Protection of personal information using the two-factor authentication feature from the point of view of users of Google and Facebook services

Mohammed Abdulwahab A. Al-Ahmadi [a]

Dr. Maher Mohsen Saleh Faqeha[b]

[b] Faculty of Arts and Humanities - Department of Information Science - King Abdul Aziz University

mfakeha@kau.edu.sa

Abstract: A feeling of security and reassurance is one of the ways of comfort in our lives, and a feeling of security includes all aspects of life, starting from protecting oneself and presentation, even protecting the name and identity. To achieve this feeling of security, we must protect ourselves and our properties, including our personal information. One of the advantages offered by some Internet service companies, and the study aimed to reveal the effectiveness of two-factor authentication in protecting personal information from the point of view of a sample of users of Google and Facebook services in the Kingdom of Saudi Arabia, and to educate them about how to protect their data and secure their information against electronic intrusion, and to show how to protect Principles and legislation for personal information in the Kingdom of Saudi Arabia. To achieve the objective of the study, the researcher used the quantitative approach for its relevance to the subject of the study by addressing the protection of personal information and two-factor authentication and by using statistical methods to analyze the responses of the study sample members of the users of Google and Facebook, then the researcher analyzed the responses using different statistical methods in the SPSS 23.

The study resulted in several results, the most important of which are: the feeling of the study sample members of Google and Facebook users of privacy and the security of their personal accounts at an average level, their high sense of privacy and security online in general, and also their appreciation of the role of the state in protecting personal data, in addition to the effectiveness of the two-factor authentication feature in protecting personal information.

In the end, the researcher recommended the importance of carrying out multiple studies and research on the application of various features of technological innovations to protect personal information and increase the level of privacy, and to direct those interested in technical fields to develop new techniques to protect privacy by filling the gaps that may be in the current technologies, and educating Internet and smartphone users of the need Protecting their personal information and not disclosing it to others, activating the media and social media to raise awareness against the dangers of lack of privacy, the circulation of personal information, and the use of real personal data on those sites, and activating the role of schools, universities and educational institutions to educate children and youth against the dangers of using the Internet, and the need to monitor them to God Almighty. In all their actions, and in how they use the Internet.

Keywords: Two-Factor Authentication - Personal Information - Privacy.

حماية المعلومات الشخصية باستخدام ميزة المصادقة الثنائية من وجهة نظر مستخدمي خدمات الجوجل والفيسبوك

محمد عبدالوهاب الأحمدي[a]

د.ماهر محسن صالح فقيها[b]

كلية الآداب والعلوم الانسانية– قسم علم المعلومات– جامعة الملك عبدالعزيز[a,b]

mfakeha@kau.edu.sa

المستخلص

الشعور بالأمان والاطمئنان أحد سبل الراحة في حياتنا، ويشمل الشعور بالأمان جميع مناحي الحياة، بدايةً من حماية النفس والعرض حتى حماية الاسم والهوية، ولتحقيق هذا الشعور بالأمان يجب أن نحمي أنفسنا وممتلكاتنا والتي من بينها معلوماتنا الشخصية ومن بين وسائل حماية المعلومات الشخصية المصادقة الثنائية، وهي إحدى الميزات التي تقدّمها بعض شركات خدمات الإنترنت، وقد هدفت الدراسة إلى الكشف عن مدى فاعلية المصادقة الثنائية في حماية المعلومات الشخصية من وجهة نظر عينة من مستخدمي خدمات جوجل والفيسبوك بالمملكة العربية السعودية، وتوعيتهم حول كيفية حماية بياناتهم وتأمين معلوماتهم ضد الاختراق الإلكتروني، وبيان كيفية حماية المبادئ والتشريعات للمعلومات الشخصية بالمملكة العربية السعودية. ولتحقيق الهدف من الدراسة استخدم الباحثان المنهج الكمي لمناسبته موضوع الدراسة بتناول حماية المعلومات الشخصية والمصادقة الثنائية وباستخدام الأساليب الإحصائية لتحليل استجابات أفراد عينة الدراسة من مستخدمي خدمات الجوجل والفيسبوك، حيث اعتمد الباحثان كأداة للدراسة استمارة استبيان تم توزيعها إلكترونيًا بطريقة عشوائية، وقد استجابت عينة قوامها (98) مستخدم، ثم قام الباحثان بتحليل الاستجابات بالأساليب الإحصائية المختلفة ببرنامج الحزمة الإحصائية SPSS 23.

وقد أسفرت الدراسة عن عدة نتائج، أهمها: شعور أفراد عينة الدراسة من مستخدمي خدمات الجوجل والفيسبوك بوجود الخصوصية وأمان حساباتهم الشخصية بمستوى متوسط، وارتفاع شعورهم بالخصوصية والأمان عبر الإنترنت عمومًا، وأيضاً تقديرهم لدور الدولة في حماية البيانات الشخصية، بالإضافة لفاعلية ميزة المصادقة الثنائية في حماية المعلومات الشخصية.

وفي النهاية قد أوصى الباحثان بأهمية القيام بدراسات وبحوث متعددة حول تطبيق ميزات متنوعة من المستحدثات التكنولوجية لحماية المعلومات الشخصية وزيادة مستوى الخصوصية، وتوجيه المهتمين بالمجالات التقنية لاستحداث تقنيات جديدة لحماية الخصوصية من خلال سد الثغرات التي قد تكون في التقنيات الحالية، وتوعية مستخدمي الإنترنت والهواتف الذكية بضرورة حماية معلوماتهم الشخصية وعدم الإفصاح عنها للآخرين، وتفعيل دول الإعلام ووسائل التواصل الاجتماعي للتوعية ضد

مخاطر عدم الخصوصية، وتداول المعلومات الشخصية، واستخدام بيانات شخصية حقيقية بتلك المواقع، وتفعيل دور المدارس والجامعات والمؤسسات التعليمية لتوعية الأطفال والشباب ضد مخاطر استخدام الإنترنت، وضرورة مراقبتهم لله عز وجل في كل تصرفاتهم، وفي كيفية استخدامهم للإنترنت.

الكلمات المفتاحية: المصادقة الثنائية – المعلومات الشخصية – الخصوصية.

المقدمة:

تعيش مجتمعاتنا في الوقت الحالي عصراً تزايدت فيه التخوفات، يسوده استخدام الإنترنت بشكل لم يكن كالسابق، وأصبح تبادل وتداول المعلومات والبيانات على نطاق واسع لم يعد له حدود، حتى أًصبحت المخاطر التي نتعرض لها وشبابنا اليوم لا تقتصر على الجرائم والتعدّيات المعروفة، بل أصبحت وسيلة التعلّم والترفيه والتواصل ـ الإنترنت ـ هي نفسها الخطر الأكبر علينا، حيث انتشرت مؤخرًا الجرائم التي ترتكب عبر الإنترنت، وتُعد إحدى تلك المخاطر التي قد نتعرض لها في أي لحظة نظرًا لاستخدامنا شبكة الإنترنت تهديد معلوماتنا الشخصية، ويرجع ذلك الخطر لما يستطيع مستخدمو هذه التكنولوجيا من فعله نتيجة تخزينها المعلومات المتعلقة بالأفراد واستغلالها في غير الأغراض التي أنشئت من أجله، حيث أصبحت البيانات سلعة تباع وتُشترى، ولها قيمة اقتصادية كبيرة لا يستهان بها، فنجد الشركات المتخصصة في شراء وبيع البيانات على مرأى ومسمع من الجميع، ويلجأ إلى خدماتها الكثيرين ممن يستخدمون تلك البيانات في أغراض غير مشروعة كالتهديد والابتزاز وغيرها، أو مشروعة كالتسويق والتجارة، وذلك بما تحمله هذه البيانات من إمكانية التنبؤ بتوجّهات الأفراد واهتماماتهم وما قد يثير اهتمامهم مستقبلاً، فضلاً عن أن الاحتفاظ بهذه البيانات يجعل من السهل الوصول إلى أصحابها وتوجيههم أو استهدافهم لخدمة أغراض معينة.(يونس، 2004)

في الواقع إن انتهاك الخصوصية عبر مواقع الشبكات الاجتماعية قد ينتج عن عدة عوامل؛ فعلى سبيل المثال قد يفصح المستخدمون عن معلومات شخصية تتطلبها بعض المواقع التي لا تتخذ الإجراءات الملائمة لحماية المستخدمين، حيث تتيح مثل هذه المواقع الإلكترونية حق تداول بيانات المستخدمين ومشاركتها مع أطراف ثالثة لاستخدام تلك المعلومات في عدة أغراض تخدم مصالح تلك الأطراف، وغالبًا لا تُفصح هذه المواقع عن سياسة الخصوصية التي يوافق عليها المستخدم من خلال زر يعطيه حق الولوج للصفحة التالية أو الخطوة التالية من التسجيل بالموقع على سبيل المثال؛ ومن ثَمَّ تلعب هذه البيانات دورًا اقتصاديًا كبيرًا في عمليات التسويق والإعلانات، واختيار جمهور مستهدف بالدعاية، ومعرفة النمط الاستهلاكي لكل فرد، وتصنيف المستخدمين حسب شرائحهم العمرية أو الاجتماعية أو الاقتصادية.

وعلى جانب آخر يشير (الملط، 2006) إلى عدة أسباب تدفع شبكات التواصل الاجتماعي لاعتماد المواصفات القياسية الخاصة بحماية البيانات الشخصية والخصوصية، مثل شهادة المواصفة ISO27001-2005 الخاصة بإدارة نظم حماية البيانات، ومن هذه الأسباب:

- المصداقية وزيادة الثقة.
- تحسين التعامل مع المستخدمين.
- زيادة ثقة المستخدمين وأصحاب العلاقة.
- التنظيم وحماية البيانات... إلخ.

وتُعد خدمات الجوجل Google والفيسبوك Facebook حاليًا شريانا التواصل بين شعوب العالم، وكذلك مركزا تبادل الثقافة والأخبار والمعلومات لكل الأعمار والمستويات ولكافة التخصصات العلمية والأدبية، وبالرغم من الانتقادات الشديدة التي تتعرض لها الخدمات المقدمة من هذه الشركات، إلا إن عدد مستخدميها في زيادة مستمرة وبشكل ملحوظ في كافة دول العالم، ومع انتشار شبكات التواصل الاجتماعي عبر الإنترنت أصبح من الضروري التنبيه والتعريف بمخاطر جمع وتخزين وتبادل البيانات الشخصية، ومخاطر تكنولوجيا المعلومات، وكل ما قد يمس الخصوصية والحريات العامة، ما يوجب على مقدمي الخدمات والمعلومات المتاحة عبر الإنترنت وخصوصًا خدمات الجوجل والفيسبوك المشاركة في تبنّي إجراءات أكثر شفافية لمعالجة البيانات والحصول على موافقة مستخدميهم من خلال نظام يمنح المستخدمين حق القبول أو الرفض قبل تداول البيانات الخاصة بهم، ومنحهم إمكانية الاختيار بوضوح لصفة الاتصالات الخاصة، كما ينبغي أن تتوفر لهم إمكانية اتخاذ القرارات حول درجة نفاذ الآخرين إلى بياناتهم واحتمالية استخدام أطراف ثالثة لها.(عرب، 2002)

وتنص سياسة حماية المعلومات والبيانات الشخصية في العديد من المواقع الإلكترونية والتطبيقات على بعض الشروط التي تمثّل انتهاكًا واضحًا لخصوصية المستخدم، والتي قد لا يلتفت إليها هذا الأخير عند إنشائه حسابًا جديدًا على الموقع أو تحميله التطبيقات عبر الهاتف المحمول أو المواقع الإلكترونية، وعلى النقيض مؤخرًا استجابت بعض الشركات المنتجة للتطبيقات لمطالبات المستخدمين التي أثيرت حول مستويات الخصوصية التي توفرها، وعملت على تحسين شروط خصوصية مستخدميها، ورهن نشر ومشاركة بياناتهم عبر هذه الشبكات الاجتماعية، أيضًا عملت تلك الشركات على منع السماح لأي شخص سواء بذاته أو ممثلاً عن أي جهة سيادية داخل الدولة أو خارجها في الحصول على ترخيص للولوج للبيانات الخاصة بالمستخدمين، وعدم السماح أو تسهيل نشر تسجيلات نصية أو صوتية للمستخدمين من خلال أي منافذ أخرى عبر شبكات التواصل الاجتماعي أو الإنترنت بشكل عام أو حتى من خلال وسائل الإعلام المختلفة المرئية والمسموعة، حيث لا يتم أي إجراء من ذلك إلا بالحصول على موافقة من المستخدمين أنفسهم واطلاعهم على ذلك سواء كان هذا بعد التسجيل في الموقع أو كأحد شروطه أو متى طُلب ذلك، إضافةً إلى ذلك فإن هناك إشكاليات عديدة تتعلق بحماية البيانات الشخصية في المنطقة العربية، حيث تتداخل المسؤولية القانونية للمحتوى في بعض الأحيان فيما بين المستخدم ووسطاء الإنترنت وخدمات الاتصالات، وتتعقد الأمور أكثر في بعض الأحيان عند الإشارة للجوانب القانونية لحماية البيانات الشخصية في مثل هذه المواقع، حيث يرى معظم الخبراء والقانونيين في كتاباتهم أنه لا يجب على المستخدمين الوثوق في ممارسات وخدمات الويب بشكل عام وشبكات التواصل الاجتماعي على وجه الخصوص، وذلك فيما يتعلق بحماية بياناتهم الشخصية.(الشمر، 2017)

وتُعد المصادقة الثنائية إحدى الطرق الحديثة الفعّالة لزيادة الأمان وحماية المعلومات والبيانات الشخصية للمستخدم أثناء استخدامه للتطبيقات والمواقع المختلفة، وهي إحدى المميزات التحفّظية التي تبنّتها العديد من الشركات مؤخرًا، حيث تتميز

المصادقة الثنائية الآن بالانتشار الواسع والتطبيق على مستوى العديد من الحسابات الشخصية عبر مواقع وتطبيقات متنوعة الأغراض، مثل تويتر Twitter، والفيس بوك Facebook، وحسابات ميكروسوفت Microsoft، وحسابات جوجل Google، وحساب دروب بوكس Dropbox وغيرها من الحسابات التي ينشئها المستخدم ليتمكن من استخدام خدمات الموقع أو التطبيق، وتكمن فكرة المصادقة الثنائية في أنه عند تسجيل المستخدم الدخول لإحدى تلك الحسابات المختلفة التي أنشأها من قبل من جهاز يختلف عن الجهاز المعتاد استخدامه للولوج لتلك الخدمات يتطلب منه حينها أن يدخل بياناته، ثم يؤكد أنه مالك الحساب من خلال الموافقة على رسالة تأكيد الهوية، وهي إما رسالة نصية هاتفية SMS تحتوي على كود يتم كتابته فيُسمح للمستخدم الولوج من الجهاز الجديد، أو رسالة تعريفية تظهر على شاشة الهاتف المحمول –المقترن بالحساب– أو عبر البريد الإلكتروني، حيث يجب على المستخدم الضغط على رابط إلكتروني أو أمر بالموافقة للسماح للجهاز الجديد الولوج مع تعريف المستخدم بنوع الجهاز الذي يحاول الولوج لحسابه وموقعه ووقت محاولة الدخول، وفي المقابل تظهر رسالة تعريفية على الجهاز الذي يطلب إذن الولوج للحساب تبين أنه تم إرسال طلب الإذن للهاتف المحمول المقترن، وعادةً ما يتم طلب الموافقة من خلال المصادقة الثنائية في كلّ تسجيل دخولٍ جديد كما ذكرنا، ولا يتم تطبيق هذه الخاصية إلا في حالة استخدام جهاز أو متصفحٍ جديد للولوج، وينصح بتفعيل خاصية المصادقة جنبًا إلى جنب مع كلمة المرور السرية –الشكل التقليدي لحماية البيانات–.(نصر الله، 2019)

وأهم مميزات المصادقة والتحكم في الوصول التقليل من مشكلات أمان البيانات التنظيمية والوصول المميز واستعادة البيانات وأيضًا تحديد مزايا وعيوب التشفير المتماثل والتشفير غير المتماثل، حيث يتم وضع مجموعة من السياسات لإنشاء كلمات المرور وصيانتها وتعديلها لاحقًا، بالإضافة إلى أمانها، حيث يعد التشفير وسياسة كلمات المرور القوية الركيزتان الإلزاميتان للأمان لمستخدمي خدمات جوجل Google والفيسبوكFacebook، ويمكن أن تقدم عملية المصادقة التي تؤكد أو تصادق على هوية الشخص وعمله عند استخدامها بالاقتران مع التوقيع الإلكتروني دليلاً على ما إذا كان قد تم العبث بالبيانات المستلمة بعد توقيعها من قبل المرسل الأصلي، في الوقت الذي أصبحت فيه عمليات الاختراق وتداول المعلومات غير المشروع منتشرة بصورة كبيرة، ما يجعل المصادقة وسيلة أكثر أمانًا للتحقق من هوية الشخص عند إجراء المعاملات عبر الإنترنت(Brando, 2018).

مشكلة الدراسة

تتمثل مشكلة الدراسة فيما ينتج عن الانفتاح وغياب الحدود بين مستخدمي مواقع التواصل الاجتماعي المختلفة والشبكات المتعددة وما تتمتع به من إيجابيات كثيرة يشعر بها المستخدم، إلا إنه يظل محاط بكثير من المخاوف التي تتصل بخصوصيته وحماية بياناته ومعلوماته الشخصية، وتعد سرقة المعلومات الشخصية من خلال تداولها مع أطراف ثالثة أو بيعها لشركات البيانات تهديداً خطيراً لمستخدمي خدمات الإنترنت؛ حيث يستخدم الملايين معلوماتهم الشخصية للحصول على تسجيل الدخول للمواقع عبر الإنترنت، مثل جوجل والفيسبوك، ويعد هذا الكم الهائل من المعلومات الشخصية من أسهل الأهداف لمخترقي الشبكات المعلوماتية وأيضًا مجمّعي البيانات بغرض بيعها لشركات البيانات، وتعتبر حماية المعلومات الشخصية من أكثر المشكلات شيوعًا التي تواجهها مواقع مثل جوجل Google والفيسبوك Facebook.

ويشير (Isaac & Frankel, 2018) إلى حادثة الاختراق التي تمت لبيانات 50 مليون حساب من حسابات مستخدمي موقع التواصل الاجتماعي الأكثر انتشارًا الفيسبوك Facebook عام 2018، والتي دفعت مؤسس موقع الفيسبوك مارك زوكربيرج Mark Zukerburg وفريقه إلى إلغاء الملفات التعريفية للوصول السريع لما يقارب من 90 مليون حساب على موقع الفيسبوك Facebook، ومن هنا كان لزامًا على هذه المواقع الدفع بميزة المصادقة الثنائية لحماية المعلومات الشخصية لمستخدميها كإحدى وسائل حماية المعلومات الشخصية من التداول غير المقيّد أو المأذون به من قبل صاحبها أو الاختراق أو المشاركة مع الغير، حتى أصبحت الكثير من الشركات تعمل على توفيرها لمستخدميها، وهو ما دفع الباحثان لتناول فاعلية ميزة المصادقة الثنائية في حماية المعلومات الشخصية من وجهة نظر مستخدمي خدمات جوجل Google والفيسبوك Facebook (Mate).

