الجريمة الإلكترونية وانعكاسها على الأمن الاجتماعي للأفراد

دراسة وصفية للنماذج واستراتيجيات المواجهة

Cybercrime and its impact on the social security of individuals: A descriptive study of models and coping strategies

إعداد
الشيماء حسن إسماعيل سرور
مدرس علم الاجتماع
كلية الآداب – جامعة الإسكندرية

ملخص:

هدف البحث وصف طبيعة الجريمة الإلكترونية في عصر تكنولوجيا الاتصالات والمعلومات وانعكاسها على الأمن الاجتماعي للأفراد، حيث أصبحت الجريمة الإلكترونية أكثر انتشاراً، وأوسع نطاقاً، وتعددت أسبابها ودوافعها، كما تشهد معدلات تنذر بالخطر، في ظل تعدد الوسائل التي يتم استخدامها من قبل مرتكبي تلك الجرائم، والتي تنوعت ما بين البرمجيات الخبيثة، والهندسة والشبكات الاجتماعية، وأحصنة طروادة، وبرامج الفدية وغيرها، ويشير الواقع الاجتماعي إلى أن فئة الشباب هي الأكثر عرضة لتلك الجرائم، نظراً لأنها الفئة الأكثر استخداماً لتكنولوجيا الاتصالات والمعلومات، وهو ما يتيح فرصة أكبر لوقوعهم ضحايا للجرائم الإلكترونية، كالتصيد الاحتيالي، والابتزاز والتشهير الإلكتروني، وانتهاكات البريد الإلكتروني، وحقوق الطبع والنشر، وغيرها من الجرائم، التي يكون لها انعكاسات وتأثيرات سلبية على الأمن الاجتماعي للأفراد، وتخلق نوعاً من عدم الثقة في استخدام التكنولوجيا، والتعامل عبر الإنترنت، الأمر الذي يتطلب إستراتيجيات فعالة للوقاية والمواجهة ، ويعد الأمن السيبراني أحد أهم هذه الإستراتيجيات، من خلال دوافع حماية الأفراد لبياناتهم وأنظمتهم الإلكترونية، إلى جانب الحفاظ على أمن بيئة الاتصالات والمعلومات، وتأمين الأجهزة التقنية بما تحتويه من أنظمة وبرامج وبيانات ومعلومات يتم تداولها عبر الإنترنت.

الكلمات المفتاحية : الجريمة الإلكترونية، الأمن الاجتماعي، النماذج، إستراتيجيات المواجهة.

المقدمة:

في ظل ما يشهده العالم من ثورة في الاتصالات والمعلومات، أصبح هناك نوعاً من الاستغلال للإنترنت، والذي عرّض الأفراد والمجتمعات لمخاطر الجريمة الإلكترونية والإرهاب الإلكتروني، ففي عالم التكنولوجيا الرقمية اتسع نطاق فرص ارتكاب الجرائم الإلكترونية، كما فتح الاستخدام المتزايد للإنترنت المجال لظهور بيئة غير آمنة نسبياً، تُمكن مرتكبي الجرائم الإلكترونية من الوصول إلى الضحايا دون قيود جغرافية؛ إذ إن الكثير من الجرائم الإلكترونية ذات ربحية مرتفعة نسبياً.

وتُعد الجريمة الإلكترونية ظاهرة معقدة ومتعددة الأوجه، وتنجم عن مجموعة من الأسباب والعوامل التي ترتبط بسرعة تطور التكنولوجيا وسرعة انتشارها، وانتشار شبكات الإنترنت، وتزايد أعداد مستخدمي تلك الشبكات، وتبني مرتكبي الجرائم الإلكترونية للتقنيات الجديدة، ويدفع هؤلاء المرتكبين لتلك الجرائم إما الكسب المادي، أو الدوافع السياسية، أو دوافع عاطفية، أو الترفيه، وهذه الجرائم تشمل مجموعة واسعة من الأنشطة غير القانونية، مثل التصيد الاحتيالي، والابتزاز، ونشر المعلومات المضللة، والرسائل غير المرغوب فيها، وغيرها من الجرائم الأخرى.

كما تُشكل الجريمة الإلكترونية تهديداً كبيراً للأفراد والمؤسسات والحكومات والمجتمعات عامة، وتتطلب جهوداً مشتركة لمواجهتها، ويظهر بشكل واضح تأثير الجريمة على الأمن الاجتماعي للأفراد، حيث يمكن أن تؤدي إلى فقدان الثقة في التكنولوجيا والأنظمة الرقمية، إلى جانب التأثيرات النفسية والاقتصادية على الضحايا، بالإضافة إلى تأثيراتِها على استقرار المجتمعات وتهديد الأمن القومي.

ومع تزايد التهديدات والجرائم الإلكترونية، أصبح من الضروري وجود إستراتيجيات الأمن السيبراني، لحماية الأنظمة والبيانات الرقمية، من خلال التوعية والتثقيف بمخاطر الجريمة الإلكترونية، وكيفية الوقاية منها، واستخدام تقنيات لحماية البيانات، وبرامج لمكافحة الفيروسات والبرمجيات الخبيثة، وتحديث الأنظمة والبرامج، مع التأكيد على أهمية التعاون الدولي لمكافحة تلك الجرائم، لذا جاء هذا البحث لوصف طبيعة الجريمة الإلكترونية ومدى انعكاسها على الأمن الاجتماعي للأفراد، من خلال التركيز على أهم أسباب ودوافع ارتكاب الجريمة الإلكترونية، إلى جانب عرض أكثر النماذج والجرائم الإلكترونية انتشاراً، والكشف عن مدى تأثير تلك الجرائم على الأمن الاجتماعي للأفراد، وكيفية الوقاية منها.

