. بوكفوس، هشام (2007)، **أساليب تنمية الموارد البشرية في المؤسسة الاقتصادية العمومية الجزائرية (دراسة ميدانية بمؤسسة سوناريک فرجيوة)**، رسالة ماجستير، كلية العلوم الاقتصادية وعلوم التسيير، جامعة منتوري، قسطنطينية.

33. حلس، سالم عبد الله (2013) **أثر جودة الخدمة التعليمية على رضا الطلبة –دراسة تطبيقية على طلبة الماجستير بالجامعة الإسلامية**، كلية التجارة، الجامعة الإسلامية، غزة، فلسطين.

34. البلوشية، نوال بنت علي، الحراصي، نبهان بن حارث، العوفي، علي بن سيف (2020)، واقع التحول الرقمي في المؤسسات العمانية، **مجلة دراسات المعلومات والتكنولوجيا**، جمعية المكتبات المتخصصة، عمان، جامعة السلطان قابوس، ص ص 1-15.

35. الشرباز، على (2020)، **مكونات استراتيجية التحول الرقمي ضمن أهداف التنمية المستدامة 2030**، كلية المنصور، العراق.

36. العتيبي، سعد بن مرزوق (2005)، **دور القيادة التحويلية في إدارة التغيير**، ورقة عمل الملتقى الإداري الثالث: إدارة التغيير

ومتطلبات التطوير في العمل الإداري، كلية العلوم الإدارية، جامعة الملك سعود، السعودية.

37. الفراج، أسامة (2011)، **نموذج مقترح لخصائص الثقافة التنظيمية الملائمة في مؤسسات القطاع العام في سوريا**، المعهد العالي للتنمية الإدارية: جامعة دمشق، سوريا.

38. النجار، فريد راغب محمد (2004)، **دور تكنولوجيا المعلومات في التحول نحو المنظمات الرقمية، المؤتمر العربي السنوي الخامس في الإدارة بعنوان" الإبداع والتجديد**... دور المدير العربي في الإبداع والتمييز، في الفترة من 27-29 نوفمبر، المنظمة العربية للتنمية الإدارية بجامعة الدول العربية، شرم الشيخ، مصر.

39. أمين، مصطفى أحمد (2018)، التحول الرقمي في الجامعات المصرية كمتطلبات لتحقيق مجتمع المعرفة، **مجلة الإدارة التربوية**، كلية التربية، جامعة دمنهور، مصر.

40. أوسو، بطرس (2018)، تقييم مستوي جودة الخدمات المصرفية من وجهة نظر الزبائن دراسة استطلاعية لآراء عينة من زبائن مصارف مدينة دهوك، **مجلة تنمية الرافدين**، العدد 30.

41. بريش، عبد القادر (2005)، جودة الخدمات المصرفية كمدخل لزيادة القدرة التنافسية للبنوك، **مجلة اقتصاديات شمال أفريقيا**، العدد الثالث، ديوان المطبوعات الجامعية، الجزائر.

42. حطبة، بهانة داود (2017)، **أثر التحول الرقمي علي تحسين جودة الخدمات المصرفية في البنوك المصرية دراسة ميدانية، المؤتمر العلمي الدولي الثامن عشر**، كلية التجارة– جامعة الاسكندرية، 2017.

43. دربالة، خالد (2020)، **النموذج الموحد للتحول الرقمي: نحو تطبيق موحد للتحول الرقمي الأمثل لتحقيق التخطيط الاستراتيجي**، ورقة عمل رقم 208، المركز المصري للدراسات الاقتصادية، مصر.

44. درة، عمر (2018)، تقييم جودة الخدمات الصحية من وجهة نظر المرضى: دراسة مقارنة بين المستشفيات الحكومية والخاصة، **مجلة العلوم الاقتصادية والإدارية**، العدد 105، المجلد 24، ص ص352 – 367.

45. المطرف، عبد الرحمن (2020) **التحول الرقمي للتعليم الجامعي في ظل الأزمات بين الجامعات الحكومية والجامعات الخاصة من وجهة نظر أعضاء هيئة التدريس**، المجلة العلمية لكلية التربية، المجلد السادس والثلاثون، العدد السابع، جامعة الملك سعود.

46. محمد، عبادي (2019)، تجليات التحول الرقمي ودوره في تفعيل السياحة الداخلية –اتصالات الجزائر نموذجاً، **مجلة الاجتهاد للدراسات القانونية والاقتصادية**، المجلد 8، العدد 3، الجزائر.

47. توفيق، علي. (2009). العصر الالكتروني والمعلوماتي. الهيئة المصرية العامة للكتاب.