وتتلخّص مشكلة الدراسة في الإجابة عن التساؤل الرئيس التالي:

ما مدى فاعلية ميزة المصادقة الثنائية في حماية المعلومات الشخصية من وجهة نظر مستخدمي خدمات الجوجل والفيسبوك؟ ويتفرع منه التساؤلات الفرعية التالية:

1. ما مدى فاعلية المصادقة الثنائية في حماية المعلومات الشخصية من وجهة نظر مستخدمي خدمات الجوجل والفيسبوك بالمملكة العربية السعودية؟
2. كيف يمكن توعية مستخدمي خدمات جوجل Google والفيسبوك Facebook حول حماية بياناتهم وكيفية تأمين معلوماتهم ضد الاختراق الإلكتروني؟
3. كيف تساعد المبادئ والتشريعات بالمملكة العربية السعودية في حماية المعلومات الشخصية لمستخدمي الإنترنت؟

أهمية الدراسة

تكمن أهمية الدراسة الحالية في موضوعها، حيث إنه موضوع حيوي وحديث على المستوى العربي، حيث قلة الدراسات العربية التي تناولت ميزة المصادقة الثنائية في حماية المعلومات الشخصية، بالإضافة إلى التطور السريع لخدمات الجوجل Google والفيسبوك Facebook واتساع دائرة المستخدمين لهذه الخدمات بشكل مذهل وكبير؛ وما يعقبه من اختراق لمعلومات المستخدمين الشخصية من قبل أطراف ثالثة بغرض سرقتها أو بيعها لشركات البيانات؛ مما يشكّل انتهاكًا لحقوق المستخدمين، ولا يقل ذلك في تأثيره عن جرائم السرقة المالية والتعدي على حقوق الآخرين؛ ومن هذا المنطلق كان لابد من التوعية بأهمية حماية المعلومات الشخصية وعدم انتهاكها ووضع ضوابط لحماية المستفيدين والمستخدمين لخدمات التواصل الاجتماعي وشبكة الإنترنت من احتمالية الإضرار بهم من خلال اختراق بياناتهم وحماية أنفسهم من خلال خدمات الحماية القوية مثل المصادقة الثنائية، وتقديم التوعية للمستخدمين بطرق حماية معلوماتهم الشخصية.

أهداف الدراسة

تهدف هذه الدراسة إلى:

1. الكشف عن مدى فاعلية المصادقة الثنائية في حماية المعلومات الشخصية من وجهة نظر عينة من مستخدمي خدمات جوجل Google والفيسبوك Facebook بالمملكة العربية السعودية.
2. توعية مستخدمي خدمات جوجل Google والفيسبوك Facebook حول حماية بياناتهم وكيفية تأمين معلوماتهم ضد الاختراق الإلكتروني.
3. بيان كيفية حماية المبادئ والتشريعات للمعلومات الشخصية في المملكة العربية السعودية.

مصطلحات الدراسة:

- **خصوصية المعلومات** Information Privacy

يعرّفها (الغافري، 2008) على أنها القواعد التي تحكم جمع وإدارة البيانات الخاصة، كمعلومات بطاقات الهوية والمعلومات المالية والسجلات الطبية والسجلات الحكومية وكل ما يتصل بمفهوم حماية البيانات، وهناك نوع من المعلومات يطلق عليها "معلومات خاصة" كونها تتعلق بالشخص ذاته وتنتمي إلى كيانه كإنسان، مثل الاسم والعنوان ورقم الهاتف... وغيرها من المعلومات الشخصية، وهي معلومات تأخذ شكل بيانات تلزم الالتصاق بكل شخص طبيعي معرّف أو قابل التعريف.

- **حماية المعلومات الشخصية** Protection of personal information

يعرّفها (كامل، 2016) بأنها حماية المعلومات والبيانات المتداولة عبر شبكة الإنترنت من العبث والتخريب والتبديل، أو من أي خطر يهددها مثل وصول أي شخص غير مخول للوصول إليها والعبث ببياناتها والاطلاع عليها، وذلك من خلال توفير الوسائل والطرق اللازمة لحمايتها من المخاطر الداخلية والخارجية، وموضوع أمن المعلومات هو موضوع قديم، ولكن زادت الحاجة والطلب عليه مع انتشار استخدام الإنترنت والاعتماد عليه في كافة مجالات الحياة؛ مما تطلب نقل البيانات والمعلومات عبر الشبكات المتعددة، كما أتاح انتشار شبكات التواصل الاجتماعي الحاجة الملحّة لذلك.

وعلى ذلك يعرّفها الباحثان ضمن نطاق الدراسة على أنها توفير الوسائل والطرق اللازمة لحماية ما من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلاً للتعرّف عليه بصفة مباشرة أو غير مباشرة، ويشمل ذلك –على سبيل– الاسم وأرقام الهويات الشخصية، والعناوين، وأرقام التواصل، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور المستخدم الثابتة أو المتحركة... وغير ذلك من البيانات ذات الطابع الشخصي.

- **المصادقة الثنائية** Two-factor authentication

كما جاء ضمن سياسة الخصوصية لشركة جوجل Google فهي إحدى وسائل حماية المعلومات الشخصية من التداول غير المقيّد أو المأذون به من قبل صاحبها أو الاختراق أو المشاركة مع الغير والتي توفرها الآن بعض الشركات لمستخدميها، وهو ما عرّفها به (Stanslav, 2015).

ويعرّفها الباحثان على أنها عملية أمنية يتم فيها الطلب من مستخدم موقع التواصل الاجتماعي Facebook وحسابات Google إثبات هويته من خلال طريقتين مختلفتين، وذلك للتأكد من هوية الشخص مالك الحساب الحقيقي المثبت بقاعدة بيانات الموقع.

الدراسات السابقة

توصل الباحثانان من خلال الاطلاع على الأدبيات والدراسات المتعلقة بموضوع الدراسة إلى عدة دراسات ذات أهمية وصلة بموضوع الدراسة الحالية، وقد قسّمها الباحثان إلى ثلاثة محاور على النحو التالي:

المحور الأول: الخصوصية

دراسة (المعداوي، 2018) بعنوان: "حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي: دراسة مقارنة."

وقد هدفت الدراسة إلى دراسة حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي من خلال البحث عن النصوص والتشريعات العربية والأوروبية في هذا الخصوص مع الاسترشاد بالأحكام القضائية الصادرة عن القضاء الفرنسي من أجل توفير الحماية اللازمة للبيانات ذات الطابع الشخصي من الاعتداء عليها عبر شبكات مواقع التواصل الاجتماعي، وقد تطرقت الدراسة إلى تحديد ماهية البيانات الشخصية محل الحماية من الاعتداء عليها عن طريق استغلالها في أغراض الإعلانات التجارية؛ وقد أسفرت الدراسة عن أن البيانات الشخصية هي جميع البيانات المتعلقة بشخص طبيعي محدد والتي تتضمن اسمه الأول واسم العائلة وعنوان البريد الإلكتروني وكلمة المرور والجنس وتاريخ الميلاد؛ وكذلك كافة المعلومات أو البيانات التي يطلبها الموقع من المستخدم الذي يرغب في التسجيل على موقع معين على شبكة الإنترنت، كما أظهرت الدراسة مظاهر وصور الاعتداء على الخصوصية المعلوماتية، وقد أوصى الباحثان بعدد من التوصيات، أهمها ضرورة إلزام المشرع المصري بالتدخل لإصدار قانون لحماية البيانات ذات الطابع الشخصي كنظيره الفرنسي، وإنشاء لجنة يكون دورها السهر على تطبيق هذا القانون كنظيرتها اللجنة الوطنية الفرنسية للمعلوماتية والحريات، وكذلك ضرورة استمرار المحاكم القضائية في قبول دعاوى الاعتداء على البيانات الشخصية على مواقع التواصل الاجتماعي حتى يصدر القانون المقترح.

دراسة (الموسوي وفضل الله، 2013) بعنوان: "الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها."

وقد هدفت الدراسة إلى بيان أهم التأثيرات الجانبية المتعلقة بالأمن والتهديدات التي تحملها تقنيات المعلوماتية ومعالمها وحدودها، حيث تناولت الدراسة حاجة المجتمعات العربية الماسة للمعرفة الكثيرة من المعلومات الاقتصادية والسياسية والاجتماعية والعلمية، حيث أصبح الحاسب الآلي أحد أهم سمات وضرورات حسن تنظيم الإدارة، وقد أسفرت الدراسة عن أن سياسة حماية الخصوصية المعلوماتية لم تُطَبَّق في دولة العراق حتى عام 2013، وعدم وجود أي قوانين أو تشريعات بالعراق وقت الدراسة لحماية معلومات المواطنين الشخصية من الانتهاك من قبل الآخرين، وأنه من الضروري تقسيم الانتهاكات غير المشروعة التي يمكن التعرّض لها في فضاء الإنترنت بتوظيف معايير قانونية، حيث تكون أنواع الجرائم حسب الجسامة والطبيعة والأركان، وقد أوصى الباحثانان بضرورة قيام المسؤولين بتشريع قوانين لحماية سرية الخصوصية المعلوماتية بالعراق، وضرورة تلقّي مستخدمي الإنترنت والمواطنين عمومًا دورات للتثقيف حول كيفية حماية خصوصيتهم المعلوماتية من خلال الندوات والدورات والمؤتمرات، وكذلك من خلال وسائل الإعلام المختلفة.

دراسة (Mendel, et al., 2012) بعنوان:

"**Global Survey on Internet Privacy and Freedom of Expression**".

وقد هدفت الدراسة إلى تقييم المحتوى الاجتماعي والسياسي والثقافي المتضمن في تشريعات الخصوصية وحماية البيانات عالمياً من خلال عرض الصعوبات والتباينات الثقافية في استخدام اصطلاح الخصوصية واختلاف المفهوم القانوني أيضًا للخصوصية بين النظم القانونية المختلفة وفي نطاق المفهوم القانوني للخصوصية، وقد أسفرت الدراسة عن أن ما يقرب من ثلاثة أرباع عينة الدراسة يعترفون بأنهم يعملون في المكتبات التي لديها سياسة رسمية أو غير رسمية لمواقع التواصل الاجتماعي، وأن حوالي 53% من تلك السياسات تذكر خصوصية المستفيد، وعدم وجود توافق في الآراء بشأن مدى التزام المكتبات بحماية خصوصية المستفيد في مواقع التواصل الاجتماعي، ما يمكن أن يشكل انتهاكًا لخصوصية المستخدمين لهذه المواقع، وقد أوصى الباحثان بضرورة أن تبذل الدول جهودًا مكثّفة لنشر الوعي حول الخصوصية والتقنيات الحديثة التي تستهدف في الأصل الشباب من خلال التعليم والمدرسة والاستخدام ضمن أنظمة أخرى، وتفعيل دور الإعلام لرفع مستوى الوعي حول أهمية الخصوصية والآثار المترتبة على انتهاك الخصوصية، وكذلك تفعيل دول الجهات الاجتماعية الأخرى كمقدمو خدمات الإنترنت على سبيل المثال لتسليط الضوء على المخاطر المحتملة لإهمال خصوصية المستخدمين.

دراسة (Fernandez, 2010) بعنوان:

"**Privacy and Generation Y: Applying Library Values to Social Networking Sites** ".

وقد هدفت الدراسة إلى تطبيق قيم المكتبات والمعلومات على مواقع الشبكات الاجتماعية، حيث تناول الباحثان أن أخصائيي المكتبات يواجهون العديد من التحديات عند التعامل مع قضايا الخصوصية داخل مواقع التواصل الاجتماعي، وتقدم الدراسة خمس توصيات لأخصائي المكتبات في توسيع نطاقها والالتزام التقليدي بالخصوصية في مجال مواقع التواصل الاجتماعي،

والتوصية الأولى هي ضرورة التفرقة بين المعرفة والمعلومات بشكل دقيق، أما الثانية فضرورة أخذ دور القيادة في المناقشة العامة حول الخصوصية، والثالثة هي احترام حدود المستفيدين، أما الرابعة فالتحديث المستمر للسياسات والخصوصية، وأخيرًا شرح نموذج الخصوصية وكيفية تطبيقه للمستفيدين بشكل عام.

دراسة (Mannheimer, et al., 2016) بعنوان:

"**On the Ethics of Social Network Research in Libraries**".

وقد هدفت الدراسة إلى الكشف عن الأبعاد الأخلاقية لأمناء المكتبات وأعضاء هيئة التدريس في جامعة ولاية مونتانا، لإجراء البحوث العلمية باستخدام بيانات مواقع الشبكات الاجتماعية بهدف توجيه أمناء المكتبات والباحثين نحو أخلاقيات الخصوصية، حيث ربطت الدراسة بين القضايا الأخلاقية وممارسة أمناء المكتبات والباحثين، حيث يتطلب دور أمين المكتبة والباحثان إطارًا أخلاقيًا خاصًا، وقد أظهرت نتائج الدراسة وجود تحدياً كبيراً يواجهه أمين المكتبة من التضارب والتكافؤ بين القيم الفريدة لخصوصية المستخدم أو المستفيد والوصول إلى البيانات، وقد اقترح الباحثون إطار أخلاقي لإجراء البحوث واحترام الخصوصية في المكتبات يربط بين الاستفادة من المكتبات وشبكات التواصل الاجتماعي ومدى احترام الخصوصية والأخلاقيات في إعداد الأبحاث العلمية، حيث يخرج بوضع ميثاق أخلاقي لأبحاث الشبكات الاجتماعية والاهتمام بالخصوصية في هذا الشأن.

دراسة (Boyd, 2008) بعنوان:

"**Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence**".

وقد تناولت الدراسة إعلان موقع الفيسبوك عن خدمة الأخبار News Feeds وعدم استجابة الأفراد للانضمام لهذه الخدمة تخوّفًا من انعدام الخصوصية، ولأغراض حماية بياناتهم الشخصية، ما جعل هناك سخط كبير بين المستخدمين لموقع فيس بوك على الموقع ذاته، ما دفع شركة فيسبوك للاهتمام بالتقيد ببنود الخصوصية وحماية بيانات المستخدمين، وتعرض الدراسة اهتمامات الخصوصية التي تم التعبير عنها في أعقاب هذه الأحداث، والبيانات التي تظهر بسهولة والتي يمكن الوصول إليها بأقل جهد، وقد أظهرت الدراسة أن مصطلح "الأصدقاء" على مواقع التواصل الاجتماعي يشير إلى اتصال توافقي بين اثنين من المستخدمين.

دراسة (Madden, 2012) بعنوان:

"**Privacy Management on Social Media Sites**"

وقد هدفت الدراسة إلى توضيح تفاصيل دقيقة ونسب كمية الملفات التي تحمل طابع الخصوصية لمستخدمي شبكات التواصل الاجتماعي وخاصةً الشباب، حيث تشير الدراسة إلى أن اثنين من بين كل ثلاثة مستخدمين لشبكة الإنترنت لهما ملف شخصي على مواقع التواصل الاجتماعي، وأن نسبة 20% فقط من المستخدمين يفعّلون خاصية حماية الخصوصية لديهم

واختيار ما هو مناسب لهم ولبياناتهم الشخصية، وقد أظهرت الدراسة وجود فجوة كبيرة في امتلاك ملفات الخصوصية بين النساء والراجل من حيث الاهتمام بمستوى الحماية لها.

المحور الثاني: المصادقة الثنائية

دراسة (Cristofaro, et al., 2013) بعنوان:

"**A Comparative Usability Study of Two-Factor Authentication**".

وقد تناولت الدراسة نقاط الضعف في كلمات المرور النصية ودفعت إلى الحاجة إلى بدائل أكثر أمانًا، حيث في السنوات الأخيرة ظهرت المصادقة الثنائية باعتبارها الحل الأكثر استخدامًا لتقوية كلمات المرور من خلال مطالبة المستخدمين بتقديم أكثر من عامل مصادقة وتهدف المصادقة الثنائية إلى تعزيز المرونة ضد هجمات التخمين وخروقات قواعد بيانات كلمات المرور، ولكنها تكلّف المستخدم ومقدمي الخدمة تكاليف لا يمكن إهمالها، ويتطلب من المستخدمين تنفيذ إجراءات إضافية أثناء عملية المصادقة، ورغم ذلك فلم تركّز الدراسة بشكل كبير على قابليتها للاستخدام، ولتحقق الدراسة هدفها حول قابلية استخدام مقارنة للمصادقة الثنائية، قام الباحثون بدراسة أولية لمعرفة تقنيات المصادقة الثنائية الأكثر شيوعًا بالتطبيق على (9) مشاركين، بالإضافة إلى الدوافع التي يتم استخدامها فيها، ومن خلال توزيع استبيان على (219) مستخدماً لـ Mechanical Turk بهدف استكشاف تقنيات المصادقة الثنائية وقياس قابلية استخدام ثلاثة أنواع شائعة، هي الرموز وأرقام التعريف الشخصية والهاتف الذكي المخصص، ما ساعد في تسجيل الدوافع، ودراسة تأثيرها على قابلية الاستخدام المتصورة، وقد قدّمت الدراسة تحليل استكشافي لرصد بعض العوامل الرئيسية التي تؤثر على قابلية استخدام المصادقة الثنائية، وقد سلطت نتائج الدراسة الضوء على ضرورة عمل المزيد من الأبحاث والدراسات في هذا المجال للوصول لأفضل تقنيات مستخدمة أو يمكن استخدامها واستحداثها لحماية البيانات الشخصية.

دراسة (Nath & Mondal, 2016) بعنوان:

"**Issues and Challenges in Two Factor Authentication Algorithms**".

وقد هدفت الدراسة إلى القضايا والتحديات في استخدام خوارزميات المصادقة الثنائية، حيث تم دراسة كيفية تقديم المصادقة ذات العاملين من أجل تعزيز الأمن في أنظمة المصادقة كذلك إدخال عوامل مختلفة، حيث تم دمجها من أجل وسائل التحكم في الوصول، حيث أدى الطلب المتزايد على تطبيقات الأمان العالي إلى اهتمام متزايد بحماية البيانات السرية باستخدام كلمة المرور، والرمز المميز، والقياسات الحيوية وما إلى ذلك، وقد أسفرت الدراسة عن أن المصادقة الثنائية أفضل أنواع المصادقة لحماية البيانات وبالأخص في حال المعاملات المالية الإلكترونية، وأنها مستقبل إجراءات الأمان، وأن شركات كثيرة قد اعتمدت المصادقة الثنائية مؤخرًا لشركة PayPal وغيرها من الشركات التي وجدت فائدة كبيرة ولاقت نجاحًا كبيرة في مجال حماية معلومات مستخدميها.

دراسة (Gunson, et al., 2011) بعنوان:

"User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking".