أولاً: الإطار النظري والمنهجي للبحث

1- الدراسات السابقة :

هناك عدد من الدراسات السابقة التي ترتبط بالجريمة الإلكترونية، والتي من خلالها يمكن تحديد الهدف من البحث الحالي، وهي:

- ***دراسة: (إبراهيم صالح منصور) (2024). " مفهوم الجريمة الإلكترونية وأثرها السلبي على مستخدمي مواقع التواصل الاجتماعي الإنترنت " [1]***

هدفت الدراسة التعرف على تاريخ الجرائم الإلكترونية، ومفهوم الجريمة الإلكترونية، وتقسيمات الجرائم الإلكترونية، والدور الذي يلعبه الإنترنت في ارتكاب تلك الجرائم على مواقع التواصل الاجتماعي، وما هي الصعوبات المتعلقة بمكافحتها ، وتُعد هذه الدراسة من الدراسات الوصفية، التي اعتمدت على المسح الاجتماعي لعينة من أعضاء هيئة التدريس والموظفين والطلبة بكلية الآداب والعلوم جامعة غريان، وقد استخدمت الاستبيان أداةً لجمع البيانات، وقد توصلت الدراسة إلى أن أغلب مستخدمي الانترنت لا يعرفون المعنى الحقيقي للجريمة الإلكترونية، وأن الإنترنت أصبح وسيلة لانتشار وزيادة الجريمة الإلكترونية، ومع تطور تكنولوجيا المعلومات أصبحت هناك أشكالٌ متعددة للجرائم الإلكترونية يصعب اكتشافها.

- ***دراسة: (Abel Yeboah-Ofori) (2023). " الحد من الجرائم الإلكترونية في بيئة تنظيمية متطورة " [2]***

هدفت الدراسة الكشف عن بيئات التهديدات الإلكترونية، والأساليب التي يستخدمها مرتكبو الجرائم الإلكترونية في المؤسسات، والجرائم الإلكترونية المختلفة، ودراسة تأثير الهجمات وتحديد الظروف المختلفة لتحسين ضوابط الأمن في بيئة تنظيمية متطورة ، وتم التوصل إلى أن عدم كفاية جمع معلومات استخبارات التهديدات الإلكترونية، وسوء تكوين الأمن، من العوامل الرئيسة التي تؤدي إلى آثار عملية في التخفيف من حدة الجرائم الإلكترونية، ثم إن للجرائم الإلكترونية عواقب وخيمة على المؤسسات والجهات الخارجية، وللتخفيف من حدة تلك الجرائم، تتطلب إدارة إستراتيجية وتشغيلية باستخدام مراحل للكشف والتحليل والتقييم للجرائم الإلكترونية.

---

[1] إبراهيم صالح منصور، مفهوم الجريمة الإلكترونية وأثرها السلبي على مستخدمي مواقع التواصل الاجتماعي الإنترنت، مجلة ريحان للنشر العلمي، العدد 49، مركز فكر للدراسات والتطوير، سوريا، 2024.

2 Abel Yeboah-Ofori and Francisca Afua Opoku- Boateng, Mitigating Cybercrimes in an Evolving Organizational Landscape, Continuity and Resilience Review, Vol 5, No 1, Emerald Publishing Limited, United Kingdom, 2023.

- ***دراسة: (فريدة بن عمروش، حكيمة جاب الله) (2023). " الجريمة الإلكترونية: المفهوم ، الأشكال والآليات "*** [1]

هدفت الدراسة إبراز ماهية الجريمة الإلكترونية، والتعرف على أهم خصائص تلك الجريمة، واتجاهاتها وأنواعها وآلياتها، وقد توصلت الدراسة إلى أن الجريمة الإلكترونية تختلف عن الجرائم التقليدية، لأنها تُرتكب في البيئة الرقمية، كما تتم باستخدام التقنيات الحديثة، وهي سلوك غير مشروع، وتتعدد أشكالها وأنواعها، فهناك جرائم إلكترونية رسمية، تقوم بها أجهزة ذات علاقة رسمية بالسلطة الحاكمة، وهناك جرائم فردية ماسة بالصالح العام، وتكون بالاعتداء على الحقوق ذات الطابع العام، إلى جانب الجرائم الاقتصادية ،مثل السلع الوهمية، والنصب والاحتيال، وتجارة السوق السوداء، بالإضافة إلى الجرائم ذات التقنيات العالمية، مثل تفكيك الشفرات، ونشر الفيروسات، كما تتعدد آليات ارتكاب تلك الجرائم.

- ***دراسة: (Fatima Al-Zahra Qamqani) (2023). " مفهوم وتطور الجريمة الإلكترونية "*** [2]

هدفت الدراسة التعرف على مفهوم الجريمة الإلكترونية، والجوانب السلبية للتقنية الحديثة، وتأثيرها على الانتشار السريع للجريمة الإلكترونية، وقد توصلت الدراسة إلى أن هناك عدة عوامل ساعدت على تطور انتشار الجريمة الإلكترونية، منها العولمة، وانتشار تكنولوجيا المعلومات واللامعيارية (ضعف القيم الاجتماعية)، والفقر، والبطالة، والاستبعاد الاجتماعي، ووقت الفراغ، ومن أهم خصائص الجرائم المعلوماتية، سرعة التنفيذ، والتنفيذ عن بُعد، وإخفاء الجريمة، والجاذبية، وكونها عابرة للدول، كما تتنوع الجرائم الإلكترونية ما بين جرائم تتم ضد الحواسب الآلية ونظم المعلومات، وجرائم تتم باستخدام الحواسب الآلية.

- ***دراسة: (Naci Akdemir and Christopher James Lawless) (2020). " استكشاف العامل البشري في وقوع ضحايا الجرائم الإلكترونية: نهج قائم على الأنشطة الروتينية لأسلوب الحياة "*** [3]

هدفت الدراسة استكشاف العوامل البشرية باعتبارها عاملاً مُيسراً محتملاً للوقوع ضحية للجرائم الإلكترونية، واختبار مدى تطبيق نظرية الأنشطة الروتينية لأسلوب الحياة على وقوع الضحايا للجرائم الإلكترونية، وقد توصلت الدراسة إلى أن مستخدمي الإنترنت سهلوا من وقوعهم ضحية للجرائم الإلكترونية

---

[1] فريدة بن عمروش، حكيمة جاب الله، الجريمة الإلكترونية: المفهوم، الأشكال والآليات، المجلة العلمية للتكنولوجيا وعلوم الإعاقة، المجلد 5 ، العدد 4، المؤسسة العلمية للعلوم التربوية والتكنولوجية والتربية الخاصة، الجزائر، 2023.