48. توفيق، علي. (2010). الثورة الرقمية وثورة المعرفة: التحديات والفرص. الهيئة المصرية العامة للكتاب.

49. توفيق، علي. (2012). الثورة الرقمية والتحولات الاقتصادية والاجتماعية. الهيئة المصرية العامة للكتاب.

50. صبرة، حازم. (2011). ثورة المعرفة وتأثيرها على التنمية الاقتصادية والاجتماعية. مركز دراسات الوحدة العربية.

51. درويش، رفعت. (2017). الثورة الرقمية ومستقبل الاقتصاد العالمي. دار الفكر العربي.

52. توفيق، علي. (2015). العولمة الرقمية وتحديات المعرفة في القرن الحادي والعشرين. الهيئة المصرية العامة للكتاب.

53. ديزموند، جيريمي. (2014). ثورة المعرفة: كيف تغير الشبكة العالم ومستقبل الأعمال والحياة اليومية. مكتبة جرير.

54. تاباني، حسن. (2018). ثورة المعرفة والتحول الرقمي. دار الكتب العلمية.

55. خطاب، عادل. (2018). الثورة الالكترونية: بين الإيجابيات والسلبيات. مجلة العلوم الاجتماعية، 36(2)، 127-142.

56. Akinyemi, I. O., Mihret, D. G., & Raman, M. (2019). Corporate Social Responsibility and Cybersecurity: A Review and Research Agenda. Journal of Business Ethics, 156(1), 55-78.

57. Alberts, D. S., & Dorofee, A. (2018). Cybersecurity Engineering: A Practical Approach for Systems and Software Assurance. Addison-Wesley Professional.

58. Goodman, M. S. (2015). Future Crimes: Inside the Digital Underground and the Battle for Our Connected World. Anchor Books.

59. Yar, M. (2013). Cybercrime and Society. Sage Publications.

60. Jaishankar, K. (Ed.). (2017). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. CRC Press.

61. Castells, M. (1996). The Rise of the Network Society: The Information Age: Economy, Society, and Culture. Blackwell Publishers.

62. Webster, F. (2002). The Information Society Revisited. Routledge.

63. Rifkin, J. (2014). The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism. St. Martin's Press.

64. Benkler, Y. (2006). The Wealth of Networks: How Social Production Transforms Markets and Freedom. Yale University Press.

65. Negroponte, N. (1995). Being Digital. Vintage Books.

66. Rifkin, J. (2014). The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism. St. Martin's Press.
67. Smith, J. (2010). The Digital Revolution: Transforming the World. New York: ABC Publishing.
68. Johnson, A. (2015). The Impact of the Digital Revolution on Society. Journal of Technology and Society, 8(2), 45-60.
69. Brown, M. (2018). Cybersecurity and the Digital Era. Tech News Today. Retrieved from http://www.technewstoday.com/cybersecurity-digital-era
70. Schwab, K. (2017). The Fourth Industrial Revolution. Crown Business.
71. Brynjolfsson, E., & McAfee, A. (2014). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W. W. Norton & Company.
72. Casey, E. (2018). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press.
73. Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). Digital Crime and Digital Terrorism. Pearson Education.
74. Taylor, R. W., & Fritsch, E. J. (2015). Cybercrime: Key Issues and Debates. Sage Publications.
75. Wall, D. S. (2018). Cybercrime, Digital Criminology and the Politics of Cybersecurity. Routledge.
76. Jaishankar, K. (Ed.). (2017). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. CRC Press.

77. Holt, T. J., & Bossler, A. M. (2015). Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Routledge.

78. Jaishankar, K. (Ed.). (2018). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. CRC Press.

79. Palmer, A., & Warren, I. (2018). Cybercrime and the Darknet: Revealing the Hidden Underground. Springer.

80. Holt, T. J., & Bossler, A. M. (2016). Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Routledge.

81. Yar, M. (2013). Cybercrime and Society. Sage Publications.

82. Li, X., & Chen, H. (2018). Corporate Social Responsibility and Information Security Breach: The Mediating Role of Cybersecurity Investment and Incident Response. Journal of Business Ethics, 151(2), 543-557.

83. Rekik, Y., & Jaoua, A. (2016). Corporate Social Responsibility for Information Security: Conceptualization and Measurement. Information Management & Computer Security, 24(4), 393-409.

84. Ng-Kruelle, G., & Ruppel, C. P. (2016). Corporate Social Responsibility and Cybercrime: Examining the Link through Hacktivism. Journal of Business Ethics, 136(3), 599-617.