وقد تناولت الدراسة التحقيق في تصورات المستخدمين لقابلية استخدامهم لأساليب أمان المصادقة أحادية وثنائية العاملين في الخدمات المصرفية الهاتفية الآلية، وقد طُبّقت الدراسة على (62) عميلاً مصرفياً، وبعد مقارنة إجراء المصادقة القائم على المعرفة، وعامل واحد، وبناءً على أنها الأكثر شيوعًا في صناعة الخدمات المالية مع نهج عاملين، حيث بالإضافة إلى الخطوة القائمة على المعرفة، تم إنشاء رمز مرور مؤقت باستخدام رمز أمان للأجهزة، ومن خلال جمع النتائج حول قابلية الاستخدام والأمان الملحوظ للطريقتين الموصوفتين جنبًا إلى جنب مع معدلات إتمام المكالمات ومدد المكالمات للطريقتين، توصلت الدراسة إلى اختلافات كبيرة بين الطريقتين، حيث يُنظر إلى الإصدار الثنائي على أنه يوفر مستويات أمان أعلى من إصدار المصادقة أحادية العامل؛ ورغم ذلك تم تعويض هذا الكسب من خلال تصورات أقل بكثير لقابلية الاستخدام، وتقديرات أقل للراحة وسهولة الاستخدام للإصدار ثنائي العوامل، بالإضافة إلى ذلك، فقد استغرق إصدار المصادقة ذات العاملين وقتًا أطول حتى يكتمل المشاركون، وقد قدّمت الدراسة أدلة تجريبية قيّمة للمفاضلة بين الأمان وقابلية الاستخدام في الأنظمة الآلية.

دراسة (Colnago, et al., 2018) بعنوان:

""It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University".

وقد ناقشت الدراسة انخفاض معدلات اعتماد المصادقة الثنائية لحماية البيانات على الرغم من الحماية الإضافية التي توفرها بهدف فهم كيفية تبني المصادقة الثنائية وعوائق ذلك بشكل أفضل، حيث لاحظ الباحثون نشر نظام المصادقة الثنائية في جامعة كارنيجي ميلون(CMU) ، ما دفعهم لهذه الدراسة لاستكشاف سلوكيات وآراء المستخدمين حول تبنّي المصادقة الثنائية بإرادتهم أو جبرًا، وقد أظهرت نتائج الدراسة أن المستخدمين ممن أجبروا على تبنيها وجدوا أن المصادقة الثنائية مزعجة ولكنها سهلة الاستخدام إلى حد ما، ويعتقدون أنها تجعل حساباتهم أكثر أمانًا؛ أما المستخدمين في جامعة CMU والذين تبنوا المصادقة الثنائية بإرادتهم أظهروا تصورات إيجابية، وقد ظهرت اختلافات بين المستخدمين حول تبني المصادقة الثنائية أولئك الذين تبنوها بإرادتهم أقل من المتوقع، وقد كشفت الدراسة العلاقة بين أنماط الاستخدام المختلفة وقابلية الاستخدام المتصورة، وحددت المفاهيم الخاطئة للمستخدم والممارسات غير الآمنة ومشكلات التصميم، وقد أوصت الدراسة بضرورة نشر نظام المصادقة الثنائية على نطاق واسع لتوسيع مجالات الاعتماد، مع التركيز على ضرورة التنفيذ، واستخدام تفويضات التبني والرسائل الاستراتيجية.

المحور الثالث: حماية المعلومات

دراسة (أحمد، 2017) بعنوان "قانون حماية البيانات الشخصية في مواقع التواصل الاجتماعي لمؤسسات المكتبات والمعلومات: دراسة تحليل مضمون."

وقد ركّزت الدراسة على معرفة سبل حماية بيانات مستخدمي شبكات التواصل الاجتماعي المتمثلة في القوانين والتشريعات وتطبيق ذلك في مواقع شبكات التواصل الاجتماعي بشكل عام، والمكتبات ومؤسسات المعلومات بشكل خاص عن طريق عدد من الإقرارات القانونية وشروط التسجيل والخصوصية المتاحة، وسياسات حفظ بيانات المستخدمين ونشرها، بالإضافة إلى زيادة وعي المستفيدين في المكتبات حول حماية بياناتهم وكيفية تأمين أنفسهم في هذا المجتمع التكنولوجي الجديد، وقد اعتمد الباحثان على تحليل محتوى مضمون ملفات الخصوصية والتسجيل على مواقع شبكات التواصل الاجتماعي من خلال تحليل وتفسير القوانين والتشريعات الخاصة بحماية البيانات الشخصية والخصوصية، ثم معرفة مدى تطبيق هذه التشريعات والقوانين في مواقع التواصل الاجتماعي للمكتبات الجامعية من حيث بناء ملفات الخصوصية للمكتبة والتسجيل في مثل هذه المواقع، وقد صمم الباحثان قائمة مراجعة وفقًا للقوانين والتشريعات التي تحمي وتحفظ البيانات الشخصية والخصوصية، وقد أسفرت الدراسة عن وضع تصور مقترح لإنشاء سياسة خاصة بالمكتبات لحماية الخصوصية والبيانات الشخصية على مواقع التواصل الاجتماعي الخاصة.

دراسة (الهادي، 2006) بعنوان "توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية."

وقد تناولت الدراسة التوسع الكبير في استخدام تطبيقات وخدمات نظم المعلومات الإلكترونية المحمولة على كافة أنواع شبكات المعلومات التي يعتمد بعضها على البعض، وناقشت متطلبات أمن المعلومات المختلفة، وعمليات التحقيق من أمن المعلومات وتطوير السياسة، وكذلك إجراءات المحاسبة والتنفيذ المحتاج إليها، والاعتبارات والأبعاد الموجهة، وحماية المعلومات في ظل الحكومة الإلكترونية، وقد أسفرت الدراسة عن دعوة للحكومات ووحدات القطاع العام والقطاع الخاص وكل الأطراف المعنية بأمن نظم المعلومات إلى اتخاذ الخطوات اللازمة لحماية أمن وشفافية النظم طبقًا لمبادئ توجيهات ومعايير الأمن التي طورتها المنظمات الدولية المختصة.

دراسة (الرشيدي، 2005) بعنوان "العدوان على البيئة المعلوماتية خطورته ومواجهته."

وقد تناولت الدراسة خطورة العدوان على البيئة المعلوماتية، وكيفية مواجهته من خلال استعراض حجم الجريمة الإلكترونية ومدى خطورتها على البيئة المعلوماتية، وقد أظهرت الدراسة أن 24% إلى 42% من الجرائم في المنظمات في القطاعين الحكومي والخاص كانت ضحية التقنية الحاسوبية، وأن (145) إلى (730) مليون دولار سنويًا حجم خسارة (72) شركة بسبب جرائم الحاسب الآلي، وقد أوصت الدراسة بضرورة تطوير الحلول الوطنية أو على الأقل وضع الحلول الأجنبية بعين الاعتبار بالاختبارات المكثّفة والدراسات المعمّقة لتوظيفها في المجتمع العربي.

دراسة (Abu–Musa, 2001) بعنوان:

"**Evaluating the Security of Computerised Accounting Information system: An Empirical Study on the Egyptian Banking Industry**".

وقد هدفت الدراسة لاستكشاف واختبار المخاطر الهامة التي تهدد حماية المعلومات المحاسبية الإلكترونية في القطاع المصرفي بمصر، حيث قام الباحثان بدراسة مسحية لجميع البنوك الرئيسية العاملة بالدولة باستخدام استمارة استقصاء للتعرف على آراء رؤساء أقسام الحاسب الآلي في البنوك العاملين بها، وقد أسفرت نتائج الدراسة عن أن الإدخال غير المتعمّد لبيانات غير صحيحة والتدمير غير المتعمّد للبيانات من قبل الموظفين، وإدخال فيروس الكمبيوتر إلى النظام، والكوارث الطبيعية والتي من صنع الإنسان، واشتراك بعض الموظفين في استخدام نفس كلمة السر، وكذلك توجيه البيانات والمعلومات إلى أشخاص غير مخوّل لهم باستلامها تُعد من أهم المخاطر التي تواجه أمن المعلومات الإلكترونية في المنشآت، وقد أظهرت الدراسة أن رؤساء أقسام المراجعة الداخلية في على مستوى الدراسة ككل قد أعطوا تقديرات أعلى لمعدلات حدوث تلك المخاطر في المنشآت التي يعملون بها مقارنة بتقديرات رؤساء أقسام الحاسب الآلي، كما أسفرت عن عدم وجود لاختلافات جوهرية بين أنواع المنشآت المختلفة إلا فيما يختص بالمرور غير المرخص به للبيانات أو النظام من قبل أطراف خارجية (قراصنة المعلومات.)

دراسة (Csonka, 2000) بعنوان:

"**Internet Crime: The Draft Council of Europ Convention on Cyber–Crime: A Response to the Challenge of Crime in the Age of the Internet?**".

وقد جاءت الدراسة كمشروع لوضع اتفاقية بمجلس أوروبا حول جرائم الإنترنت، وقد قامت الدراسة بمشاركة (358) مؤسسة أمريكية تضم وكالات حكومية وبنوك ومؤسسات مالية، ومؤسسات صحية وجامعات للوقوف على بنود الاتفاقية، وقد أظهرت الدراسة خطر جرائم الكمبيوتر وارتفاع حجم الخسائر الناجمة عنها، وأن 85% من الجهات التي تناولتها الدراسة قد تعرضت لاختراقات حاسوبية خلال 1999، وأن 64 %لحقت بهم خسائر مادية جراء هذه الاعتداءات، وأن 35% تمكّن من حساب مقدار خسائره المادية التي بلغت تقريبًا 378 مليون دولار، في حين كانت الخسائر لعام 2000 في حدود 265 مليون دولار، أما عن مصدر وطبيعة الاعتداءات فقد أشارت الدراسة إلى أن 40% من الاعتداءات تمت من خارج المؤسسات، مقابل 25% في عام 2000، وأن نسبة الموظفين الذين ارتكبوا أفعال إساءة استخدام اشتراك الإنترنت لمنافع شخصية بلغت 91% تتوزع بين الاستخدام الخاطئ للبريد الإلكتروني وتنزيل مواد إباحية من الشبكة، في حين كانت النسبة 79% لعام 2000، وأن 94% من المشاركين تعرضوا لهجمات فيروسية عبر الإنترنت.

التعليق على الدراسات

بعد أن استعرض الباحثان الدراسات السابقة خلصا إلى الآتي:

ركزت الدراسات جميعها على أهمية خصوصية المعلومات عبر مواقع التواصل الاجتماعي، مثل دراسة (المعداوي، 2018) و(الموسوي وفضل الله، 2013) و(أحمد، 2017) و(Madden, 2012)، حيث اتفقت هذه الدراسات مع موضوع الدراسة الحالية في تناول حماية المعلومات عبر وسائل التواصل الاجتماعي، والبحث عن طرق خصوصية المعلومات، كما تناولت بعض الدراسات أهمية إصدار القوانين والتشريعات لحماية خصوصية المعلومات كدراسة (المعداوي، 2018).

في حين تطرقت بعض الدراسات لإجراء بحوث باستخدام بيانات مواقع الشبكات الاجتماعية بهدف توجيه أمناء المكتبات والباحثين نحو أخلاقيات الخصوصية كدراسة (أحمد، 2017) و.(Fernandez, 2010)

بينما اهتمت دراسة (Abu-Musa, 2001) باختبار المخاطر الهامة التي تهدد حماية المعلومات المحاسبية الإلكترونية في القطاع المصرفي، بينما اهتمت دراسة (الرشيدي، 2005) بتناول خطورة العدوان على البيئة المعلوماتية، وكيفية مواجهته من خلال استعراض حجم الجريمة الإلكتروني.

وعلى الجانب الآخر فقد اتفقت الدراسة الحالية في تفعيل المصادقة الثنائية مع دراسة (Cristofaro, et al., 2013) و (Nath & Mondal, 2016) و(Gunson, et al., 2011)، حيث ظهرت المصادقة الثنائية باعتبارها الحل الأكثر استخدامًا لتقوية كلمات المرور من خلال مطالبة المستخدمين بتقديم أكثر من عامل مصادقة وتهدف المصادقة الثنائية إلى تعزيز المرونة ضد هجمات التخمين وخروقات قواعد بيانات كلمات.

كما اتفقت الدراسة الحالية مع الدراسات التي تناولت حماية المعلومات كدراسة (أحمد، 2017)، حيث ركّزت على معرفة سبل حماية بيانات مستخدمي شبكات التواصل الاجتماعي المتمثلة في القوانين والتشريعات، ودراسة (الهادي، 2006) و (Csonka, 2000) التي دعت إلى اتخاذ الخطوات اللازمة لحماية أمن وشفافية النظم طبقًا لمبادئ توجيهات ومعايير الأمن التي طورتها المنظمات الدولية المختصة حول جرائم الإنترنت.

وقد أوصت دراسة (Madden, 2012) بضرورة بذل الدول جهودًا مكثّفة لنشر الوعي حول الخصوصية والتقنيات الحديثة، وتفعيل دور الإعلام لرفع مستوى الوعي حول أهمية الخصوصية، والآثار المترتبة على انتهاك الخصوصية.

بينما أوصت دراسة (Gunson, et al., 2011) بضرورة نشر نظام المصادقة الثنائية على نطاق واسع لتوسيع مجالات الاعتماد، مع التركيز على ضرورة التنفيذ، واستخدام تفويضات التبني، والرسائل الاستراتيجية.

ومما سبق يتضح للباحث أن الدراسات السابقة كانت شاملة وكافية لجميع جوانب الموضوع من خلال حماية المعلومات الشخصية باستخدام ميزة المصادقة الثنائية، وقد حاول الباحثان من خلال الدراسة بناءً على ما سبق تناوله التعرف على أهمية ميزة المصادقة الثنائية والتطرق إلى طرق الاستفادة منها بجانب ما تم تناوله في الدراسات السابقة، بالإضافة إلى حماية المعلومات وكيفية حماية خصوصية المعلومات؛ لذلك تعد الدراسة الحالية متممة لتلك الدراسات.

ولقد توصلت الدراسات السابقة إلى مجموعة من النتائج:

- أوضحت كافة الدراسات الأهمية العامة لحماية المعلومات الشخصية عبر المواقع الإلكترونية، واتفقت جميع الدراسات السابقة على تلك الأهمية.
- تناولت بعض الدراسات وجود أهمية لميزة المصادقة الثنائية في حماية المعلومات الشخصية ومنع اختراق البيانات وسرقتها.
- استفاد الباحثان من خلال الدراسات السابقة في الأهمية العامة والخاصة لميزة المصادقة الثنائية في حماية المعلومات الشخصية.

ومن هنا تميزت الدراسة الحالية عن الدراسات السابقة في تناولها جانب ميزة المصادقة الثنائية في حماية المعلومات.

الإطار النظري:

المحور الأول: الخصوصية والأمان

- **مفهوم خصوصية المعلومات**

تُعد الخصوصية من الحقوق الدستورية الأساسية الملازمة للشخص الطبيعي بصفته الإنسانية كأصل عام، حيث تُعد أساس بنيان كل مجتمع سليم، وتُعتبر من الحقوق السابقة على وجود الدولة ذاتها، ومفهوم الخصوصية بحد ذاته هو مفهوم ديناميكي أي إنه متغير، حيث إن الجوانب التي يرمي التعريف إلى حمايتها تتميز بحساسيتها المفرطة لتطور الوسائل والتكنولوجيا التي تقترب منها كما هو الحال الآن بالنسبة لشبكة الإنترنت ومواقع التواصل الاجتماعي على وجه الخصوص؛ فعلى سبيل المثال بعد أن كان مفهوم الخصوصية مرتبط بالمراسلات التقليدية الورقية فتطور للمراسلات عن طريق التلغراف، ثم تطور إلى المراسلات الإلكترونية، وعلى هذا الأساس الزمني نجد أن هنالك تفاوت في فهم المعنى الدقيق لمصطلح "الخصوصية"، ومن التعريفات المرتبطة بمفهوم الخصوصية ما انطلق من الظروف الفيزيائية للشخص على اعتبار أن الخصوصية هي الحالة التي يُترك فيها الفرد وشأنه، أي أن يحرم الآخرون من الاقتراب منه أو كل ما يعتبر حميمًا بالنسبة إليه.(Glenn, 2003)

ويعرّفها البعض على أنها "القدرة التي يتمتع بها الفرد للمحافظة على أموره الخاصة ويمنع إفشائها، ولهذا الحق العديد من المفاهيم المنفصلة لكنها ترتبط معًا في الوقت ذاته، والخصوصية إما مكانية تتعلق بالقواعد المنظمة لدخول الأماكن، أو تكنولوجية تتعلق بسرية المراسلات الهاتفية والبريد الإلكتروني وغيرها، أو جسدية أو مادية تتعلق بحماية الفرد ضد الاعتداءات الجسدية كفحوص الجينات والمخدرات، وإما معلوماتية تتعلق بأنظمة جمع وإدارات بيانات الفرد المستخدم كبطاقات الهوية والبطاقات المصرفية والسجلات الطبية وغيرها.(العرب، 2002)

ويمكن تعريف الخصوصية تقنيًا على أنها حق المستخدمين في الحفاظ على سرية البيانات المتعلقة بهويتهم أو سلوكهم أثناء استخدام الأنظمة بما لا يتعارض مع قدرة هذه الأنظمة على أداء وظائفها.(Heurix, et al., 2015)

وتعد البيانات الشخصية، كالاسم والعنوان ورقم الهوية؛ الأساس لحماية الخصوصية، وتتوسع هذه البيانات لتشمل أيضًا معلومات أكثر حساسية تتعلق بالأفكار والسلوك، والصحة، والمعتقدات.(Eckhoff & Wagner, 2017)

- **نشأة مفهوم خصوصية المعلومات**

ارتبطت نشأة مفهوم خصوصية المعلومات بالخوف الشديد من مخاطر التقنية ذاتها، ويمكن القول أن نهاية الستينات والسبعينات من القرن الماضي شهدت انطلاق الدراسات القانونية الأكاديمية التي عنيت بالخصوصية وبحقوق الإنسان في ضوء التطورات التقنية محدودة بشكل عام، وأن هذه الفترة تحديدًا هي التي أثير فيها لأول مرة وبشكل متزايد مفهوم خصوصية المعلومات كمفهوم مستقل عن بقية مفاهيم الخصوصية وتحديدًا التدخل المادي ومسائل الرقابة، ويُعزى الفضل في توجيه الانتباه لمفهوم خصوصية المعلومات في هذه الفترة إلى مؤلَّفين أمريكيين لهما أهمية كبيرة في هذا الحقل، الأول كتاب "الخصوصية والحرية" Freedom and Privacy لمؤلفه ويستن آلان Westin Alan، والثاني كتاب "الاعتداء على الخصوصية" The Assault on the Privacy لمؤلفه آرثر ميللر Arthur Miller، وكلاهما قدما مفهومًا وتعريفًا لخصوصية المعلومات وهناك إحجام من جانب المستخدمين من وضع بياناتهم عبر الإنترنت، كما يتردد المستهلكون فى الإدلاء ببياناتهم الشخصية على شبكة الإنترنت، ومع ذلك، فإن تدفق البيانات الشخصية للمستخدمين يمثل خطرًا على خصوصية هويتهم، حيث يمكن سرقة هوية الشخص من خلال استخدام البيانات الخاصة بالبطاقات المصرفية، ويظهر سوء استخدام البيانات المصرفية أو سرقة الهوية في الهدف منه كالتشهير بسمعة الشخص أو تدمير مستقبله المهني بعد نشر المعلومات على الإنترنت، وتعتبر هذه المشكلات التي يواجهها كثير من الناس بشكل متزايد.(Wozny, 2017)