[2] Fatima Al- Zahra Qamqani ، مفهوم وتطور الجريمة الإلكترونية، المجلة الأردنية الدولية أريام للعلوم الإنسانية والاجتماعية، المجلد 5، العدد 3، مركز أريام للبحوث والدراسات، الأردن، 2023.

3 Naci Akdemir and Christopher James Lawless, Exploring The human factor in Cyber-enabled and Cyber-dependent Crime Victimization: a Lifestyle Routine Activities Approach, Internet Research, Vol 30, No 6, United Kingdom, 2020.

من خلال أنشطتهم على الإنترنت، وبرز استخدام اتصالات الإنترنت غير الآمنة وأجهزة الكمبيوتر العامة كعوامل خطر للوقوع ضحية للجرائم الإلكترونية بالإضافة إلى زيادة الكشف الطوعي وغير الطوعي عن المعلومات الشخصية عبر مواقع التواصل الاجتماعي ومواقع الاعلانات الإلكترونية، وظهرت أنشطة إلكترونية مثل البث المجاني أو مشاركة الملفات، والتي زادت من خطر الوقوع ضحية للجرائم الإلكترونية.

- ***دراسة: (Kristjan Kikerpill) (2020). "دور الفرد في منع الجرائم الإلكترونية: مجالات الحماية الداخلية وقدرتنا على حمايتها " [1]***

هدفت الدراسة توضيح كيفية تَوَجب إرشاد المسئوليات العامة بوضع احترازات من قبل الأفراد لحماية ما يقدرونه بشكلٍ كافٍ، حيث تسعى إلى صياغة دور الفرد في الوقاية من الجرائم الإلكترونية، وتشرح كيف أوجدت المسئولية حاجة حتمية لتزويد الأفراد بالمعرفة، والأدوات اللازمة لتجنب الوقوع ضحية لتلك الجرائم، وقد توصلت الدراسة إلى أهمية إعادة صياغة دور الفرد في منع الجرائم الإلكترونية، بحيث يصبح ذا أهمية وكفاءة، ثم إن السلطات العامة لا تستطيع بمفردها الحد من ضغط مجرمي الإنترنت، وبالتالي ثمة حاجة إلى نهج يبدأ بالأفراد ودوافعهم، للحماية من الجرائم الإلكترونية، وتتخذ المعرفة الإلكترونية نقطة انطلاق نحو هذه الحماية .

- ***دراسة: (لامية طالة، كهيذة سلام) (2020). " الجريمة الإلكترونية: بُعد جديد لمفهوم الإجرام عبر منصات التواصل الاجتماعي " [2]***

هدفت الدراسة التعرف على الجريمة الإلكترونية، والمجرم الإلكتروني، وخصائص الجريمة الإلكترونية، وأهدافها، وأهم تأثيراتها على نفسية الفرد وقيم المجتمع، وقد توصلت الدراسة إلى أن التشابه بين الجريمة الإلكترونية والجريمة التقليدية، يتمثل في أن مرتكب الجريمة لديه الدافع لارتكاب الجريمة، في حين أن الاختلاف بين نوعي الجريمة، يكون في أن الجريمة الإلكترونية ذات تقنية عالية، ولا تتطلب انتقال الجاني إلى مكان الجريمة، وأصبحت الجرائم الإلكترونية تهدد قيم المجتمع، وتهدد الأمن القومي، ويتوجب مواجهتها مشاركة من جانب الدول والأفراد .

- ***دراسة: (Jacqueline M. Drew) (2020). " دراسة حول ضحايا الجرائم الإلكترونية والوقاية منها: استكشاف استخدام سلوكيات وإستراتيجيات الوقاية من الجرائم الإلكترونية " [1]***

1 Kristjan Kikerpill, The Individual's Role in Cybercrime Prevention: Internal Spheres of Protection and our Ability to Safe Guard Them, Kubernetes, Vol 50, No 4, Emerald Publishing Limited, United Kingdom, 2021

2 لامية طالة، كهيذة سلام، الجريمة الإلكترونية: بُعد جديد لمفهوم الإجرام عبر منصات التواصل الاجتماعي، مجلة الرواق للدراسات الاجتماعية والإنسانية، المجلد 6، العدد 2، المركز الجامعي أحمد زبانة غليزان، مخبر الدراسات الاجتماعية والنفسية والأنثروبولوجية، الجزائر، 2020.

هدفت الدراسة استكشاف تجربة التعرض للضحية والتصورات حول الجرائم الإلكترونية، واستخدام إستراتيجيات الوقاية منها، وقد شملت الدراسة استطلاعاً لعينة تمثيلية من السكان الأستراليين البالغين، وبلغت (595) مشاركاً، وقد توصلت الدراسة إلى أن هناك علاقة بين وقوع الضحايا للجرائم الإلكترونية وإستراتيجيات الحماية الذاتية عبر الإنترنت، وأن التعرض للجرائم الإلكترونية سابقاً يرتبط بزيادة استخدام إستراتيجيات الحماية الذاتية والوقاية من تلك الجرائم، حيث يستخدم الفرد إستراتيجيات تجعل التعرض للجرائم الإلكترونية أكثر صعوبة، إلى جانب أن بعض الأفراد يجهلون أنواع إستراتيجيات الحماية الذاتية التي ينبغي عليهم استخدامها، وقد يرجع ذلك إلى صعوبة الوصول إلى معلومات حول كيفية حماية النفس عبر الانترنت .

- ***دراسة: (بو مامي العباس) (2015). " الجريمة الإلكترونية نتاج أجهزة ومواقع تواصل اجتماعي " [2]***

هدفت الدراسة إلى الإجابة عن مدى إمكانية أن تكون بعض البرامج والأجهزة دافعا قوياً لارتكاب المجرمين لجرائمهم الإلكترونية، وهل بعض مواقع التواصل الاجتماعي متورطة في ارتكاب بعض الجرائم الإلكترونية ؟ ، وتعد هذه الدراسة من الدراسات الوصفية التحليلية، وقد توصلت الدراسة إلى أن الجريمة الإلكترونية نتاج لأجهزة وبرامج إلكترونية، بالإضافة إلى أن بعض مواقع التواصل الاجتماعي كالفيسبوك وجوجل لها يد في حدوث بعض الجرائم المعلوماتية، من خلال تورطها في التلاعب ببيانات المستخدمين، والمتاجرة بها، أو القيام بالإشهار من خلال برامج وبرمجيات مشبوهة، لا هدف من ورائها غير الربح المادي.