- **طرق اختراق الخصوصية عبر وسائل التواصل**

أولاً: التصيد الاحتيالي

ويُعد التصيد الاحتيالي من أكثر الطرق انتشاراً، وهو مجموعة من التقنيات التي يستخدمها المخترقين (قراصنة الإنترنت) Hackers من أجل جمع المعلومات الشخصية عن مستخدمي الإنترنت لقرصنة حساب الفيسبوك على سبيل المثال؛ بحيث يقوم قراصنة التصيد بإنشاء صفحة تسجيل وهمية أو إنشاء استنساخ من صفحة تسجيل الدخول الخاصة بالمستخدم بحيث يبدو من خلال المظهر الخارجي لها أنها تمثّل صفحة فيسبوك الحقيقية، كما أن التصيد يستخدم الرسائل الخاصة بالبريد الإلكتروني من أجل الحصول على الأموال بطرق احتيالية، وكذلك جمع المعلومات السرية التي ينقل معظمها من رسائل البريد الإلكتروني، كما يهدف الاعتداء أيضًا إلى سرقة المعلومات السرية كالاسم والعنوان وكلمة السر ورقم الهوية أو المعلومات المصرفية من خلال قيام القراصنة باستخدام مواقع الويب الزائفة ورسائل البريد الإلكتروني الخاصة بالهيئات الحكومية أو مواقع مصارف أو بنوك أو علامات تجارية كبرى لإقناع المستخدم بالكشف عن تفاصيل بطاقات الائتمان الخاصة به أو عن أي بيانات أو معلومات شخصية يمكن استخدامها في الوصول إلى حسابات مصرفية أو غير ذلك من الإجراءات التي تحتاج إلى إثبات هوية المستخدم.(عثمان، 2017)

ثانياً: البرامج الضارة المثبتة على جهاز الحاسب الآلي

ويشير ذلك إلى البرامج العدائية أو المتطفلة أو المزعجة التي تتسلل مستترة إلى أجهزة الحاسب الآلي؛ وتسميتها بالبرامج الضارة يرجع إلى أنها ناشئة عن كلمة Malicious ،التي تعني "خبيث"، وكلمة Software تعني برنامج، وتثبت هذه البرامج الخبيثة بدون علم المستخدم الضحية من أجل جمع المعلومات الأكثر خصوصية، وكذلك الحصول على الدخول غير المرخص للأنظمة المعلوماتية، وهناك عدة أنواع من البرامج الضارة؛ ويعتبر أخطرها هو keylogger الذي يرصد لوحة المفاتيح الخاصة بالمستخدم دون علمه، حيث تعمل على تخزين كلمات المرور والرسائل الخاصة وكذلك المعلومات الأكثر خصوصية للمستخدم، ثم تقوم بإرسالها إلى الهاكر أو المحتال من أجل تحليلها واستخلاص المعلومات ذات الأهمية للمستخدم.(المؤيد، 2009)

ثالثاً: سرقة هوية المستخدم

ويقصد بها قيام شخص بسرقة هوية شخص آخر والتظاهر أمام الناس بأنه الشخص نفسه من أجل الحصول على أمواله أو القيام بكافة المعاملات باسمه، ويمكن أن يكون ذلك من أجل تحقيق أغراض مختلفة، مثل طلب قرض أو شراء السلع أو البضائع نيابة عنه، أو الاستفادة من الخدمات التي يتمتع بها الشخص الضحية، مثل خدمات التأمين الصحي عن طريق تقديم المستندات الخاصة، مثل جواز السفر أو بطاقة التأمين الصحي.(فهمي، 2017)

رابعاً: استخدام البيانات الشخصية الخاصة بقبول مستخدم جديد على مواقع التواصل الاجتماعيَ

ويقصد بها رصد بيانات المستخدم عند التسجيل كمستخدم جديد للمواقع الإلكترونية كالفيسبوك، ومن أبرز مخاطر هذه الطريقة في سرقة البيانات اختراق الحساب، وتوزيع الصور المحرجة، وصعوبة إزالة أو إلغاء الحساب... وغيرها، وهو ما يؤثر بشدة على سمعة المستخدم الرقمية، حتى إن الأمر يصل إلى أن يظن الآخرين أن المستخدم نفسه هو من يقوم بنشر المعلومات والصور الخاصة به ويشارك الروابط عبر الشبكات الاجتماعية، حيث مكان النشر يمثّل ملفه الشخصي الرقمي.(مصطفى، 2013)

ويمكن أن يتم خرق الخصوصية على شبكة الإنترنت من قبل جهات ثلاث أساسية، هي:

- مزدو خدمة الإنترنت Provider Service Internet.
- المواقع التي يزورها المتصفح.
- مخترقو الشبكة أو الأجهزة الأمنية والاستخباراتية.

حيث يمكن لمزود الخدمة أن يرصد كل ما تقوم به على الإنترنت (مكان وزمان الدخول إلى الشبكة، والمواقع التي تم الولوج إليها والرسائل المتبادلة... وغيرها)، وذلك من خلال، الكلمات التي جرى البحث عنها، الحوارات، الرسائل الإلكترونية خلال رقم الإنترنت الخاص بالمستخدم Protocol Internet، ووسائل وأدوات أخرى تعرف بال"Proxy" و"Packet"

و"Sniffer"، وهي برمجيات قادرة على تحليل كل حركة تجري على الشبكة الإلكترونية، بالإضافة إلى ما تتضمنه ثغرات المنتديات ومواقع التواصل الاجتماعي، حيث يمكن لمواقع إلكترونية كالفيسبوك رصد تحركات المستخدم ومحادثاته والأماكن التي يزورها بالتاريخ والساعة؛ حيث يترك المستخدم آثار ودلالات كثيرة تتصل به في شكل سجلات رقمية حول الموقع الذي زاره والوقت الذي قضاه على الشبكة والأمور التي بحث عنها، بما يمكّن المتطفلين من الاطلاع على أدق التفاصيل الشخصية للمشتركين فيها؛ لذا تمثّل مهمة ابتكار سبل لحماية الخصوصية تحدٍ كبير للأفراد والشركات والمواقع الإلكترونية.(المؤيد، 2009)

- **الخصائص التقنية للخصوصية**

بغض النظر عن تصنيف البيانات وأنواعها، فإن العديد من الدراسات العلمية والقانونية قد حددت بعض الخصائص أو الأهداف المرجوة من التقنيات التي تتعامل مع البيانات، حيث تشير دراسة (Heurix, 2015) إلى بعض تلك الخصائص أو الأهداف على النحو التالي:

- إخفاء الهوية أو التعمية عليها بحيث لا يمكن تحديد هوية فرد من ضمن بيانات لمجموعة من الأشخاص.
- عدم القدرة على الربط، بحيث لا يمكن لمن يمتلك البيانات أن يربط بين حدثين قام بهما نفس المستخدم، كما لا يمكنه ربط أي حدث بالمستخدم.
- استخدام الأسماء المستعارة، وهي من أكثر خصائص الخصوصية انتشارًا، ولا يُقصد بالاسم المستعار هنا الكنية، بل هي الاستعاضة عن استخدام بيانات تعريفية كرقم الهوية لتخزين ملفات المستخدمين واستبدالها برموز أو أرقام عشوائية، الأمر الذي يسمح للنظام بالتعرّف على المستخدم دون الكشف عن هويته.
- السرية، بحيث يُمنع وصول أي طرف غير مخوّل له إلى المعلومات الخاصة بالأفراد، وغالبًا ما تُصنَّف السرية من أساسيات أمن المعلومات وليس خصوصيتها، إلا إنها متطلب أساسي لحماية الخصوصية.

- **نماذج تقنيات تعزيز الخصوصية**

تهدف تقنيات تعزيز الخصوصية إلى تحقيق أحد الخصائص المذكورة السابقة على الأقل باستخدام مزيج من الوسائل التقنية أو المنهجية، وقد شهدت هذه التقنيات قفزة في السنوات الأخيرة تمثّلت في ظهور العديد من البرامج التي تركّز على حماية خصوصية الأفراد، مثل متصفّحات Tor وBrave، والتي اعتمدت على أساسيات أشارت إليها جريدة (The Guardian, 2014) الإلكترونية على النحو التالي:

أولاً: التوجه لاعتماد الخصوصية كمتطلب أثناء تصميم البرمجيات

حيث بهذا تُبنى الأنظمة لتحمي خصوصية المستخدم لا أن يستخدمها فقط دون حماية، وتستند هذه المنهجية على الالتزام بمبدأ اعتماد الحد الأدنى من البيانات الشخصية التي يجمعها ويحتاجها النظام، والشفافية من ناحية إبلاغ المستخدم بشكل واضح عن مبررات الحاجة إلى هذه البيانات، وكيفية استخدامها حصرياً، وتتعزز هذه المبادئ بوجود قوانين حماية بيانات

عصرية، مثل القانون الأوروبي لحماية البيانات (GRPR) الذي أجبر WhatsApp مثلاً على استثناء الأوروبيين من التحديث المثير للجدل لتعارضه الواضح مع القانون (GRPR).

ثانياً: تقنيات التشفير

حيث تستخدم تقنية التشفير لتحويل البيانات إلى نصوص غير مفهومة باستخدام أساسيات رياضية للبيانات، عندها تصبح القدرة على استعادة البيانات معدومة للأطراف التي لا تمتلك مفاتيح التشفير، وقد طورت بعض خوارزميات التشفير، مثل خوارزمية التشفير المتشاكل Homomorphic Encryption لتتيح إمكانية إجراء عمليات معالجة أو حسابية على النصوص المشفرة مع الإبقاء على سريتها دون الحاجة إلى فكّ تشفيرها، وعليه تستطيع الجهات التي تجمع البيانات الشخصية أن توفر خدماتها دون الحاجة إلى كشف البيانات –فك تشفيرها–، كما تستطيع أن تشارك هذه البيانات مع جهات أخرى غير مؤتمنة لتوفير خدماتها؛ فمثلاً تستطيع شركة الهاتف أن تخزّن نسخ مشفرة من بيانات الاتصالات الهاتفية لمستخدميها وأن تحتسب لاحقًا قيمة فواتير المستخدمين دون الاطلاع على بيانات هذه الاتصالات.

ثالثاً: تقنيات إخفاء البيانات التعريفية

وتستند هذه التقنيات إلى التعمية عن البيانات الدالة على هويات الأفراد من مجموع البيانات، وتستعمل هذه الأساليب عند نشر بيانات التقارير الإحصائية، كالتقرير اليومي عن حالات Covid-19 مثلاً، ومن أمثلة هذه الأساليب تقنية الخصوصية التفاضلية التي تستند إلى فكرة تلويث البيانات بإضافة بيانات مزيفة لأفراد غير حقيقيين مع الحفاظ على صحة المعلومات الإحصائية كمعدل أعمار المصابين بفيروس Covid-19 مثلاً، بمعنى أن تتبُّع الحالات الفردية غير ممكن لأن البيانات ملوثة ولكن الاتجاهات الإحصائية العامة للبيانات صحيحة.

المحور الثاني: المصادقة الثنائية

- **مفهوم المصادقة الثنائية**

هي عملية أمنية يتم فيها مطالبة المستخدم إثبات نفسه من خلال طريقتين مختلفتين، وذلك للتأكيد على أن الشخص نفسه هو صاحب الحساب الحقيقي.(Cohen, 1995)

وتتضمن المصادقة الثنائية الحماية القصوى لحسابات المستخدمين من هجمات المخترقين، حيث يستحيل على المخترق الحصول على هاتين الطريقتين معًا لإثبات أنه هو صاحب الحساب الفعلي، وبالتأكيد تقوم المصادقة الثنائية بحماية المستخدم بشكل أكبر بكثير من المصادقة الأحادية، حيث عادةً ما تتطلب المصادقة الأحادية إدخال كلمة السر فقط، أما المصادقة الثنائية فتطلب أكثر من كلمة السر لحساب المستخدم، فبعد القيام بإدخال معلومات تسجيل الدخول يطلب النظام من

المستخدم إدخال إثبات آخر يدل على أنه صاحب الحساب؛ فقد يُطلب منه إدخال بصمة إصبعه عن طريق الهاتف الذكي أو إدخال رقم سري إضافي يتم إرساله إلى رقم الهاتف المقترن بالحساب.(Savarese & Hart, 1999)

- **فوائد المصادقة الثنائية**

تُعد الفائدة الأهم المطلوب من المصادقة الثنائية تحقيقها هي إضافة طبقة حماية أمنية ذات فعالية عالية لحماية حساب المستخدم؛ فكلمة السر لم تعد هي الأمر الوحيد الذي يمكنه حماية حسابه، ومع ازدياد أعداد المخترقين وتسريب البيانات والاحتيال الإلكتروني، كان لابد من التوجّه نحو مسار مختلف في الحماية الأمنية؛ ففي عام 2018، تم سرقة معلومات الدخول لأكثر من 50 مليون مستخدم في الولايات المتحدة الأمريكية في حادثة الأضخم من نوعها دفعت القائمين على موقع الفيسبوك لإزالة أكثر من 90 مليون ملف تعريفي محفوظ بقاعدة بياناته وفق ما أشار إليه (Isaac & Frankel, 2018) لذا لم تعد كلمة السر أمرًا كافيًا لتأمين حسابات المستخدمين.

ويشير (Wilkins, 2021) إلى حادثة اختراق هي الأضخم حتى الآن، حيث في عام 2020 تم تسريب ما يزيد عن 16 مليار معلومة على شبكة الإنترنت ما بين بريد إلكتروني وكلمات مرور سرية وأرقام حسابات... وغيرها من المعلومات.

ماذا تستفيد الشركات من تفعيل المصادقة الثنائية لمستخدميها؟

لا تستطيع الشركات تأمين الحماية الكافية لمستخدميها عن طريق اعتماد كلمة السر وحدها، كما أن هذا الأمر قد يؤدي إلى تخفيف تكاليف أقسام الحماية وتكنولوجيا المعلومات لدى الشركات؛ ويشير موقع Oath.org الإلكتروني إلى واحدة من الإحصائيات، حيث تشير إلى أن ما يقارب 30٪ من تواصل المستخدمين مع قسم تكنولوجيا المعلومات لديها يتعلق بموضوع تغيير كلمة السر، ولكن مع استخدام المصادقة الثنائية من قِبل الشركات ستزداد قوة الحماية الأمنية لمستخدميها، بما سيقلل من مشكلات سرقة وتسريب كلمات المرور لدى المستخدمين.

- **اختراق المصادقة الثنائية**

على الرغم من إمكانية اختراق عامل المصادقة الثنائية، إلا إن نسبة حدوث هذا الأمر ضئيلة جدًا؛ لذا يعتبر استخدام عامل المصادقة الثنائية من أفضل أنواع الحماية للحسابات الإلكترونية، ومن الطرق التي يمكن اختراق المصادقة الثنائية من خلالها الرسائل النصية، حيث إن كلمة السر الإضافية الصالحة لمرة واحدة يتم إرسالها عبر رسالة نصية إلى رقم الهاتف للمستخدم لذا سيحتاج المخترق إلى اختراق شركة الهاتف التي يتعامل معها المستخدم الضحية والقيام بتحويل الرسائل التي يتم إرسالها إلى رقم هاتف المستخدم إلى هاتفه –المخترق–، أو عن طريق انتحال شخصية المستخدم واستخراج شريحة اتصال جديدة تحمل رقم الهاتف نفسه، ولكن هذا الأمر ليس بتلك السهولة، فشركات الاتصالات تمتلك أنظمة حماية أمنية متطورة لا يمكن تجاوزها بسهولة وفق ما أشار إليه موقع Oath.org الإلكتروني.

- **وسائل المصادقة الثنائية**

مع انتشار استخدام المصادقة الثنائية بشكل كبير ما بين المستخدمين في الوقت الحالي، بدأت الشركات في توسيع مدى الخيارات التي يمكن استعمالها كطرق لتفعيل المصادقة الثنائية، ويشير موقع Oath.org الإلكتروني إلى أكثر هذه الطرق شيوعاً على النحو التالي:

- **المكالمة الصوتية والرسالة النصية** SMS

عند التسجيل في موقع إلكتروني ما، قد يطلب الموقع من المستخدم رقم الهاتف لتخزينه ضمن معلومات الحساب لاحقًا، وعند تسجيل الدخول إلى حساب المستخدم يقوم الموقع بإرسال رسالة نصية تحتوي على كلمة السر صالحة لمرة واحدة، أو ترد مكالمة مسجلة مسبقًا يتم إخبار المستخدم من خلالها بكلمة السر الصالحة لمرة واحدة؛ فهي طريقة سهلة الاستخدام ولا تتطلب وجود برامج خاصة، ورغم إنها لا تعتبر من أقوى الطرق، إلا إن القليل من الشيء خير من لا شيء، ولكن من سلبيات هذا النوع أن العديد من المستخدمين لا يحبّذون فكرة إعطاء أرقام هواتفهم للمواقع الإلكترونية، حيث تقوم بعض المواقع باستغلال أرقام هواتف مستخدميها لأغراض إعلانية، وقد يعتبر هذا الأمر مزعجًا للعديد من المستخدمين، ومن المشكلات الأخرى التي تواجهها هذه الطريقة هي حاجتها إلى توافر شبكة الهاتف المحمول، فبعض الأشخاص يقومون بالسفر بشكل متكرر وقد لا تعمل شبكة هاتفهم في بعض الدول؛ ففي هذه الحالة يمكن اللجوء إلى تطبيقات المصادقة الثنائية التي تحتاج إلى الاتصال بشبكة الإنترنت، حيث إن الوصول إلى شبكة واي فاي يعتبر أمرًا شديد السهولة في أيامنا هذه.

- **الإشعارات**

فعند قيام المستخدم بتسجيل الدخول إلى حسابه من جهاز جديد، يجد إشعارًا على شاشة الهاتف يطلب منه الموافقة على عملية تسجيل الدخول، مع بيانات الموقع للجهاز الذي يرغب بتسجيل الدخول من خلاله، ويمكن استخدام هذه الطريقة مع العديد من المواقع والأجهزة، حيث يتم إرسال إشعار إلى جهاز الهاتف المحمول المقترن بالحساب يطلب السماح للجهاز الجديد بتسجيل الدخول، وقد يحتوي هذا الإشعار على كلمة مرور صالحة لمرة واحدة بدلاً من إرسالها كرسالة نصية، وما يميز هذه الطريقة هو إظهارها للموقع التقريبي للجهاز الذي يحاول تسجيل الدخول إلى حساب المستخدم.

- **تطبيقات الطرف الثالث**

تتطلب هذه الطريقة تنزيل برنامج أو تطبيق يقوم بعملية المصادقة الثنائية على جهاز المستخدم، ومن خلال هذا البرنامج يمكن الحصول على كلمة سر صالحة لمرة واحدة؛ فعند القيام بتسجيل الدخول إلى موقع معين ـ في حال كان متوافقاً مع البرنامج الذي قام المستخدم بتحميله ـ وبعد إدخال اسم المستخدم وكلمة المرور، يقوم الموقع بالاتصال تلقائياً مع البرنامج ويطلب منه إصدار كلمة سر صالحة لمرة واحدة ليدخلها المستخدم إلى الموقع.

ومن أشهر برامج المصادقة المنتشرة بكثرة من بين المستخدمين Google Authenticaton و Microsoft Authenticator.

- **المصادقة البيولوجية**

مع انتشار الأجهزة الذكية التي تحتوي على مستشعر للبصمة أو مستشعر للوجه، بدأ التوجّه نحو استخدام هذا النوع من المصادقة؛ حيث عند محاولة المستخدم تسجيل الدخول إلى حسابه الإلكتروني، يظهر له على شاشة الجهاز إشعار يطلب منه مسح بصمة الإصبع أو بصمة الوجه للتأكد من أنه صاحب الحساب، وفي هذه الحالة سيكون المستخدم نفسه هو أداة التحقق؛ فهو يحل محل كلمة السر الواحدة باستخدام بصمة إصبعه أو وجهه، ما يجعل هذا الأمر من المصادقة البيولوجية أكثر الأنواع أمانًا، حيث يستحيل تقريبًا تزوير بصمات شخص معين، خصوصًا مع الحاجة لإدخال البصمة إلى جهاز المستخدم نفسه الذي يكون في حوزته.

- **أشهر التطبيقات المستخدمة لخاصية المصادقة الثنائية**

يشير (Elliott, 2017) إلى أن من أشهر التطبيقات والمواقع المستخدمة لخاصية المصادقة الثنائية، ما يلي:

- تطبيق LastPass Authenticator، وهو يدعم بروتوكول TOPT؛ مما يميزه عن باقي التطبيقات، ولكنه لا يعمل منفردًا ويفضل أن يعمل مع تطبيق أو بروتوكول Google Authenticator، كما يدعم إدارة كلمات المرور، ويوفر توليد رموز أو أكواد للمصادقة الثنائية بشكل تلقائي، ويدعم إرسال رسائل قصيرة.

- تطبيق Google Authenticator، يعد من أشهر التطبيقات وأسهلها في الاستخدام، وهو مقدم من شركة جوجل ويدعم حماية جميع الحسابات بالمصادقة الثنائية، بالإضافة لسرعته فهو ينتج كل 15 ثانية 8 أرقام لحماية الحساب؛ مما يصعّب عملية السرقة.

- تطبيق Microsoft Authenticator، يعد أكبر منافس لتطبيق Google Authenticator، وهو مقدم من شركة مايكروسوفت، ويعمل على حماية الحسابات عن طريق المصادقة الثنائية، يتميز بسهولة الاستخدام والبساطة في التعامل بجانب أنه ينتج أكواد بشكل تلقائي لحماية الحسابات بشكل أكبر.

- تطبيق Authy، أحد أكثر التطبيقات شهرة وموثوقية بين المستخدمين، يعمل على توليد الرموز لحماية الحسابات بشكل تلقائي ولا يحتاج لعمله وجود اتصال بالإنترنت، وهو يدعم الكثير من المواقع، كما يعمل بدون إعلانات، ويدعم حماية عمليات الشراء بشكل كامل، وهو مجاني تمامًا مثل باقي تطبيقات المصادقة الثنائية.

المحور الثالث: حماية المعلومات الشخصية

- **مفهوم حماية المعلومات**

يشير (صالح وآخرون، 2020) إلى مفهوم حماية المعلومات كما عرّفته لجنة أنظمة الأمن القومي الأمريكية Committee on National Security System، وهو جمع وتخزين المعلومات وعناصرها المهمة ومنع الوصول إليها بما يضر صاحبها بما في ذلك الأنظمة والأجهزة التي تستخدم هذه المعلومات وتخزنها وترسلها.

ويمكن تعريف حماية المعلومات بأنها مجموعة من الوسائل والأدوات والإجراءات المطلوب توفيرها لضمان الحفاظ على المعلومات من الأخطار الداخلية والخارجية، ومن شأنها حماية سرية وسلامة وخصوصية محتوى المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال أنظمتها لارتكاب الجرائم الإلكترونية.(Doherty & Fulford, 2005)

ونتيجة لانتشار وسائل وأدوات الاختراق والقرصنة على شبكة الإنترنت تنامى أهمية حفظ المعلومات وحمايتها من المخاطر المتعددة من جهات أخرى، وقد حدد خبراء الحماية والتشفير عدة عناصر مهمة ينبغي أن تتصف بها الأنظمة الحاسوبية لكي يمكن وصفها بالآمنة، وقد لخّص (Gordon & Loeb, 2006) تلك العناصر في العناصر الثلاثة التالية مشكّلة بمجموعها مثلثًا أُطلق عليه مثلث CIA للحماية.

- الموثوقية Confidentiality: ويقصد بهذا العنصر أن تكون المعلومة محمية من الوصول والقراءة غير المشروعة.
- النزاهة والتكاملية Integrity: حيث يجب أن تكون المعلومة صحيحة غير مغلوطة؛ مما يعني أنه يجب حمايتها ليس فقط من محاولة الوصول غير المشروع؛ بل يجب حمايتها أيضًا من التعديل والتغيير في محتواها.
- التوافرية Availability: أي أن تكون المعلومة متوفرة حينما يريد المستخدم أن يصل إليها، وأن لا تُحجب عنه عند حاجته لها.

- **أهداف برامج حماية المعلومات**

هناك عدة أهداف رئيسة وفرعية لبرامج حماية المعلومات، وتتمثّل جميعها فيما حدده (Abu-Musa, 2010) مما يلي:

- إتاحة المعلومات (القدرة على الوصول) Information of Availability: وتعني إتاحة المعلومات التأكد من استمرار عمل نظام المعلومات، واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمستخدمها وتوافرها عند الحاجة إليها، والتأكد من أن مستخدمي تلك المعلومات لن يتعرضوا إلى منع استخدامهم لها بطريقة غير مشروعة.

- سرية المعلومات (خصوصية المعلومات) Confidentially: وتعني إخفاء المعلومات أو الموارد، أي حماية المعلومات من اطلاع أي شخص غير مخوّل له بالاطلاع عليها.

- تكاملية المعلومات (سلامة المحتوى) Information of Integrity، وتعني ضمان سلامة محتوى المعلومات وضمان عدم تغييرها أو تدميرها من قبل جهات غير مخوّلة لذلك.

- **عناصر حماية المعلومات**

يشير (Maarop, et al., 2015) إلى عناصر حماية المعلومات ملخّصةً فيما يلي:

- المحافظة على صحة المعلومات الموجودة والتأكد من عدم العبث بها أو تعديلها أو تغييرها في أي مرحلة من مراحل حمايتها.
- حسن المراقبة، حيث تتوفر القدرة على معرفة هوية كل شخص وصل إلى المعلومات والتعديلات التي أجريت عليها.
- السرية، وتعني عدم السماح للأشخاص الذين لا يحق لهم الاطلاع على المعلومات بالوصول إليها.
- إدامة عمل الخدمة، فمن عناصر حماية المعلومات المحافظة على صلاحية المعلومات لضمان استمرار الخدمة المتوفرة من خلالها، واستمرارية القدرة على الوصول إليها لمن يخوَّل له ذلك.

- **متطلبات حماية المعلومات**

تتعرض نظم المعلومات الإلكترونية للكثير من المخاطر والتهديدات، منها التلاعب في البيانات بقصد تدميرها سواء بالحذف أو بالدمج غير الصحيح لبعضها، أو بخلطها ببيانات أخرى غير حقيقية، أو تبويبها بشكل خاطئ لتفقد معه مدلولها ومعناها وقد يحدث التلاعب في البيانات بشكل يجعلها لا تعبر عن الحقائق التي نتجت عنها أصلاً، كما أن هذا التلاعب يحدث في مراحل مختلفة من النظام حيث المدخلات أو التخزين أو المخرجات، ومن الممكن أن تكون تلك التهديدات في شكل سرقة وقت أجهزة الحاسب واستخدامها في الأغراض الشخصية والدخول غير المصرح به للنظم والشبكات، وتخريب وتدمير بعض الملفات، وفشل النظام وسقوط شبكة الاتصال، ومنع الأشخاص المخول لهم بالدخول إلى النظام، والإظهار غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها وتوزيعها بواسطة أشخاص غير مصرح لهم بذلك، وكذلك مقاطعة تحويل البيانات من أماكن بعيدة.

- **إدارة حماية المعلومات**

هي نهج أمني مستمر ومنظم لإدارة حماية معلومات المنظمة من التعرض للخطر من قبل الأطراف غير المسؤولة، ولضمان بقاء المعلومات آمنة، حيث تواجه عملية حماية المعلومات العديد من المشكلات سواء على الأجل البعيد أو الأجل القريب؛ لذا يجب على الإدارة وضع خطة طويلة الأجل لمنع حدوث أي تهديد للمعلومات وتخفيض آثارها السلبية على المنظمة إلى أدنى حد ممكن في حالة حدوثها، كما يجب عليها تحديد نوع القضايا الهامة التي تواجه حماية المعلومات، وأن تدرسها بعناية وتتفهم طبيعة المشكلات المتعلقة بكل قضية حتى تستطيع تجنبها في المستقبل وتقديم حلول مناسبة لها.(Allen & Westby, 2007)

- **سياسة حماية المعلومات**

سياسة حماية المعلومات هي مزيج من المبادئ والأنظمة والمنهجيات والتقنيات والأدوات التي أنشئت لحماية المنظمة من التهديدات، وهي وثيقة استراتيجية بمعنى أنها تنشأ قبل القيام بأي نشاط من أنشطة حماية المعلومات؛ فهي تتكون من الأهداف والاتجاهات والقواعد التي يجب وضعها واتباعها من قبل الموظفين والأطراف الأخرى التي تتعامل مع المنظمة؛ لذا يجب أن تكون هذه السياسة واضحة في تحديد الأهداف والأدوار ومسؤوليات الموظفين والأطراف الأخرى ذوي المصلحة، كما يجب أن تكون شاملة لجميع جوانب متطلبات وضوابط حماية المعلومات، وأن تكون متناسقة مع سياسة المنظمة ورؤيتها، وتمثّل سياسة حماية المعلومات حجر الزاوية في إدارة حماية المعلومات الجيدة.

كما أن هذه السياسة ليست ثابتة، أي يجب أن يتم مراجعتها بانتظام على الأقل مرة في السنة للتأكد من أنها ذات صلة باحتياجات الوقت الحاضر، ويتم إرسالها إلى كامل الموظفين والأطراف الأخرى ذوي المصلحة مع مراعاة أنه عند قيام المنظمة بإحلال أساليب أمن تكنولوجية حديثة بدلاً من أساليب الأمن التقليدية يجب المفاضلة من حيث درجة الاستفادة ونجاح برامج حماية المعلومات بين البقاء على الأساليب التقليدية لحماية المعلومات والمستحدثات التكنولوجية.(Zammani & Razali, 2016)

- **المبادئ العامة لحماية المعلومات**

رغم تعدد المبادئ العامة لحماية المعلومات الشخصية باختلاف الجهات الصادرة عنها، فإن مبادئ ثلاثة يمكن اعتبارها أسسًا عامة للنظام القانوني لحماية المعلومات الشخصية، وقد أشار (Evans, 2011) إلى تلك المبادئ على النحو التالي:

- وجوب الرقابة على عمليات تخزين البيانات وتحليلها، وإعمال مبدأ المسؤولية والعقوبة لكل من يسيء استخدام البيانات الشخصية.
- جواز تحليل البيانات شريطة أن يكون ذلك لسبب مشروع وعادل، وبطريقة تحفظ حقوق أصحاب تلك البيانات.
- وجوب حماية البيانات الشخصية من خلال جمعها وحفظها بطريقة آمنة، والالتزام بعدم نقلها إلا بعد التأكد من أمان طريقة النقل، وأنها ستكون آمنة لدى الجهة المنقول إليها.

وبالرغم من وحدة المبادئ الأساسية لحماية البيانات الشخصية، فإن تطبيقاتها قد تختلف من بلد إلى آخر؛ حيث قد لا يتم تطبيقها في بعض البلدان على جميع القطاعات، وفي بلدان أخرى يستثنى القطاع العام من نطاق تطبيق قوانين حماية المعلومات.

- **حقوق أصحاب البيانات**

إن حفظ حقوق الأفراد وتمكينهم من السيطرة نسبيًا على معلوماتهم الشخصية من الأهداف الأساسية لقوانين حماية البيانات بحيث لا تستخدم إلا في ما هو مفيد، ولتحقيق هذا الهدف حرص قانون حماية البيانات البريطاني لسنة 1998 على أخذ

رأي صاحب البيانات في مختلف المراحل بدءًا من جمع البيانات وانتهاءً بالتخلص منها، ومن ثَمَّ أقر له بعض الحقوق جاءت في حكم محكمة الاستئناف البريطانية في قضية ديورانت أمام هيئة الخدمات المالية، وتلك الحقوق هي:

- الحق في التعويض في حالة عدم الامتثال لمتطلبات محددة، وهذا الحق يعطي صاحب البيانات الحق في طلب التعويض عن الضرر الناتج عن مخالفة حافظ البيانات لمقتضيات هذا القانون.
- الحق في منع معالجة البيانات إذا كانت معالجتها تلحق به أو بغيره ضررًا ماديًا أو معنويًا.
- الحق في تصحيح البيانات الخاطئة، وبمقتضى هذا الحق، يمكن لصاحب البيانات أن يصحح البيانات الخاطئة أو حتى يمحيها مع كل ما يتعلق بها.
- الحقوق المتعلقة باتخاذ القرار آليًا، وبموجب هذه الحقوق يملك صاحب البيانات الحق في أن يطلب من معالج البيانات أن لا يتخذ قرارًا يؤثر عليه اعتمادًا فقط على البيانات المعالجة إلكترونيًا، وذلك مثل تقييم فاعليته في العمل أو ثقته أو سلوكه.
- الحق في الوصول إلى البيانات، وبمقتضى هذا الحق يلزم من يعالج البيانات الشخصية أن يخبر صاحب البيانات بالغرض من معالجة البيانات والجهات التي يمكن أن تطلع عليها، وهذا يمكن المستخدم أيضًا من الاطلاع على كل البيانات المسجلة حوله ومصادرها.
- الحق في منع استخدام البيانات الشخصية لأهل التسويق المباشر، مثل الإعلانات.

- **معايير حماية المعلومات**

المعايير التي ينبغي على المنظمة اتباعها من أجل تنفيذ سياسة حماية فعالة للمعلومات كما يرى (Whitman & Mattord, 2017)، هي:

- أن تكون سياسة حماية المعلومات واضحة ومفهومة من قبل جميع الأطراف المعنية، وأن يتم متابعة هذه السياسة بانتظام لمعرفة ما إذا كان يتم انتهاكها.
- وجود مبادئ توجيهية إجرائية محددة بشكل جيد للتعامل مع حوادث انتهاك السياسة.
- أن تكون ملائمة للثقافة التنظيمية، وملائمة للنمط الذي يتسق مع أسلوب الاتصال العام في المنظمة.
- استخدام لغة بسيطة لضمان سهولة فهمها، وتحديد الغرض من السياسة ونطاق المنظمة وشرح النشاط المقبول وغير المقبول.
- ينبغي وضع سياسة أمن المعلومات على أساس الاحتياجات الأمنية والأهداف التجارية للمنظمة.

- **حماية المعلومات في الوطن العربي**

تقدّر خسائر منطقة الشرق الأوسط جرّاء الجرائم الإلكترونية المتعددة المنتشرة بأكثر من مليار دولار، وتُعد منطقة الخليج العربي الأكثر تعرضًا للهجمات في الشرق الأوسط، حيث احتلت المملكة العربية السعودية في نهاية عام 2017 المرتبة الثالثة عالميًا في التعرض للهجمات الإلكترونية في جميع مرافقها الحكومية والخاصة من جهات خارجية، حيث وصل عدد الهجمات إلى 54 ألف هجمة سنويًا، وتواجه قطاعات الخدمات المالية، والرعاية الصحية، والنفط والغاز معظم التهديدات الإلكترونية،

وفي هذا السياق، وكان متوقعاً أن يبلغ حجم الإنفاق العربي على حماية المعلومات نحو 9.2 مليار دولار عام 2018 نتيجة ازدياد مستوى التهديدات الإلكترونية بنسبة 25% بحسب مشاركون في فعاليات مؤتمر التكنولوجيا والابتكار والمجتمع "سايفاي أفريقيا 2018"، في حين يعتبر القطاع المصرفي من أبرز القطاعات المستهدفة. وبالتالي، تبرز أهمية تبنّي استراتيجية لاحتواء مخاطر التهديدات الإلكترونية ورفع مستوى الجاهزية لمواجهتها عبر تطوير البنية التحتية لقطاع التكنولوجيا وتعزيز مستويات الإنفاق على حماية المعلومات في الدول العربية.

وتوقعت مؤسسة جارتنر أن يصل إنفاق منطقة الشرق الأوسط وشمال إفريقيا على تكنولوجيا المعلومات ككل إلى 155 مليار دولار خلال عام 2018، بزيادة قدرها 3.4% عن عام 2017. وفي عام 2018 فإن القطاع الرئيسي الذي سيعزز من نمو الإنفاق على تكنولوجيا المعلومات في المنطقة هو قطاع البنوك والأوراق المالية الذي سينمو إنفاقه بنسبة 3.6%، ويعود إنفاق المصارف المتزايد على تكنولوجيا المعلومات إلى التوجهات المتزايدة نحو الرقمنة والاستثمارات في التقنيات المتقدمة مثل التحليلات، والبلوك تشين، والذكاء الاصطناعي، والتكنولوجيا المالية بشكل عام، وذلك وفق ما أشار إليه اتحاد المصارف العربية (2018).