التعقيب على الدراسات السابقة:

من خلال إلقاء الضوء على الدراسات السابقة نلاحظ أنها تناولت الجريمة الإلكترونية، والمجرم الإلكتروني، وتاريخ الجرائم الإلكترونية، وتقسيماتها، وبيئات التهديدات الإلكترونية، واستكشاف العوامل البشرية باعتبارها عاملاً مُيسراً للوقوع ضحية للجرائم الإلكترونية، وما يتوجب من دعم المسئوليات العامة

1 Jacqueline M. Drew, A Study of Cybercrime Victimization and Prevention: Exploring The use of Online Crime Prevention Behaviors and Strategies, Journal of Criminological Research, Policy and Practice, Vol 6, No 1, United Kingdom, 2020.

2 بو مامي العباس، الجريمة الإلكترونية نتاج أجهزة ومواقع تواصل اجتماعي، مجلة جيل العلوم الإنسانية والاجتماعية، العدد 12، مركز جيل البحث العلمي، الجزائر، 2015.

وتوعيتها للفرد بدوره في الوقاية من الجريمة الإلكترونية، واتجاهات الجريمة الإلكترونية، والجوانب السلبية للتقنية الحديثة، وتأثيرها على انتشار تلك الجرائم وصعوبات مكافحتها.

وقد أشارت نتائج الدراسات إلى أن الجريمة الإلكترونية نتاج للأجهزة والبرامج الإلكترونية، بالإضافة إلى دور بعض وسائل التواصل الاجتماعي في انتشار تلك الجرائم، وتتشابه الجريمة الإلكترونية مع الجريمة التقليدية، في أن مرتكب الجريمة لديه دافع لارتكاب الجريمة، في حين أن الاختلاف بين نوعي الجريمة، أن الجريمة الإلكترونية تكون ذات تقنية عالية. وتنقسم الجرائم إلى جرائم إلكترونية رسمية تقوم بها أجهزة ذات علاقة بالسلطة، وجرائم فردية ماسة بالصالح العام، كما أن أغلب مستخدمي الإنترنت لا يعرفون المعنى الحقيقي للجريمة الإلكترونية، رغم أن الإنترنت أصبح وسيلة لانتشار تلك الجرائم، وتُعد العولمة من العوامل التي ساعدت على انتشار الجريمة الإلكترونية، وجعلها عابرة للدول، ويُعد التعرض المسبق للجرائم الإلكترونية أحد الدوافع لاتخاذ الأفراد آليات للوقاية من تلك الجرائم، كما أن هناك دوراً هاماً للأفراد في التصدي لها.

لذلك جاء هذا البحث ليقدم مساهمة جديدة في مجال الجريمة الإلكترونية، من خلال التعرف على أهم أسباب ودوافع تلك الجرائم، والنماذج الأكثر انتشاراً للجرائم الإلكترونية، ومدى انعكاس هذه الجرائم على الأمن الاجتماعي للأفراد، بالإضافة إلى الكشف عن إستراتيجيات الأمن السيبراني، كآلية للوقاية والمواجهة للجرائم الإلكترونية، وأهم معوقات التعاون الدولي في هذا المجال.

وفي ضوء عدم وضوح الاتجاه النظري في أغلب الدراسات السابقة، فقد اهتم هذا البحث بالاعتماد على توجه نظري، يمكن من خلاله تفسير موضوع البحث، تمثل هذا التوجه النظري في نظريتي **"دوافع الحماية"** و **"الأنشطة الروتينية لأسلوب الحياة"** حيث تقدم نظرية **"دوافع الحماية"** إطاراً نظرياً يفسر سلوكيات الأفراد للتكيف مع التهديدات، فدوافع الأفراد لحماية أنفسهم من تهديدات الجرائم الإلكترونية ترتبط بشكلٍ أساسٍ بتقييمهم لتلك التهديدات، وتأثيراتِها السلبية، في حين أن نظرية **"الأنشطة الروتينية لأسلوب الحياة"** تشير إلى أن الأنشطة اليومية للأفراد، مثل استخدامهم المتزايد لتكنولوجيا الإنترنت قد يزيد من احتمال تعرضهم لتهديدات الجرائم الإلكترونية.

2- إشكالية البحث:

لقد شهدت الجرائم الإلكترونية تزايداً هائلاً، واتسع نطاق تأثيرها على الأفراد، وتصاعدت تعقيدات الهجمات الإلكترونية، خاصةً في ظل الاعتماد المتزايد على تكنولوجيا الاتصالات والمعلومات، والوصول السريع إلى الإنترنت، الأمر الذي جعل الخدمات الإلكترونية أكثر عرضةً للهجمات، وأمكن ارتكاب الكثير من الجرائم ، وفي ظل تزايد هذه الجرائم أصبحت المجتمعات تعيش حالة من الاضطرابات، ويشعر الأفراد بحالة من انعدام الأمن الاجتماعي، واتساع مجال التهديدات الأمنية التي نتج عنها تغير في حياة الأفراد.

ورغم أهمية تكنولوجيا الاتصالات والمعلومات، والفوائد التي تقدمها تلك التكنولوجيا، إلا أنها تجلب معها الكثير من التهديدات، نظراً لأن الجرائم الإلكترونية المرتبطة بهذه التكنولوجيا معقدة في التعامل معها، وتتسم بأنهاعابرة للحدود، ويتم تنظيمها بفعالية كبيرة، وغالباً ما يستغل مرتكبو تلك الجرائم نقاط الضعف التنظيمية الخاصة بتكنولوجيا الاتصالات والمعلومات، وهذا مما يساعد في تطوير قدرات عمل هؤلاء المجرمين على نطاق عالمي، ويمكنهم من نقل أنشطتهم من بلدٍ إلى آخر بسهولة.

وتُعد المشكلة الأكبر فيما يتعلق بالجرائم الإلكترونية، هي عدم وعي الكثير من الأفراد بأنواع الجرائم الإلكترونية، إذ يدرك البعض أنهم ضحايا بعد وقوع الجريمة، وقد لا يدركون ذلك أبداً، وبذلك يستغل مرتكبو الجرائم الإلكترونية ضعف وجهل بعض المستخدمين لارتكاب جرائمهم.