- **مبادئ وتشريعات حماية المعلومات الشخصية**

أولاً: التشريعات الدولية لحماية المعلومات الشخصية

تغلغلت تكنولوجيا المعلومات كافة المجالات الحياتية ومنها المالية والمصرفية، كما ظهرت البنوك والحكومات الإلكترونية وانتشرت التجارة الإلكترونية والتعليم الإلكتروني ووسائل التواصل الاجتماعي، وفي مقابل تزايد استخدام تكنولوجيا المعلومات وشبكات المعلومات ارتفع مستوى ارتكاب الجرائم، وانتشرت برامج التجسس والقرصنة وتضررت الكثير من القطاعات خاصة القطاع المصرفي؛ وبالتالي، أصبح من الضروري وضع تشريعات قانونية متعلقة بالجرائم الإلكترونية، حيث وضع أول نص قانوني يتعلق بجرائم الحاسب الآلي عام 1978 –قانون ولاية فلوريدا–، وتنص المادة الثانية عشرة من الإعلان العالمي لحقوق الإنسان على ألا يتعرض أحد لتدخّل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته...، ولكل شخص الحق في حماية القانون من مثل هذا التدخل... أما المادة التاسعة عشرة من الإعلان نفسه فتنص على أن لكل شخص الحق في حرية الرأي والتعبير، ويشمل هذا الحق حرية اعتناق الآراء دون أي تدخل والحصول على المعلومات والأفكار وتلقيها وإذاعتها بأي وسيلة كانت دون تقيد بالحدود الجغرافية.(الإعلان العالمي لحقوق الإنسان، 1945)

وقد أصدر الاتحاد الأوروبي الأمر التشريعي الخاص بحماية البيانات ونقلها عبر الحدود لعام 1995، والذي مثّل مرحلة جديدة في إعادة تنظيم خصوصية المعلومات أدت إلى إعادة وضع العديد من دول أوروبا تشريعات جديدة أو تطوير تشريعاتها القائمة في هذا الحقل، وغالبية هذه القوانين إن لم تكن كلها اعتمدت في محتواها وما تضمنته على قرارات مجلس أوروبا لعامي 73 و74 واتفاقية (مجلس أوروبا) الخاصة بحماية البيانات من مخاطر المعالجة الآلية لعام 1980، وعلى دليل منظمة التعاون الاقتصادي والتنمية، ودليل الأمم المتحدة عام 1990، وفي تطورها وشموليتها خلال السنوات الخمس الأخيرة اعتمدت بشكل

واضح على تعليمات (الأمر التشريعي) للاتحاد الأوروبي لحماية البيانات عام 1995، وقد مثّلت قواعد هذه المدونات ما يمكن تسميته بالشرعة الدولية لحماية البيانات أو دستور خصوصية المعلومات، وهي تسمية تُطلق في هذه المرحلة من تطور موضوع خصوصية المعلومات لها في صياغة النظام القانوني لحماية البيانات والخصوصية في العصر الرقمي.(Ahmed & Zulhuda, 2015)

وقد أصدر الاتحاد الأوروبي عام 1995 دليلاً شاملاً ـ ملزماً لدول الاتحاد الأوروبي ولهذا نطلق عليه الأمر التشريعي، ويسميه البعض قانونًا أو تعليمات ـ ويتعلق بحماية خصوصية المعلومات وتنظيم نقل المعلومات خارج الحدود، وقد أقر من قبل البرلمان الأوروبي ومجلس أوروبا معًا، وتبعه عام 1997 دليلاً آخر لتنظيم معالجة البيانات الشخصية في قطاع الاتصالات، وهذا الجهد الجديد مضافًا إليه استمرار الجهود من قبل أطر الأمم المتحدة ومؤسسات أوروبا الموحدة ومنظمة التعاون الاقتصادي والتنمية عبر إصدار أدلة متعددة تعالج مختلف طوائف البيانات وحمايتها في البيئة الرقمية وتميز الأمر التشريعي للاتحاد الاوروبي لعام 1995 بإلزام الدول الأوروبية بإدماجه ضمن تشريعاتها في فترة أقصاها نهاية أكتوبر 1998، ما أدى إلى موجة تشريعية جديدة وموجة تعديل التدابير التشريعية القائمة في مختلف دول أوروبا، وتحديدًا الدول الخمسة عشر الأعضاء في الاتحاد آنذاك، وأثر ذلك على عشرات دول العالم من خارج أوروبا التي وجدت في هذه التجربة الناضجة لحماية البيانات الشخصية هاديًا لها ونموذجًا متقدمًا أمكنها الاعتماد عليه لإقرار تشريعات حماية البيانات الشخصية أو تشريعات الخصوصية الشمولية في دولها.(Vizcayno, 2012)

في حين اتجهت دول مثل هنجاريا إلى تنظيم التشريعات من أجل ضمان سلامة معيار التوازن بين الحق في المعلومات والحق في الخصوصية وانعكاسه على نحو صحيح في الأحكام التفصيلية، وساهم في ذلك أن الأمر التشريعي الأوروبي لعام 1995 نظم حماية البيانات الشخصية وبنفس الوقت الحق في نقل البيانات خارج الحدود، وهو جزء من مسائل الحق في الوصول للمعلومات، وقد وجدت بعض الدول حتى مع وجود التشريعين ـ كل على استقلال ـ أن الجهة المعنية بأحكامهما معًا يتعين أن تكون جهة واحدة؛ لهذا مثلاً نجد توجهًا لإناطة صلاحيات مراقبة ومتابعة مسائل الحق في الوصول للمعلومات لجهات (مفوضي) حماية البيانات المنشأة بموجب قوانين حماية البيانات، كما هو الشأن في بريطانيا، وقد قامت بريطانيا عام 1998 بتسمية جهة الرقابة على حماية البيانات الشخصية بـ"مفوض حماية البيانات" في أعقاب قانون حماية البيانات البريطاني لعام 1998، وكذلك صدور قانون حقوق الإنسان البريطاني عام 1998 بدل مفوض تسجيل البيانات الذي أنشئ بموجب قانون حماية البيانات عام 1984، وبصدور قانون حرية المعلومات البريطاني لعام 2000 أيضًا جرى تعديل قانون حماية البيانات لعام 1998 في مسائل عديدة، منها إعادة تسمية مفوض حماية البيانات ومحكمة البيانات المنشأتين بموجب قانون 1998 ليصبحا "مفوض المعلومات"، و"محكمة المعلومات"، مسندة لهما اختصاصات تتعلق بالحقين معاً ـ حماية البيانات الشخصية (الخصوصية) وحرية المعلومات (الحق في الوصول للمعلومات والسجلات) ـ وهو توجه أريد منه إيجاد جهة واحدة تباشر مهام متعددة بالنسبة المعلومات، سواء حق الوصول إليها أو حق حظر المساس بالبيانات الشخصية منها لضمان عدم اختلال معيار التوازن لدى مباشرة الحقين، وعلى جانب آخر نجد أن الحق في احترام الحياة الخاصة في فرنسا محمي في المادة التاسعة من القانون المدني الفرنسي، إضافةً إلى ذلك فقد أقرت المحكمة الدستورية الفرنسية أن الحق في الخصوصية متضمن في

المادة الثانية من إعلان حقوق الإنسان والمواطنين لعام 1789، وكذلك في دستور الجمهورية الفرنسية لعام 1955.(Vizcayno, 2012)

ثانياً: التشريعات العربية لحماية المعلومات الشخصية

أشار (اتحاد المصارف العربية، 2018) إلى العديد من التشريعات والقوانين المتعلقة لحماية المعلومات الشخصية في الكثير من الدول العربية، وفيما يلي حصر بعض منها على سبيل المثال:

الأردن:

- قانون المعاملات الإلكترونية رقم (85) عام 2001.
- قانون جرائم أنظمة المعلومات عام 2010.
- قانون الجرائم الإلكترونية رقم (5343) عام 2015.

المملكة العربية السعودية:

- نظام حماية البيانات الشخصية (مرسوم ملكي) رقم (م/19) لعام 2021، وقرار مجلس الوزراء رقم (98) لعام 2021.
- نظام مكافحة جرائم المعلوماتية (مرسوم ملكي) رقم (م/17) لعام 1428هـ.

البحرين:

- قانون رقم (60) لعام 2014 بشأن جرائم تقنية المعلومات.

الكويت:

- قانون رقم (63) لعام 2015 في شأن مكافحة جرائم تقنية المعلومات.

سلطنة عمان:

- قانون مكافحة جرائم تقنية المعلومات لعام 2011.

الإمارات العربية المتحدة:

- القانون الاتحادي رقم (12) لسنة 2016، بتعديل المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات – وزارة العدل.
- إرشادات استخدام الإنترنت – الهيئة العامة لتنظيم قطاع الاتصالات.
- فئات المحتوى المحظور – الهيئة العامة لتنظيم قطاع الاتصالات.
- قانون نشر وتبادل البيانات في إمارة دبي.
- القانون الاتحادي رقم (5) لسنة 2012 بشأن مكافحة الجرائم الإلكترونية.
- القانون الاتحادي رقم (1) لسنة 2006 بشأن المعاملات والتجارة الإلكترونية.
- إدارة النفاذ إلى الإنترنت – الهيئة العامة لتنظيم قطاع الاتصالات.
- الخطة الاستراتيجية للحكومة الإلكترونية الإتحادية.

- قرار وزاري رقم (1) لسنة 2008 بشأن إصدار لائحة مزودي خدمات التصديق.

- **معوقات وضع القوانين والتشريعات الخاصة بحماية البيانات**

هناك مجموعة من المتناقضات التي تعوق الدول في سن ووضع القوانين والتشريعات الخاصة بحق الفرد في حماية حياته وبياناته الخاصة، ويشير (يونس، 2004) إلى بعضها على النحو التالي:

- التناقض بين حق الحياة الخاصة وحق الدولة في الاطلاع على شؤون الأفراد.
- التناقض بين حق الفرد في الاحتفاظ بسريته، ومصلحته في كشف حياته الخاصة باعتبار أن الاحتفاظ بالسرية حق والكشف الطوعي عن هذه السرية حق أيضًا، إلا إن احتمال استغلال المعلومات المعطاة طوعًا لأغراض غير التي أعطيت لأجلها يمثّل انتهاكًا لحرمة الفرد.
- التناقض بين الحياة الخاصة، والحق في جمع المعلومات لغايات البحث العلمي، أو حرية البحث العلمي.
- التناقض بين الحق في الحياة الخاصة، وبين حرية الصحافة وتبادل المعلومات (الحرية الإعلامية).

- **حماية المعلومات الشخصية في المملكة العربية السعودية**

أولاً: مبادئ وتشريعات حماية المعلومات في المملكة العربية السعودية

توضع التشريعات الأساسية لحماية حقوق الأفراد فيما يتعلق ببياناتهم الشخصية في جميع الجهات الحكومية، وكذلك الجهات خارج المملكة التي تتعامل مع البيانات الشخصية للأفراد المقيمين داخل المملكة بأي شكل من الأشكال، بما في ذلك معالجة البيانات الشخصية عبر شبكة الإنترنت، وتحدد التشريعات أيضًا حقوق أصحاب البيانات، وأهداف مراقب البيانات، والمبادئ الأساسية لحماية البيانات.

ثانياً: سياسة حماية البيانات الشخصية في المملكة

يشير (الغويري، 2014) إلى أن سياسة حماية البيانات الشخصية بالمملكة تعمل على تمكين أصحاب البيانات الشخصية من القيام بعدد من الأشياء، منها:

- إبلاغ أصحاب البيانات ببياناتهم في أي وقت يريدونها، حيث تشرح لهم الغرض من المعالجة والتجميع.
- السماح للمالكين بالوصول إلى البيانات وطباعتها مع إمكانية الحصول على نسخة.
- تسهيل عملية تنظيم البيانات بين الأطراف التي تريد استخدامها.
- إمكانية الاعتراض أو إلغاء الموافقة على معالجة بعض البيانات.
- إتاحة الإمكانية للمالكين لطلب تعديل البيانات أو تصحيحها، وحذفها وتقييدها في معالجتها.

ثالثاً: أهداف نظام حماية البيانات الشخصية في المملكة

يبحث العديد من المواطنين في المملكة العربية السعودية عن الأهداف الأساسية لإصدار "نظام حماية البيانات الشخصية" لأن الغرض الأساسي من إصدار هذا النظام الجديد هو حماية البيانات الجديدة أثناء العمل على تحقيق أهداف رؤية المملكة 2030، ويتضمن هذا النظام عددًا من الأهداف الفرعية، يشير (الزهراني، 2013) إلى بعض منها فيما يلي:

- الحفاظ على خصوصية البيانات الشخصية لأصحابها.
- مساعدة الوصول إلى مجتمع المعلومات والاقتصاد الرقمي على تسريع عملية التحول الرقمي.
- تطوير البنية التحتية والتنمية الرقمية؛ مما يساهم بشكل كبير في تعزيز الابتكار.
- العمل على تحقيق الريادة والتقدم العالميين، مع مراعاة الاستدامة والتقدم الاقتصادي للدولة والسيادة الوطنية لتلك البيانات.
- محاولة جذب الاستثمار الأجنبي للمملكة.
- العمل على حماية حقوق معالجة البيانات لأي مستثمر أجنبي.
- السعي نحو بناء الثقة من خلال خدمة تقنية المعلومات وكذلك الخدمة البريدية.
- وضع الأسس والمعايير التنظيمية لتمكين مستخدمي البيانات من الابتكار من خلال استخدام أي بيانات شخصية.

رابعاً: القواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة

تتمثل القواعد والمعايير الخاصة بنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة بما يضمن الحفاظ على السيادة الوطنية على هذه البيانات، وكذلك الحفاظ على خصوصية البيانات الشخصية، وحماية حقوق المالكين لها من خلال تحديد التزامات المراقبين والمعالجين فيما يتعلق بنقل البيانات الشخصية خارج المملكة. وتسري أحكام هذه الوثيقة على جميع الجهات (الحكومية والخاصة وغير الربحية) في المملكة التي تنقل البيانات الشخصية إلى أطراف أخرى خارج الحدود الجغرافية للمملكة بغرض المعالجة، وقد أظهرَ تحليل "نظام حماية البيانات الشخصية" أنّه يبدو متوافقًا مع المعايير الدولية في نواحٍ معيّنة، ولكن بعض المواد مثيرة للقلق وتحتوي على ثغرات قد تسمح بانتهاك الحق في الخصوصية وحماية البيانات، ولا تكمُن المشكلة في نص القانون بحد ذاته، بل في إمكانية تطبيقه وتنفيذه في المملكة العربية السعودية.(المعداوي، 2018)

خامساً: علاقة نظام حماية البيانات الشخصية في المملكة بالمعايير الدولية

يتضمن "نظام حماية البيانات الشخصية" السعودي معظم المعايير الدولية الأساسية في مجال حماية البيانات، ومنها على سبيل المثال حقوق أصحاب البيانات، والأساس القانوني لمعالجة البيانات –الخاضعة وغير الخاضعة للموافقة–، ومتطلبات سياسات الخصوصية، وواجب الإبلاغ في حال انتهاك خصوصية البيانات، وضرورة تقييم الأثر قبل معالجة البيانات الشخصية، والأحكام المحددة بشأن البيانات الصحية، وبيانات الائتمان، والتزامات جهات التحكم، وإجراءات العناية الواجبة، وإنشاء جهة مشرفة، والعقوبات في حالات الانتهاكات... والقائمة تطول، وتتفق العديد من خصائص "نظام حماية البيانات الشخصية" السعودي

مع معايير ومبادئ قوانين حماية البيانات الدولية، مثل اللائحة الأوروبية العامة لحماية البيانات 679/2016 (GDPR) أي اللائحة التي ينص عليها قانون الاتحاد الأوروبي حول حماية البيانات والخصوصية في الاتحاد الأوروبي والمنطقة الاقتصادية الأوروبية، كما توفر ''اللائحة العامة الأوروبية لحماية البيانات" أوسع حماية للبيانات الشخصية، ولها تأثير مهم على القوانين واللوائح خارج الاتحاد الأوروبي، إذ إنَ التشريعات الناشئة تستند إلى اللائحة الأوروبية كنقطة انطلاق للقوانين التي تنص عليها.(الغويري، 2014)

الإطار التطبيقي

يتناول الباحثان في هذا الفصل عرضًا لمنهجية الدراسة ومجتمع وعينة الدراسة، والأساليب الإحصائية، وأداة الدراسة، وكيفية حساب معاملات الصدق والثبات لأداة الدراسة، كما سيتناول إجراءات الدراسة حيث وصف عينة الدراسة وتحليل أداة الدراسة، ثم استخلاص النتائج، وتحليلها بغرض الوصول إلى إجابات عن تساؤلات الدراسة.

▪ منهجية الدراسة

استخدم الباحثان المنهج الكمي باعتباره الأقرب لتحقيق أهداف الدراسة، باستخدام أداة الدراسة ـ استمارة استبيان ـ واستخدام أساليب التحليل الإحصائي لتحليل البيانات الخاصة بالدراسة للوصول إلى نتائج وتوصيات تحقق أهداف الدراسة.

▪ مجتمع وعينة الدراسة

يتمثّل مجتمع الدراسة في كافة مستخدمي خدمات جوجل Google والفيسبوك Facebook في المملكة العربية السعودية، ونظرًا لكبر حجم مجتمع الدراسة، ولصعوبة إجراء الحصر الشامل له فقد قام الباحثان باستخدام أسلوب العينة العشوائية البسيطة في اختبار أفراد عينة الدراسة عن طريق نشر الرابط الإلكتروني الخاص بالاستبيان على كافة مواقع التواصل الاجتماعي التي يتواجد بها أفراد مجتمع الدراسة، وقد بلغ عدد أفراد عينة الدراسة (98) فرد، وهم الذين قاموا بالإجابة عن أسئلة الاستبيان.

▪ الأساليب الإحصائية

- التوزيعات التكرارية، النسب المئوية، المتوسطات الحسابية، الانحرافات المعيارية، الوزن النسبي وذلك لوصف خصائص عينة الدراسة ومتغيراتها.
- اختبار كرونباخ ألفا: لقياس ثبات أداة الدراسة.
- معامل الارتباط لبيرسون: لقياس الاتساق الدّاخلي لعبارات الاستبيان.