ومن ثم تتطلب معالجة الجرائم والتهديدات الإلكترونية نهجاً تعاونياً، يشمل التكنولوجيا وإنفاذ القانون والتعليم الإلكتروني لتعزيز الأمن السيبراني، ومع تطور تلك الجرائم تُعد الإستراتيجيات الفعالة ضرورة لحماية المجتمع الإلكتروني، وتخفيف المخاطر، وبالتالي يُمثل تعزيز تدابير الأمن السيبراني أمراً بالغ الأهمية لاستعادة الثقة في الخدمات الالكترونية، وحماية الأفراد من الجرائم الإلكترونية ومخاطرها ، مع الأخذ في الاعتبار أن تحقيق الوضع المثالي لبيئة رقمية آمنة من الجرائم الإلكترونية أمراً صعباً، في حالة عدم إدراك الأفراد للمعلومات الكاملة حول التهديدات الإلكترونية، ومن ثم فالإستراتيجيات الوقائية تتطلب أولا معرفة الأفراد وإدراكهم للتهديدات، وبالتالي النظر إلى التدابير والاجراءات الأكثر فعالية.

وفي ضوء ما سبق تتحدد القضية الرئيسة للبحث في :

(مدى انعكاس الجريمة الإلكترونية على الأمن الاجتماعي للأفراد)

3- أهمية البحث :

لقد أصبحت تكنولوجيا الاتصالات والمعلومات جزءًا لا يتجزأ من حياة الغالبية من الأفراد، وتزامنت التطورات التكنولوجية مع تزايد المخاوف بشأن الجرائم الإلكترونية، وتأثيراتها على الأمن الاجتماعي للأفراد .

ومن ثم يمكن بيان أهمية هذا البحث من خلال :

- **الأهمية النظرية :**

تتضح أهمية هذا البحث في ظل التغيرات التي يشهدها العالم سواءً على المستوى العالمي أو المحلي، خاصة التحولات في عالم تكنولوجيا الاتصالات والمعلومات، وما يتبعها من تحديات وسلبيات تمثل خطورة على المجتمع والحياة الاجتماعية والأمنية للأفراد، فقد خلق المجتمع الرقمي والمعلوماتي فرصاً أكبر لمزيد من الجرائم التي تقوم على التقنية العالية، الأمر الذي يتطلب مزيداً من الاهتمام بالكشف عن الجرائم الإلكترونية الأكثر انتشاراً، ومدى تأثيرها على الأمن الاجتماعي للأفراد.

ومن ثم تتزايد أهمية هذا البحث من خلال تناوله لأهم أسباب ودوافع الجرائم الإلكترونية، وأكثر نماذج هذه الجرائم انتشاراً، وانعكاسها على الأمن الاجتماعي، وكيفية الوقاية منها ومواجهتها من خلال إستراتيجيات الأمن السيبراني.

- **الأهمية التطبيقية :**

إن تزايد معدلات الجرائم الإلكترونية يخلق نوعاً من عدم الأمن لدى الأفراد، وعدم الثقة في التعامل مع تكنولوجيا الاتصالات والمعلومات، والتعامل بشكل عام مع الانترنت، ومن خلال هذا البحث يتمكن الأفراد من الوصول إلى معرفة أكبر فيما يتعلق بأكثر أنواع الجرائم الإلكترونية، التي من المحتمل أن يتعرضوا لها، ومن ثم كيفية التعامل معها، إلى جانب مساعدة الحكومات والهيئات الدولية والهيئات المسئولة عن المواقع الإلكترونية في الكشف عن أسباب انتشار بعض أنواع الجرائم الإلكترونية، ومدى تأثيرها على الأفراد، من خلال رؤية الأفراد في الواقع الاجتماعي، حيث تساعد رؤية الواقع الاجتماعي في التعرف على أهم الآليات والإستراتيجيات الأكثر فعالية في مواجهة تلك الجرائم والوقاية منها.

كما يساعد البحث في تطوير حملات تثقيفية وتوعوية أكثر فعالية، لمواجهة الجرائم الإلكترونية، والتخفيف من مخاطرها نظراً لأن الوعي بمخاطر الجرائم الإلكترونية، يساعد على تغيير مسار ضحايا تلك

الجرائم، وبالتالي يمكن للسلطات العامة تقديم المزيد من الدعم، لحماية الأفراد من الجرائم الإلكترونية، وتحقيق الأمن الاجتماعي لهم.

4- هدف البحث وتساؤلاته :

يتمثل الهدف الرئيس للبحث في (***وصف طبيعة الجريمة الإلكترونية وانعكاسها على الأمن الاجتماعي للأفراد***) ويمكن تحقيق هذا الهدف من خلال الإجابة على عدد من التساؤلات التي تتمثل في:

- ✓ ما أسباب ودوافع الجريمة الإلكترونية ؟
- ✓ ما أكثر نماذج الجرائم الإلكترونية انتشاراً ؟
- ✓ كيف تؤثر الجريمة الإلكترونية على الأمن الاجتماعي للأفراد ؟
- ✓ ما أهم إستراتيجيات مواجهة الجريمة الإلكترونية ؟

5- مفاهيم البحث :

يشتمل البحث على عدداً من المفاهيم الرئيسة التي تتمثل في :

- **الجريمة الإلكترونية:** Cyber Crime

تشير "الجريمة الإلكترونية" إلى الجرائم المرتكبة باستخدام بيانات الاتصالات، أو اتصالات الإنترنت، وهذه الأشكال من الجرائم في جوهرها سلوكيات غير مشروعة، تتضمن نظاما حاسوبياً، ومع تطور الإنترنت تزايد حجم الجرائم الإلكترونية أيضاً، ولم يعد وجود المجرم ضروريا في مكان الجريمة أثناء ارتكابها، وقد لا يكون هناك تواصل وثيق بين الضحية والمجرم، وهي سمة فريدة لمجرمي الإنترنت.[1]

وتتضمن الجريمة الإلكترونية الوصول غير المصرح به إلى معلومات حساسة، خاصة بأفراد، أو شركات، أو هيئات، لتحقيق مكاسب شخصية، ويحدث هذا أينما وجد اتصال حاسوبي داخل الفضاء

1 Kuldeep Singh Kaswan and Others, Cybersecurity Law-Based Insurance Market, Emerald Group Publishing Limited, United Kingdom, 2022, p 310.

الإلكتروني، ووسائل الاتصالات والمعلومات، وبالتالي فالجريمة الإلكترونية هي عمليات غير قانونية، ترتكب داخل الفضاء الالكتروني، وباستخدام وسيلة إلكترونية، وتشتمل على العديد من الاختراقات.[1]

كما تعرف (شبكة إنفاذ الجرائم المالية في الولايات المتحدة الأمريكية) (FinCEN) الجريمة الإلكترونية أو "الجرائم الممكنة إلكترونيا" بأنها: "أنشطة غير قانونية، مثل الاحتيال، وغسل الأموال، وسرقة الهوية، تنفذها أو تسهلها أنظمة وأجهزة إلكترونية، مثل الشبكات وأجهزة الحاسوب".[2]

وقد عرفت (منظمة التعاون الاقتصادي والتنمية) (OCDE) الجريمة الإلكترونية بأنها: "كل سلوك غير مشروع، أو غير أخلاقي، أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو نقلها".[3]

ومن الجدير بالذكر الإشارة إلى أن هناك عدة مسميات للجريمة الإلكترونية، منها (الجرائم المعلوماتية، جرائم الكمبيوتر، جرائم التقنية العالمية، جرائم الهاكرز، جرائم الإنترنت، الإجرام في الفضاء الخيالي، الجرائم عبر شبكات الاتصال عن بعد).[4]

التعريف الإجرائي:

يُستخدم مفهوم "الجريمة الإلكترونية" ليشير إلى جميع أشكال الاحتيال المشبوهة، التي يستخدمها المجرمون لاستهداف الأشخاص مستخدمي الإنترنت والفضاء الإلكتروني، لسرقة أموالهم وبياناتهم الشخصية ، وابتزازهم .

ويمكن قياس الجريمة الإلكترونية من خلال عدة مؤشرات، يتمثل أهمها في:

1- معدل انتشار الجرائم الإلكترونية.

2- عدد الجرائم الإلكترونية المبلغ عنها.

3- أنواع الجرائم الإلكترونية الأكثر شيوعاً.

4- الخسائر المادية والاجتماعية الناتجة عن الجرائم الإلكترونية.

5- معدلات الكشف عن الجرائم الإلكترونية.

- **الأمن الاجتماعي :** Social Security

1 Oluwatoyin Esther Akinbowale and others, Analysis of Cyber-Crime Effects on The banking Sector Using The Balanced Score Card: a Survey of Literature, Journal of Financial Crime, Vol 27, No 3, United Kingdom, 2020, p 951.

2 Tanya Gibbs, Seeking Economic Cyber Security: a Middle Eastern Example, Journal of Money Laundering Control, Vol 23 No 2, United Kingdom, 2020, p 495.

3 خالد علي الجنيبي، الجريمة الإلكترونية بين تحديات الواقع واستشراق المستقبل، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية- ICACC، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، السعودية، 2015، ص 82.

4 نوال كروش، بحث في إشكالات الجريمة الإلكترونية، المجلة الجزائرية للدراسات الإنسانية، المجلد 2، العدد 2، جامعة وهران أحمد بن بلة، الجزائر، 2021، ص 221.

يشير "الأمن الاجتماعي" من منظور علم الاجتماع إلى أقصى إشباع ممكن لاحتياجات الجماهير، في إطار العدالة الاجتماعية التي تنبذ الصراع بين فئات المجتمع، وتوفر المناخ الملائم، لكي يعيش المجتمع في إطار مقبول من التقبل والتعاون والشعور بالأمن والسلام الاجتماعي، ويتمحور الأمن الاجتماعي حول محورين:

١- المحور الأول (العامل الأمني): الذي يهتم بتحرير الفرد والمجتمع من الخوف وعدم الاستقرار المعنوي والمادي.

2- المحور الثاني (العامل الاقتصادي والاجتماعي والسياسي): الذي يُعنَى بتحقيق متطلبات الحياة العاملة من رفاهية اقتصادية وتنمية وتطوير.[1]

كما يقصد بالأمن الاجتماعي الحالة التي يكون فيها الإنسان محمياً أو بعيداً عن خطر يهدده، ويتمثل في حالة الهدوء والاستقرار والوئام والاتفاق والانسجام، داخل المجتمع الإنساني نفسه، وفي العلاقة بين شرائحه وأفراده، وقواه المتعددة المختلفة.[2]

التعريف الإجرائي:

يشير مفهوم "الأمن الاجتماعي" إلى حماية الأفراد من المخاطر، والآثار السلبية للجرائم الإلكترونية، والتي تهدد رفاهيتهم واستقرارهم الاجتماعي والنفسي، وشعورهم بالأمن والثقة في استخدام تكنولوجيا الاتصالات والمعلومات.

ويمكن قياس الأمن الاجتماعي من خلال عدة مؤشرات، يتمثل أهمها في:

1- مستوى الرضا عن الحياة لدى الأفراد والعلاقات الاجتماعية.

2- مستوى الشعور بالاستقرار والأمان الاجتماعي والنفسي.

3- مستوى الثقة في الأنشطة الإلكترونية والمؤسسات الحكومية والأمنية.

4- مستوى القلق من التكنولوجيا.

5- معدل الجريمة الإلكترونية.

- **الأمن السيبراني:** Cyber Security

[1] أحمد حسن عبد الله، صفاء كريم جواد، الأمن الاجتماعي ومقوماته: دراسة نظرية تحليلية، مجلة جامعة بابل- العلوم الإنسانية، المجلد 30، العدد 3، جامعة بابل، العراق، 2022، ص 4.

[2] إبراهيم بن مبارك بن موسى الجوبر، تحقيق الأمن الاجتماعي، المجلة العربية للآداب والدراسات الإنسانية، المجلد 8، العدد 33، المؤسسة العربية للتربية والعلوم والآداب، مصر، 2024، ص ص 150، 151.