▪ أداة الدراسة

اعتمد الباحثان في الدراسة الميدانية على استخدام استمارة استبيان إلكتروني كأداة للدراسة، وقد تضمنت استمارة الاستبيان قسمين، الأول يشتمل على الأسئلة المتعلقة بخصائص أفراد عينة الدراسة، والثاني يشتمل على محاور الدراسة، والتي تشتمل

على محور خصوصية وأمان حساباتي الشخصية ويتضمن (19) عبارة، ومحور الخصوصية والأمان عبر الإنترنت ويتضمن (13) عبارة، ومحور دور الدولة في حماية البيانات الشخصية ويتضمن (12) عبارة، واستخدم الباحثان مقياس ليكرت الخماسي في الإجابة على عبارات الاستبيان، والذي يتكون من أوافق بشدة (5)، أوافق (4)، محايد (3)، لا أوافق (2)، لا أوافق مطلقاً (1)

- **صدق أداة الدراسة**

تم حساب صدق عبارات استمارة الاستبيان من خلال القيام بحساب قيمة معامل الارتباط بيرسون بين درجة كل عبارة والدرجة الكلية للمحور التي تنتمي إليه العبارة، وذلك لتحديد مستوى الاتساق الداخلي لأداة الدراسة، وجاءت النتائج كما يلي:

المحور الأول: خصوصية وأمان حساباتي الشخصية

جدول رقم (1) معاملات الارتباط بين درجة كل عبارة والدرجة الكلية لمحور خصوصية وأمان حساباتي الشخصية

العبارة	معامل ارتباط بيرسون	الدلالة الاحصائية
- لا أمتلك حساب بريد إلكتروني خاص بي.	**0.389	0.000
- يعد تأمين وحماية خصوصية معلوماتي من الأمور الهامة التي أحرص عليها.	**0.306	0.000
- عادةً ما أستخدم كلمة سر قوية ومختلفة لا يمكن اختراقها.	**0.392	0.000
- أمكّن محرك البحث (جوجل) من الاحتفاظ بتسجيل كامل لجميع الأنشطة الخاصة بي على الإنترنت.	**0.234	0.000
- اضطررت من قبل أن أغير كلمات المرور الخاصة بحساباتي لحمايتها من الاختراق.	**0.587	0.000
- أستخدم كلمة مرور تزيد عن (12) حرف ورقم ورموز تعبيرية.	**0.497	0.000
- أستخدم ميزة المصادقة الثنائية لتسجيل الدخول الجديد لحساب الجوجل الخاص بي.	**0.477	0.000
- أستخدم ميزة المصادقة الثنائية لتسجيل الدخول لحساب الفيسبوك.	**0.471	0.000
- يرسل تفعيل ميزة المصادقة الثنائية كود خاص لهاتفي المقترن بالحساب لأتمكن من تسجيل الدخول.	**0.357	0.000
- لا أتشارك معلوماتي الشخصية مع الغرباء عبر الإنترنت.	**0.318	0.000
- لا أتشارك تفاصيل حساب بريدي الإلكتروني مع الآخرين.	**0.235	0.000
- أتجنب ربط أن تطبيقات تابعة لجهات خارجية بحساب البريد الإلكتروني الخاص بي.	**0.264	0.000
- تعرضت من قبل لاختراق حسابي الشخصي على جوجل.	**0.609	0.000
- تعرضت من قبل لاختراق حسابي الشخصي على الفيسبوك.	**0.491	0.000
- لدي معلومات كافية عن سرقة البيانات الشخصية والجرائم الإلكترونية.	**0.356	0.000
- عادة ما أستخدم الحساب الخاص بي من جهازي الخاص.	**0.474	0.000
- أستخدم مواقع وسائل التواصل الاجتماعي والبريد الإلكتروني بصورة فعّالة.	**0.314	0.000

– لا أتمكن من إدارة الإعدادات الخاصة ببياناتي الشخصية.	**0.281	0.000
– لا أهتم بحماية بياناتي الشخصية عبر المواقع الإلكترونية.	**0.333	0.000

** ذات دلالة إحصائية عند 0.01

المحور الثاني: الخصوصية والأمان عبر الإنترنت

جدول رقم (2) معاملات الارتباط بين درجة كل عبارة والدرجة الكلية لمحور الخصوصية والأمان عبر الإنترنت

العبارة	معامل ارتباط بيرسون	الدلالة الاحصائية
– يتم تفعيل ميزة المصادقة الثنائية لأي تسجيل دخول جديد لحساب الجوجل.	**0.627	0.000
– يتم تفعيل ميزة المصادقة الثنائية لأي تسجيل دخول جديد لحساب الفيسبوك.	**0.598	0.000
– عند تفعيل ميزة المصادقة الثنائية يتم إرسال كود خاص لهاتف المستخدم المقترن بالحساب ليتمكن من تسجيل الدخول.	**0.693	0.000
– توفر مواقع (فيسبوك –جوجل) ميزة المصادقة الثنائية للحفاظ على خصوصية المعلومات ومنع المخترقين من الوصول للبيانات.	**0.661	0.000
– تقلل ميزة المصادقة الثنائية من احتمالية الاحتيال أو سرقة الهوية أو فقدان البيانات.	**0.548	0.000
– ترفع ميزة المصادقة الثنائية من درجة حماية البيانات الشخصية.	**0.533	0.000
– تعد حماية بيانات البريد الإلكتروني عملية هامة للغاية.	**0.357	0.000
– تتوفر لدى (جوجل – فيسبوك) أنظمة أمان عالية الجودة، إلا إنها تواجه معوقات لتحقيق ذلك في ظل تطور البرامج المستخدمة في التجسس.	**0.389	0.000
– لبرامج حماية الخصوصية عبر الإنترنت دور في منع البرامج الأخرى من اختراق الحسابات أو التجسس على المعلومات الشخصية.	**0.425	0.000
– لابد من تغيير إعدادات الخصوصية للحساب الخاص بشكل دوري.	**0.455	0.000
– يمكن للمستخدم أن يعرف ما إذا تم اختراق حسابه عن طريق تفعيل ميزة المزامنة الدورية للأنشطة.	**0.555	0.000
– عادة ما يتم تسجيل الخروج من البريد الإلكتروني أو الفيسبوك عند استشعار الموقع لنشاط غير مألوف لحماية الحساب من الاختراق.	**0.571	0.000
– للحفاظ على سرية المعلومات الشخصية يتم استخدام الاسم ورقم الجوال لتأمين البريد الإلكتروني والفيسبوك.	**0.570	0.000

** ذات دلالة إحصائية عند 0.01

المحور الثالث: دور الدولة في حماية البيانات الشخصية

جدول رقم (3) معاملات الارتباط بين درجة كل عبارة والدرجة الكلية لمحور دور الدولة في حماية البيانات الشخصية

العبارة	معامل ارتباط بيرسون	الدلالة الاحصائية
- تلقيت أو أحد أصدقائي من قبل رسائل تهديد إلكترونية.	**0.319	0.000
- عند التعرض للتهديد أو الابتزاز عبر الإنترنت أقوم بإبلاغ الجهات المختصة.	**0.498	0.000
- توفر الجهات المختصة الرقابة الكافية على المواقع المختلفة.	**0.587	0.000
- يساهم الوعي القانوني للمستخدم على تنمية شعوره بالمسؤولية.	**0.686	0.000
- تهتم الدول بسَنّ قوانين وتشريعات لحماية معلومات المستخدمين وبياناتهم.	**0.781	0.000
- تساهم قوانين حماية البيانات الشخصية في حماية الأفراد من مخاطر الإنترنت.	**0.738	0.000
- يجب استخدام مواقع الإنترنت بصورة قانونية وألا يتم التعدّي على خصوصية الآخرين.	**0.727	0.000
- تقوم الدولة بتنظيم حملات توعوية لمستخدمين الإنترنت عن كيفية المحافظة على بياناتهم الشخصية.	**0.556	0.000
- سرعة التغيرات التكنولوجية تطغى في بعض الأحيان على المعايير الأخلاقية والتشريعات.	**0.398	0.000
- حماية البيانات الشخصية حقًا أساسيًا للمستخدمين.	**0.644	0.000
- يجب الحفاظ على المعلومات الشخصية بطريقة لا تمكّن أي طرف ثالث من الوصول لها.	**0.528	0.000
- الإنترنت ليس مكانًا لنشر المعلومات الهامة ونشر البيانات الشخصية.	**0.331	0.000

** ذات دلالة إحصائية عند 0.01

تبين من خلال ما سبق أن جميع معاملات الارتباط لجميع عبارات استمارة الاستبيان كانت ذات دلالة إحصائية عند مستويات معنوية (0.01)، وهذا يعني أن الأداة تتمتع بمستوى صدق مرتفع وهي صالحة لأغراض الدراسة.

- **ثبات أداة الدراسة**

تم حساب معامل ألفا كورنباخ لعبارات محاور الاستبيان، وجاءت النتائج كما يلي:

جدول رقم (4) معامل الثبات لمحاور استمارة الاستبيان

المحاور	معامل الفا كورنباخ	عدد العبارات
- خصوصية وأمان حساباتي الشخصية	0.644	19
- الخصوصية والأمان عبر الإنترنت	0.786	13
- دور الدولة في حماية البيانات الشخصية	0.755	12
- إجمالي استمارة الاستبيان	0.816	44

يتبين من الجدول رقم (4) أن قيمة معامل الثبات Alpha هي أكبر من (0.6) لجميع محاور استمارة الاستبيان؛ مما يؤكد على صلاحية وارتباط عبارات محاور استمارة الاستبيان وارتفاع مستوى ثبات أداة الدراسة؛ مما يسمح باستخدامها لغرض الدراسة.

- **إجراءات الدراسة**

بعد جمع استجابات الأفراد عينة الدراسة على الاستبيان الموزع، قام الباحثان بتحليل تلك الاستجابات واستخلاص النتائج من خلال المفاهيم الإحصائية للوصول إلى النتائج لتحليلها، وتفسيرها في ضوء الإطار النظري للدراسة والدراسات السابقة ذات العلاقة بموضوع الدراسة.

أولاً: وصف عينة الدراسة

جدول رقم (5) توزيع أفراد عينة الدراسة وفقًا للخصائص الشخصية

الخاصية	الفئات	العدد	النسبة
الجنس	ذكر	77	78.6
	انثي	21	21.4
الفئة العمرية	أقل من 30 سنة	20	20.4
	من 30 – أقل من 40 سنة	26	26.5
	من 40 – أقل من 50 سنة	30	30.6
	50 عام فأكثر	22	22.4
المؤهل التعليمي	متوسط	11	11.2
	جامعي	71	72.4
	دراسات عليا	16	16.3
المهنة	إدارية	70	71.4
	فنية	28	28.6
التخصص الأكاديمي	نظري	42	42.9
	عملي	56	57.1

ثانياً: تحليل عبارات استمارة الاستبيان

للإجابة عن التساؤل الفرعي الأول:

"ما مدى فاعلية المصادقة الثنائية في حماية المعلومات الشخصية من وجهة نظر مستخدمي خدمات الجوجل والفيسبوك بالمملكة العربية السعودية؟"

تم حساب المتوسطات الحسابية والانحرافات المعيارية لموافقة أفراد عينة الدراسة على العبارات التي تعكس مدى فاعلية المصادقة الثنائية في حماية المعلومات الشخصية من وجهة نظر أفراد عينة الدراسة.

المحور الأول: خصوصية وأمان حساباتي الشخصية

جدول رقم (6) المتوسط الحسابي والانحراف المعياري والوزن النسبي والترتيب لعبارات محور خصوصية وأمان حساباتي الشخصية

العـــــبارة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الترتيب	مستوي الموافقة
لا أمتلك حساب بريد إلكتروني خاص بي.	4.847	0.389	0.969	2	مرتفع
يعد تأمين وحماية خصوصية معلوماتي من الأمور الهامة التي أحرص عليها.	4.908	0.290	0.982	1	مرتفع
عادةً ما أستخدم كلمة سر قوية ومختلفة لا يمكن اختراقها.	4.327	0.847	0.865	6	مرتفع
أمكّن محرك البحث (جوجل) من الاحتفاظ بتسجيل كامل لجميع الأنشطة الخاصة بي على الإنترنت.	3.296	1.318	0.659	14	متوسط
اضطررت من قبل أن أغير كلمات المرور الخاصة بحساباتي لحمايتها من الاختراق.	3.908	1.113	0.782	10	مرتفع
أستخدم كلمة مرور تزيد عن (12) حرف ورقم ورموز تعبيرية.	3.602	1.282	0.720	12	متوسط
أستخدم ميزة المصادقة الثنائية لتسجيل الدخول الجديد لحساب الجوجل الخاص بي.	4.061	1.003	0.812	9	مرتفع
أستخدم ميزة المصادقة الثنائية لتسجيل الدخول لحساب الفيسبوك.	3.592	1.234	0.718	13	متوسط
يرسل تفعيل ميزة المصادقة الثنائية كود خاص لهاتفي المقترن بالحساب لأتمكن من تسجيل الدخول.	4.337	0.885	0.867	5	مرتفع
لا أتشارك معلوماتي الشخصية مع الغرباء عبر الإنترنت.	4.765	0.552	0.953	3	مرتفع
لا أتشارك تفاصيل حساب بريدي الإلكتروني مع الآخرين.	4.582	0.798	0.916	4	مرتفع
أتجنب ربط أن تطبيقات تابعة لجهات خارجية بحساب البريد الإلكتروني الخاص بي.	4.163	1.173	0.833	8	مرتفع
تعرضت من قبل لاختراق حسابي الشخصي على جوجل.	2.296	1.286	0.459	17	منخفض
تعرضت من قبل لاختراق حسابي الشخصي على الفيسبوك.	2.112	1.217	0.422	18	منخفض
لدي معلومات كافية عن سرقة البيانات الشخصية والجرائم الإلكترونية.	3.622	1.108	0.724	11	متوسط
عادة ما أستخدم الحساب الخاص بي من جهازي الخاص.	2.490	1.186	0.498	15	متوسط

أستخدم مواقع وسائل التواصل الاجتماعي والبريد الإلكتروني بصورة فعّالة.	4.224	0.844	0.845	7	مرتفع
لا أتمكن من إدارة الإعدادات الخاصة ببياناتي الشخصية.	2.469	1.168	0.494	16	متوسط
لا أهتم بحماية بياناتي الشخصية عبر المواقع الإلكترونية.	1.918	1.282	0.384	19	منخفض
المتوسط العام	**3.659**	**0.999**	**متوسط**		

عند دراسة عبارات محور "خصوصية وأمان حساباتي الشخصية" من حيث قيمة الوزن النسبي الأكبر من وجهة نظر عينة الدراسة تبين أن العبارة "يعد تأمين وحماية خصوصية معلوماتي من الأمور الهامة التي أحرص عليها" هي أكثر العبارات أهمية بوزن نسبس بلغ 0.982 بمستوى موافقة مرتفع، بينما كانت عبارة (لا أهتم بحماية بياناتي الشخصية عبر المواقع الإلكترونية) هي أقل العبارات أهمية بوزن نسبي بلغ 0.384 بمستوى موافقة منخفض، وتبين أن عبارات محور "خصوصية وأمان حساباتي الشخصية" جاءت (10) عبارات منها في مستوى الموافقة المرتفع و(6) عبارات في مستوى الموافقة المتوسط و(3) عبارات في مستوى الموافقة المنخفض؛ مما يوضح وجود مستوى متوسط من شعور أفراد عينة الدراسة من مستخدمي خدمات الجوجل والفيسبوك بوجود خصوصية وأمان لحساباتهم الشخصية، حيث بلغت قيمة المتوسط العام 3.659 بانحراف معياري 0.999

للإجابة عن التساؤل الفرعي الثاني "كيف يمكن توعية مستخدمي خدمات جوجل Google والفيسبوك Facebook حول حماية بياناتهم وكيفية تأمين معلوماتهم ضد الاختراق الإلكتروني؟" تم حساب المتوسطات الحسابية والانحرافات المعيارية لموافقة أفراد عينة الدراسة على العبارات التي تعكس مدى وعيهم حول حماية بياناتهم وكيفية تأمين معلوماتهم ضد الاختراق الإلكتروني من وجهة نظر أفراد عينة الدراسة.

المحور الثاني: الخصوصية والأمان عبر الإنترنت

جدول رقم (7) المتوسط الحسابي والانحراف المعياري والوزن النسبي والترتيب لعبارات محور الخصوصية والأمان عبر الإنترنت

العـــــبارة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الترتيب	مستوي الموافقة
يتم تفعيل ميزة المصادقة الثنائية لأي تسجيل دخول جديد لحساب الجوجل.	4.265	0.937	0.853	8	مرتفع
يتم تفعيل ميزة المصادقة الثنائية لأي تسجيل دخول جديد لحساب الفيسبوك.	3.918	1.137	0.784	12	مرتفع
عند تفعيل ميزة المصادقة الثنائية يتم إرسال كود خاص لهاتف المستخدم المقترن بالحساب ليتمكن من تسجيل الدخول.	4.500	0.662	0.900	4	مرتفع
توفر مواقع (فيسبوك –جوجل) ميزة المصادقة الثنائية للحفاظ على خصوصية المعلومات ومنع المخترقين من الوصول للبيانات.	4.469	0.749	0.894	5	مرتفع
تقلل ميزة المصادقة الثنائية من احتمالية الاحتيال أو سرقة الهوية أو فقدان البيانات.	4.612	0.683	0.922	2	مرتفع

ترفع ميزة المصادقة الثنائية من درجة حماية البيانات الشخصية.	4.602	0.622	0.920	3	مرتفع
تعد حماية بيانات البريد الإلكتروني عملية هامة للغاية.	4.765	0.472	0.953	1	مرتفع
تتوفر لدى (جوجل – فيسبوك) أنظمة أمان عالية الجودة، إلا إنها تواجه معوقات لتحقيق ذلك في ظل تطور البرامج المستخدمة في التجسس.	4.000	0.897	0.800	11	مرتفع
لبرامج حماية الخصوصية عبر الإنترنت دور في منع البرامج الأخرى من اختراق الحسابات أو التجسس على المعلومات الشخصية.	4.316	0.794	0.863	7	مرتفع
لابد من تغيير إعدادات الخصوصية للحساب الخاص بشكل دوري.	3.888	0.973	0.778	13	مرتفع
يمكن للمستخدم أن يعرف ما إذا تم اختراق حسابه عن طريق تفعيل ميزة المزامنة الدورية للأنشطة.	4.122	0.777	0.824	10	مرتفع
عادة ما يتم تسجيل الخروج من البريد الإلكتروني أو الفيسبوك عند استشعار الموقع لنشاط غير مألوف لحماية الحساب من الاختراق.	4.173	0.920	0.835	9	مرتفع
للحفاظ على سرية المعلومات الشخصية يتم استخدام الاسم ورقم الجوال لتأمين البريد الإلكتروني والفيسبوك.	4.418	0.907	0.884	6	مرتفع
المتوسط العام	**4.312**	**0.810**	**متوسط**		

عند دراسة عبارات محور "الخصوصية والأمان عبر الإنترنت" من حيث قيمة الوزن النسبي الأكبر من وجهة نظر عينة الدراسة، تبين أن العبارة (تعد حماية بيانات البريد الإلكتروني عملية هامة للغاية) هي أكثر العبارات أهمية بوزن نسبي بلغ 0.953 بمستوى موافقة مرتفع، بينما كانت عبارة (لابد من تغيير إعدادات الخصوصية للحساب الخاص بشكل دوري) هي أقل العبارات أهمية بوزن نسبي بلغ 0.778 بمستوى موافقة مرتفع، وتبين أن عبارات محور "الخصوصية والأمان عبر الإنترنت" جاءت كلها في مستوى الموافقة المرتفع؛ مما يوضح ارتفاع مستوى شعور أفراد عينة الدراسة من مستخدمي خدمات الجوجل والفيسبوك بوجود الخصوصية والأمان عبر الإنترنت، حيث بلغت قيمة المتوسط العام 4.312 بانحراف معياري 0.810

للإجابة عن التساؤل الفرعي الثالث "كيف تساعد المبادئ والتشريعات بالمملكة العربية السعودية في حماية المعلومات الشخصية لمستخدمي الإنترنت؟" تم حساب المتوسطات الحسابية والانحرافات المعيارية لموافقة أفراد عينة الدراسة على العبارات التي تعكس دور المبادئ والتشريعات بالمملكة العربية السعودية في حماية المعلومات الشخصية لمستخدمي الإنترنت من وجهة نظر أفراد عينة الدراسة.