يشير "الأمن السيبراني" إلى عملية حماية البيانات، وخوادم الشبكات، والأنظمة الإلكترونية، والأجهزة المحمولة، وما إلى ذلك، ويعرف أيضا باسم أمن تكنولوجيا المعلومات، وأمن المعلومات الإلكترونية.[1]

ويُعد الأمن السيبراني جهداً لحماية الفضاء الإلكتروني من التهديدات الداخلية والخارجية للمتسللين والمجرمين والمتعدين، وغيرها من نقاط الضعف، التي قد تنشأ عن أي اقتحام غير مصرح به للبيانات الحيوية الوطنية، أو أي هجوم على البنية التحتية الحيوية، وبالتالي فالأمن السيبراني هو جميع البرامج والسياسات والقوانين المصممة لحماية الفضاء الإلكتروني من أي اختراق غير مصرح به.[2]

كما يعرف الأمن السيبراني بأنه حماية الشبكات والبيانات والمعلومات المرتبطة بالإنترنت من التهديدات، التي من الممكن أن تلحق بها، ومحاولة الوقوف على التحديات التي تعترض توفير الحماية للمعلومات المتواجدة في الأوساط الإلكترونية، ومصطلح "سيبراني" مشتق من كلمة "سايبرcyber" وتعني "كل ما يتعلق أو يرتبط بالحواسيب وتكنولوجيا المعلومات والواقع الافتراضي".[3]

وبالتالي يعرف الأمن السيبراني بأنه: "حماية الفضاء الإلكتروني نفسه، والمعلومات الإلكترونية ، وتقنيات المعلومات والاتصالات التي تدعمه، ومستخدميه بصفتهم الشخصية والمجتمعية والوطنية، بما في ذلك أي من مصالحهم، سواء كانت ملموسة أو غير ملموسة، والتي تكون عرضة للهجمات الناشئة في الفضاء الإلكتروني.[4]

التعريف الإجرائي:

يستخدم مفهوم "الأمن السيبراني" ليشير إلى الإجراءات والممارسات والآليات، التي تهدف إلى حماية الأنظمة والبرامج والشبكات المعلوماتية، ومنع أي تدخل غير مشروع أو غير مصرح به لاستخدام البيانات والمعلومات الخاصة بالأفراد، وبالتالي حمايتهم من الأذى عبر الإنترنت، وتأمينهم من الوقوع ضحايا للجرائم الإلكترونية.

ويمكن قياس الأمن السيبراني من خلال عدة مؤشرات، يتمثل أهمها في:

1- مستوى الامتثال للمعايير واللوائح الأمنية الخاصة بمكافحة الجريمة الإلكترونية.

---

1 Magnus Osahon Igbinovia and Bolan Le Clifford Ishola, Cyber Security in University Libraries and Implication for Library and Information. Science Education in Nigeria, Digital Library Perspectives, Vol 39, No 3, United Kingdom, 2023, p 249.

2 Babayo Sule and Others, Countering Cyber crimes as The Strategy of Enhancing Sustainable Digital Economy in Nigeria, Journal of Financial Crime, vol 30, No 6, United Kingdom, 2023, p 1559.

3 بدر الحيمودي، الأمن السيبراني وحماية الأنظمة المعلوماتية، مجلة المنارة للدراسات القانونية، العدد 46، المغرب، 2023، ص ص 47، 48.

4 Nourin Farooq and Others, Explanatory and Predictive Analysis of Smartphone Security Using Protection Motivation Theory: a Hybrid SEM-AI Approach, Information Technology and People, ITP, United Kingdom, 2024, p ITP.

2- مدى الالتزام باستخدام تقنيات حماية البيانات وبرامج مكافحة الفيروسات.

3- تحديث الأنظمة والبرامج بانتظام.

4- مستوى وعي الأفراد بمخاطر الجريمة الإلكترونية.

6- التوجه النظري للبحث :

يعتمد البحث على مدخلين نظريين هما نظرية **"دوافع الحماية"** ونظرية **"الأنشطة الروتينية لأسلوب الحياة"**، ويمكن عرضهما على النحو التالي:

- **المدخل الأول :** نظرية **" دوافع الحماية "** (PMT) (Protection Motivation Theory)

ترتبط هذه النظرية بأعمال **"روجرز"**، وتتضمن عدداً من المفاهيم والمسلمات وبعض القضايا النظرية التي طرحتها، والتي جاءت على النحو التالي:

أ- المفاهيم :

تشتمل نظرية "دوافع الحماية" على عدد من المفاهيم، يتمثل أهمها في:

1- دافع الحماية : Protection Motivation

يشير مفهوم دافع الحماية إلى أن دافع الأفراد إلى حماية أنفسهم من المخاطر، ينبع من تقييم التهديدات، والاختيار بين بدائل المواجهة، بالإضافة إلى ذلك، يتلقى الأفراد معلومات من مصادر مختلفة، مثل الاقتناع اللفظي، أو التعلم الملاحظ أو الخبرة السابقة، ويستخدم الأفراد هذه المعلومات لدعم تقييمهم للمخاطر، واتخاذ التدابير والقرارات اللازمة وفقا لذلك.[1]

2- الفعالية الذاتية : Self- Efficacy

تُعرف الفعالية الذاتية بأنها إيمان الفرد بقدرته وجهده، لتحقيق رد الفعل التكيفي بنجاح، وإيمان مستخدمي تكنولوجيا المعلومات بقدرتهم على حماية تفضيلات البحث الإلكتروني الخاص بهم وبياناتهم، والحد من الكشف عن بياناتهم الشخصية.[2]

1 Hao Chen and Yufei Yuan, The Impact of Ignorance and Bias on Information Security Protection Motivation: a Case of E-Waste Handling, Internet Research, vol 33, No 6, United Kingdom, 2023، p 2245.

2 Andreas Skalkos and Others, Exploring Users Attitude Toward S Privacy-Preserving Search Engines: aprotection Motivation Theory Approach. Information and Computer Security, Vol 32, No 3, United Kingdom, 2024, p 329.