المحور الثالث: دور الدولة في حماية البيانات الشخصية

جدول رقم (8) المتوسط الحسابي والانحراف المعياري والوزن النسبي والترتيب لعبارات محور دور الدولة في حماية البيانات الشخصية

العـــــبارة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الترتيب	مستوي الموافقة
تلقيت أو أحد أصدقائي من قبل رسائل تهديد إلكترونية.	3.112	1.442	0.622	12	متوسط
عند التعرض للتهديد أو الابتزاز عبر الإنترنت أقوم بإبلاغ الجهات المختصة.	4.571	0.799	0.914	5	مرتفع
توفر الجهات المختصة الرقابة الكافية على المواقع المختلفة.	4.020	1.084	0.804	11	مرتفع
يساهم الوعي القانوني للمستخدم على تنمية شعوره بالمسؤولية.	4.480	0.721	0.896	7	مرتفع
تهتم الدول بسَنّ قوانين وتشريعات لحماية معلومات المستخدمين وبياناتهم.	4.429	0.825	0.886	8	مرتفع
تساهم قوانين حماية البيانات الشخصية في حماية الأفراد من مخاطر الإنترنت.	4.531	0.735	0.906	6	مرتفع
يجب استخدام مواقع الإنترنت بصورة قانونية وألا يتم التعدّي على خصوصية الآخرين.	4.663	0.657	0.933	3	مرتفع
تقوم الدولة بتنظيم حملات توعوية لمستخدمين الإنترنت عن كيفية المحافظة على بياناتهم الشخصية.	4.398	0.858	0.880	9	مرتفع
سرعة التغيرات التكنولوجية تطغى في بعض الأحيان على المعايير الأخلاقية والتشريعات.	4.378	0.739	0.876	10	مرتفع
حماية البيانات الشخصية حقًا أساسيًا للمستخدمين.	4.786	0.460	0.957	2	مرتفع
يجب الحفاظ على المعلومات الشخصية بطريقة لا تمكّن أي طرف ثالث من الوصول لها.	4.806	0.446	0.961	1	مرتفع
الإنترنت ليس مكانًا لنشر المعلومات الهامة ونشر البيانات الشخصية.	4.582	0.798	0.916	4	مرتفع
المتوسط العام	**4.396**	**0.797**	**مرتفع**		

عند دراسة عبارات محور "دور الدولة في حماية البيانات الشخصية" من حيث قيمة الوزن النسبي الأكبر من وجهة نظر عينة الدراسة، تبين أن العبارة (يجب الحفاظ على المعلومات الشخصية بطريقة لا تمكّن أي طرف ثالث من الوصول لها) هي أكثر العبارات أهمية بوزن نسبي بلغ 0.961 بمستوى موافقة مرتفع، بينما كانت عبارة (تلقيت أو أحد أصدقائي من قبل رسائل تهديد إلكترونية) هي أقل العبارات اهمية بوزن نسبي بلغ 0.622 بمستوى موافقة متوسط، وتبين أن عبارات محور دور الدولة في حماية البيانات الشخصية جاءت (11) عبارة منها في مستوى الموافقة المرتفع، وعبارة واحدة في مستوى الموافقة المتوسط؛ مما يوضح ارتفاع مستوى وعي أفراد عينة الدراسة من مستخدمي خدمات الجوجل والفيسبوك بأهمية دور الدولة في حماية البيانات الشخصية، حيث بلغت قيمة المتوسط العام 4.396 بانحراف معياري 0.797

من الجداول السابقة يتبين ارتفاع مستوى حماية المعلومات الشخصية باستخدام ميزة المصادقة الثنائية من وجهة نظر أفراد عينة الدراسة من مستخدمي خدمات الجوجل والفيسبوك، حيث بلغت قيمة المتوسط العام 4.053 بانحراف معياري 0.888

النتائج:

توصلت الدراسة إلى النتائج الآتية:

- وجود مستوى متوسط من شعور أفراد عينة الدراسة من مستخدمي خدمات الجوجل والفيسبوك بوجود خصوصية وأمان لحساباتهم الشخصية، حيث بلغت قيمة المتوسط العام 3.659 بانحراف معياري 0.999، ما يعني أن أفراد عينة الدراسة من مستخدمي خدمات الجوجل والفيسبوك لديهم شعور متوسط بتمتّعهم بالأمان والخصوصية لحساباتهم الشخصية.

- ارتفاع مستوى شعور أفراد عينة الدراسة من مستخدمي خدمات الجوجل والفيسبوك بوجود الخصوصية والأمان عبر الإنترنت، حيث بلغت قيمة المتوسط العام 4.312 بانحراف معياري 0.810، ما يعني أن أفراد عينة الدراسة من مستخدمي خدمات الجوجل والفيسبوك شعورهم قوي بأنهم يتمتعون بالأمان والخصوصية عبر الإنترنت عمومًا.

- ارتفاع مستوى وعي أفراد عينة الدراسة من مستخدمي خدمات الجوجل والفيسبوك بأهمية دور الدولة في حماية البيانات الشخصية، حيث بلغت قيمة المتوسط العام 4.396 بانحراف معياري 0.797، ما يعني أن أفراد عينة الدراسة من مستخدمي خدمات الجوجل والفيسبوك يرون أن للدولة دور مهم ذا تأثير في حماية بياناتهم الشخصية.

- ارتفاع مستوى حماية المعلومات الشخصية باستخدام ميزة المصادقة الثنائية من وجهة نظر أفراد عينة الدراسة من مستخدمي خدمات الجوجل والفيسبوك حيث بلغت قيمة المتوسط العام 4.053 بانحراف معياري 0.888، ما يعني فاعلية ميزة المصادقة الثنائية في حماية المعلومات الشخصية ما يؤكد على تحقق أهداف الدراسة.

التوصيات:

على ضوء نتائج الدراسة، يوصي الباحثانان بما يلي:

- القيام بدراسات وبحوث متعددة حول تطبيق ميزات متنوعة من المستحدثات التكنولوجية لحماية المعلومات الشخصية وزيادة مستوى الخصوصية.

- توجيه المهتمين بالمجالات التقنية لاستحداث تقنيات جديدة لحماية الخصوصية من خلال سد الثغرات التي قد تكون في التقنيات الحالية.

- توعية مستخدمي الإنترنت والهواتف الذكية بضرورة حماية معلوماتهم الشخصية وعدم الإفصاح عنها للآخرين.

- تفعيل دول الإعلام ووسائل التواصل الاجتماعي للتوعية ضد مخاطر عدم الخصوصية، وتداول المعلومات الشخصية، واستخدام بيانات شخصية حقيقية بتلك المواقع.

- تفعيل دور المدارس والجامعات والمؤسسات التعليمية لتوعية الأطفال والشباب ضد مخاطر استخدام الإنترنت، وضرورة مراقبتهم لله عز وجل في كل تصرفاتهم، وفي كيفية استخدامهم للإنترنت.

قائمة المراجع:

- الحمصاني، صبحي (1979) أركان حقوق الإنسان "بحث مقارن في الشريعة الإسلامية والقوانين الحديثة". دار العلم للملايين، بيروت.
- الشمر، وليد سليم (2017) حماية الخصوصية في الإنترنت. دار الفكر الجامعي، الإسكندرية.
- الملط، أحمد خليفة (2006) الجرائم المعلوماتية. ط1، دار الفكر، الإسكندرية.
- يونس، عمر أبو بكر (2004) الجرائم الناشئة عن استخدام الإنترنت. دار النهضة العربية – القاهرة.
- أبو حجيلة، محمد رشيد حامد (2007) الحماية الجزائية للمعلومات الشخصية للأفراد في مواجهة أخطار بنوك المعلومات: دراسة مقارنة. رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في القانون في كلية الدراسات الفقهية والقانونية، جامعة آل البيت.
- أحمد، هندي عبد الله هندي (2017) قانون حماية البيانات الشخصية في مواقع التواصل الاجتماعي لمؤسسات المكتبات والمعلومات: دراسة تحليل مضمون. المؤتمر الثامن والعشرون: شبكات التواصل الاجتماعي وتأثيراتها في مؤسسات المعلومات في الوطن العربي، الاتحاد العربي للمكتبات والمعلومات، ص ص1-25، 27-29 نوفمبر.
- الرشيدي، علي بن ضبيّان (2005) العدوان على البيئة المعلوماتية خطورته ومواجهته. مجلة كلية الملك خالد العسكرية، ع81.
- الزهراني، يحيى بن مفرح (2013) تحديات الأمن المعلوماتي في الشبكات الاجتماعية في المملكة العربية السعودية من منظور قانوني. المجلة العربية الدولية للمعلوماتية، اتحاد الجامعات العربية – جمعية كليات الحاسبات والمعلومات، مج2، ع3، ص ص1-12.
- صالح، رضا إبراهيم؛ وأبو موسى، أحمد عبد السلام؛ وأبو سعدة، ندا حامد توفيق (2020) دراسة أثر إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية: مع دراسة ميدانية على الشركات المصرية. مجلة الدراسات التجارية المعاصرة، مج6، ع10، ج1، ص ص106-142.
- عثمان، عثمان بكر (2017) المسئولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي. بحث مقدم إلى المؤتمر العلمي الرابع: القانون والإعلام، الجلسة الرابعة، اليوم الثاني كلية الحقوق – جامعة طنطا، 23-24 إبريل.
- العرب، يونس (2002) دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي. ورقة عمل مقدمة إلى ندوة اخلاق المعلومات، الأردن: نادي المعلومات العربي، 17-16 أكتوبر.

- العنزي، زياد خليف (2018) المسؤولية القانونية عن طرد عضو من المجموعة في مواقع التواصل الاجتماعي في التشريع الأردني. دراسات، علوم الشريعة والقانون، مج45، ع2، ص ص209-222.
- الغافري، حسين بن سعيد (2008) الحماية القانونية للخصوصية المعلوماتية في ظل مشروع قانون المعاملات الإلكترونية العماني. بحث مقدم إلى مؤتمر أمن المعلومات والخصوصية في ظل قانون الإنترنت، القاهرة 2-4 يونيو.
- الغويري، ضيف الله بن نوح (2014) ضمانات الحق في الحماية الخاصة في النظام السعودي. إدارة الأعمال، جمعية إدارة الأعمال العربية، ع146، ص ص37-43.
- فهمي، دينا عبد العزيز (2017) المسئولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي. بحث مقدم إلى المؤتمر العلمي الرابع: القانون والإعلام، الجلسة الرابعة، اليوم الثاني كلية الحقوق - جامعة طنطا، 23-24 إبريل.
- كامل، جبالي أبو هشيمة (2016) حماية البيانات الشخصية في البيئة الرقمية. بحث مقدم إلى مؤتمر العصر الرقمي وإشكالياته القانونية، كلية الحقوق - جامعة أسيوط، 12-13 أبريل.
- مصطفى، خالد حامد (2013) المسؤولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي. رؤى استراتيجية، مج1، ع2، ص ص8-45.
- المعداوي، محمد أحمد (2018) حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي دراسة مقارنة. مجلة كلية الشريعة والقانون بطنطا، مج33، ع4، ص ص1926-2057.
- الموسوي، منى تركي؛ وفضل الله، جان سيريل (2013) الخصوصية المعلوماتية واهميتها ومخاطر التقنيات الحديثة عليها. مجلة كلية بغداد للعلوم الاقتصادية الجامعة، مج2013، ع4، ص ص303-355.
- المؤيد، محمد عبد الله (2009) صور المسئولية التقصيرية الناشئة عن الاعتداء على بيانات الكمبيوتر والتعامل عبر الانترنت وتسوية منازعاتها. مجلة الدراسات الاجتماعية، جامعة العلوم والتكنولوجيا، ع28، ص ص159-212.
- الهادي، محمد محمد (2006) توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية. Cybrarians Journal، البوابة العربية للمكتبات والمعلومات، ع9، ص ص34-76.
- اتحاد المصارف العربية (2018) أمن المعلومات: المخاطر وتحديات المستقبل. منشورات إتحاد المصارف العربية، ع454. أمن-المعلومات-المخاطر-وتحديات-المستق/ https://uabonline.org/ar/
- نظام حماية البيانات الشخصية، مجموعة الأنظمة السعودية، مج1. راجع:
https://laws.boe.gov.sa/boelaws/laws/lawdetails/b7cfae89-828e-4994-b167-adaa00e37188/1.
- نظام مكافحة جرائم المعلوماتية، مجموعة الأنظمة السعودية، مج7. راجع:
https://laws.boe.gov.sa/BoeLaws/Laws/Viewer/18cb4fe6-ab94-47b1-ad4c-a8ba9005382f?lawId=25df73d6-0f49-4dc5-b010-a9a700f2ec1d.

- Abu-Musa, A. (2010). Information Security Governance in Saudi Organizations: An Empirical Study. Information Management and Computer Security, 18(4):226-276.
- Ahmed, S. & Zulhuda, S. (2015). The Concept of internet of Things and Its Challenges to Privacy. South East Asia Journal of Contemporary Business, Economics and Law, 8(4):1-6.
- Allen, J. & Westby, J. (2007). Characteristics of Effective Security Governance. EDPACS: The EDP Audit, Control, and Security Newsletter, 35(5):1-17.
- Boyd, D. (2008). Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence. Convergence: The International Journal of Research into New Media Technologies, 14(1):13-20 .
- Brandão, P. (2018). The Importance of Authentication and Encryption in Cloud Computing Framework Security. International Journal on Data Science and Technology, 4(1):1-5.
- Cohen, F. (1995). A Short History of Cryptography: Introductory Information Protection. Retrieved from http://all.net/edu/curr/ip/Chap2-1.html on 15 May 2022.
- Colnago, J., Delvin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L. & Christin, N. (2018). "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University. CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 21-26 Apr., Montréal, Canada. Paper 456, 1-11.
- Csonka, P. (2000). Internet Crime: The Draft Council of Europe Convention on Cyber-Crime: A Response to the Challenge of Crime in the Age of the Internet?. Computer Law & Security Report, 16(5):329-330.
- Cristofaro, E., Du, H., Freudiger, J. & Norcie, G. (2014). A Comparative Usability Study of Two-Factor Authentication. arXiv:1309.5344v2. https://doi.org/10.48550/arXiv.1309.5344
- Doherty, N. & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. Information Resources Management Journal, 18(2):21-39.

- Durant v Financial Services Authority (2003). EWCA Civ 1746. Retrieved from https://www.5rb.com/case/durant-v-financial-services-authority/ on 17 May 2022.
- Eckhoff, D. & Wagner, I. (2017). Privacy in the Smart City-Applications, Technologies, Challenges and Solutions. IEEE Communications Surveys & Tutorials, 20(1):489-516.
- Elliott, M. (2017). Two-factor authentication: How and why to use it. Rerieved from https://www.cnet.com/tech/mobile/how-and-why-to-use-two-factor-authentication/?openLogin=1 on 29 Apr. 2022.
- Evans, D. (2011). The Internet of Things: How the Next Evolution of the Internet is Changing Everything. Cisco Internet Business Solutions Group (IBSG).
- Federal Financial Institutions Examination Council. (2011). Supplement to Authentication in an Internet Banking Environment. Retrieved from https://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf on 12 May 2022 .
- Fernandez, P. (2014). Privacy and Generation Y: Applying library values to social networking sites. Community & Junior College Libraries, 16(2):100-113.
- Glenn, R. (2003). The Right to Privacy: Rights and Liberties under the Law (America's Freedoms). ABC-CLIO. Retrieved from https://books.google.com.eg/books?id=-4XuJ9-Ma-oC&lpg=PP1&pg=PR30#v=onepage&q&f=false on 20 May 2022.
- Gordon, L. & Loeb, M. (2006). Budgeting Process for Information Security Expenditures. Communications of the ACM, 49(1):121-125.
- Gunson, N., Marshall, D., Morton, H. & Jack, M. (2011). User Perceptions of Security and Usability of Single-Factor and Two-Factor Authentication in Automated Telephone Banking. Computer & Security, 30:208-220.
- Heurix, J., Zimmermann, P., Neubauer, T. & Fenz, S. (2015). A Taxonomy for Privacy Enhancing Technologies. Computers & Security, 53:1-17.
- Isaac, M. & Frankel, S. (2018). Facebook Security Breach Exposes Accounts of 50 Million Users. Retrieved from

https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html?smid=url-share on 5 Mar 2022.

- ISACA. (2012). COBIT 5 for Information Security. ISACA Knowledge Center. Rolling Meadows, USA.
- ISO/IEC 27002:2013, "Information Technology_ Security Techniques_ Code of Practice for Information Security Controls", ISO, 2013. Retrieved from https://www.iso.org/standard/54533.html on 22 May 2022.
- Maarop, N., Mustapha, N., Yusoff, R., Ibrahim, R. & Zainuddin, N. (2015). Understanding Success Factors of an Information Security Management System Plan Phase Self-Implementation. International Journal of Computer and Information Engineering, 9(3):884-889.
- Madden, M. (2012). Privacy Management on Social Media Sites. Pew Research Center's Internet & American Life Project .
- Mannheimer, S., Young, S. & Rossmann, D. (2016). On the Ethics of Social Network Research in Libraries. The Journal of Information Communication, and Ethics in Society, 14.(**2**)
- Mendel, T., Puddephatt, A., Wagner, B., Hawtin, D. & Torres, N. (2012). Global survey on internet privacy and freedom of expression. UNESCO, The United Nations Educational, Scientific and Culture Organization.
- Nath, A. & Mondal, T. (2012). Issues and Challenges in Two Factor Authentication Algorithms. International Journal of Latest Trends in Engineering and Technology, 6(3):318-327.
- Oath. (2012(. About Oath, Initiative for Open Authentication. Retrieved from https://openauthentication.org/about-oath/ on 23 May 2022.
- Savarese, C. & Hart, B. (1999). Historical Cryptography. In The Caesar Cipher, Retrieved from http://www.cs.trincoll.edu/~crypto/historical/caesar.html on 20 May 2022.
- Stanislav, M. (2015) Two-Factor Authentication. IT Governance Ltd, United Kingdom. Retrieved from https://books.google.com.eg/books?id=3EU3DwAAQBAJ&lpg=PA3&dq=Cornelis%20Robat%2C%20(2006%20)%E2%80%9CATM%20(Automatic%20Teller%20Machine)%E2%80%9D%2C%20The%20History%20of%20Computing%20Project&pg=PA78#v=onepage&q=Cornelis%20Robat,%20(2006%

20)%E2%80%9CATM%20(Automatic%20Teller%20Machine)%E2%80%9D,%20The%20History%20of%20Computing%20Project&f=false on 19 May 2022.

- The Guardian. (2014). Any Palestinian is exposed to monitoring by the Israeli Big Brother. Retrieved from https://www.theguardian.com/world/2014/sep/12/israeli-intelligence-unit-testimonies on 17 May 2022.
- Vizcayno, D. (2012). What is Information Security Governance?. Retrieved from https://dcvizcayno.wordpress.com/2012/02/16/what-is-information-security-governance/#:~:text=Information%20security%20governance%20is%20all,defined%20tasks%20and%20oversight%20mechanisms. On 10 May 2022.
- Whitman, M. & Mattord, H. (2017). Principles of Information Security. 6th Ed., Cengage Learning products are represented in Canada by Nelson Education, Ltd.
- Wilkins, A. (2021). Biggest Data Breach 'of all time' leaks Billions of Emails and Passwords. Merto.co.uk, Retrieved from https://metro.co.uk/2021/02/11/biggest-data-breach-of-all-time-comb-has-billions-of-emails-14062987/?ito=article.desktop.share.top.link on 21 May 2022.
- Wozny, M. (2017). Exploitation des données personnelles: raison commerciale, raison d'état et opportunités. Master ARN, Uuniversité De Lyon.
- Zammani, M. & Razali, R. (2016). An Empirical Study of Information Security Management Success Factors. International Journal on Advanced Science Engineering Information Technology, 6(6):904-913.