3- تقييم التهديد : Threat Appraisal

يشير تقييم التهديد إلى مراعاة الأفراد احتمالية وحجم الضرر الناجم عن خطر معين، ومدى اعتقاد الفرد بخطورة عواقب التهديد "الخطورة المتصورة"، واحتمالية تأثير التهديد سلباً "الضعف المتصور"، ومدى فعالية الاستجابة في مواجهة التهديدات "الكفاءة الذاتية"، والتكاليف المترتبة على تطبيق تدابير التكيف "تكلفة الاستجابة".[1]

ب- المسلمات :

تعتمد نظرية "دوافع الحماية" على عدد من المسلمات، تتمثل في:

1- يستند تصور الفرد المتعلق بشدة أي تهديد إلى مدى الخوف من هذا التهديد.

2- لشده التهديد المدركة وقابلية التعرض للتهديد علاقة إيجابية مع البيئة السلوكية لتجنب الضرر الناتج عن التهديد الإلكتروني.[2]

3- كلما شعر المستخدمون لتكنولوجيا المعلومات بالتهديد، فإنهم يُلزمون أنفسهم بسلوك الحماية الذاتية.

4- مستخدمو تكنولوجيا الاتصالات والمعلومات يميلون أكثر إلى اتخاذ تدابير وقائية عندما يعتبرون أن إساءة استخدام البيانات تشكل خطراً أشد وأنهم أكثر عرضة لهذا الخطر.[3]

5- الأفراد سيحمون أنفسهم من مستوى كافٍ من التهديد الجسدي أو النفسي أو الاجتماعي.

6- خوف الأفراد يكون محفزاً لتقييم التهديدات التي من الممكن التعرض لها.[4]

جـ - القضايا النظرية :

تقوم نظرية "دوافع الحماية" على عدد من القضايا النظرية، يتمثل أهمها في:

1- السلوكيات التكيفية لمواجهة التهديدات :

تفترض نظرية "دوافع الحماية" أنه عندما يواجه الشخص تهديداً، فإنه يقيمه فكرياً (شدة التهديد وقابلية التعرض له)، ويحدد العلاج المتاح له، وبعد تحليل التهديدات وتقييمات التأقلم، يتصرف الشخص إما بطريقه تكيفية أو بطريقة غير تكيفية (السلوكيات غير التكيفية هي تلك التي يتجنب فيها

1 Hao Chen and Yufei Yuan, The Impact of Ignorance and Bias on Information Security Protection Motivation: a Case of E-Waste Handling, Op Cit، p 2247.

2 Hassan Jamil and Others, Human-Centric Cyber Security: Applying Protection Motivation Theory to Analyze Micro Business Owners' Security Behaviors, Information and Computer Security, Vol 33, No 1, United Kingdom, 2025, p 58.

3 Andreas Skalkos and Others, Exploring Users Attitude Towards Privacy-Preserving Search Engines: aprotection Motivation Theory Approach, Op Cit, p 322.

4 Megan C. Good and Michael R. Hyman, Protection Motivation Theory and Brich-and-Mortar Sales People, International Journal of Retail and Distribution Management, Vol 48, No 8, United Kingdom, 2020, pp 869, 780.

الفرد القيام باستجابة موصي بها، والسلوكيات التكيفية هي الاستجابات الموصي بها لمواجهة التهديد)، ويحدد تقييم التهديد وتصورات الفرد حول شدة التهديد ومدى التعرض للتهديد، وبالتالي بعد تقييم التهديد يستخدم الشخص الأدوات المتاحة للتعامل معه، وتشتمل تقييمات التكيف على:

- الكفاءة الذاتية: هي اعتقاد الشخص وقدرته على التعامل مع التهديد بفاعلية.
- فعالية الاستجابة: هي تصور الشخص لمدى قدرته على تنفيذ الاستجابة الموصي بها لمواجهة التهديد.
- تكاليف الاستجابة: هي إدراك الفرد للتكاليف مثل (الوقت، والجهد، والمال، وما إلى ذلك...) لمواجهة التهديد.[1]

2- الجهل وتقييم التهديدات :

يمثل الجهل هنا غياب المعرفة بتهديد أمن المعلومات، فالأشخاص الذين يفتقرون إلى المعرفة بالتهديدات والمخاطر الإلكترونية، لن يتمكنوا من معرفة التهديدات والأضرار المحتملة، ولن يستجيبوا لها بشكل مناسب، فالذي يفتقر إلى المعرفة الفعلية بتهديدات أمن المعلومات سيصدر حكماً غير صائب بشأن هذه التهديدات، وبالتالي يؤثر الجهل الفعلي سلباً على التهديد المتصور، في حين أن المعرفة تؤثر ايجاباً على فعالية استجابة الفرد في مواجهة تهديدات أمن المعلومات المحتملة، كما تؤثر الخبرة السابقة في ممارسات أمن المعلومات على فاعلية الاستجابة في مجال الأمن السيبراني، وهنا يجدر الإشارة إلى أنه كلما زادت خبرة الفرد في استخدام أجهزة الكمبيوتر والانترنت، زادت الكفاءة الذاتية في مجال أمن المعلومات، والتعامل مع تهديدات الجرائم الإلكترونية.[2]

3- للوعي بالأمن السيبراني تأثير إيجابي على دافع حماية المعلومات :

إن الأفراد الأكثر وعياً بالتهديدات هم أكثر عرضة لتعلم كيفية تأمين أجهزتهم، مما يؤدي إلى سلوك وقائي سيبراني أقوى، وتشمل أمثلة السلوكيات الوقائية على (تغيير كلمات المرور بانتظام، وتوخي الحذر قبل النقر على الروابط من مصادر غير معروفة، النسخ الاحتياطي للبيانات، تحديث

1 Hassan Jamil and Others, Human-Centric Cyber Security: Applying Protection Motivation Theory to Analyze Micro Business Owners' Security Behaviors, Op Cit, p 58.

2 Hao Chen and Yufei Yuan, The Impact of Ignorance and Bias on Information Security Protection Motivation: a Case of E-Waste Handling, Op Cit، pp 2250, 2251.

البرامج، اتخاذ أدوات الدفاع السيبراني)، فالوعي بالأمن السيبراني يساعد على منع إساءة استخدام أنظمة المعلومات، وزيادة إدراك مخاطر التهديدات الإلكترونية.[1]

وتفسر نظرية "دوافع الحماية" عملية اتخاذ القرار لدى الأفراد عند مواجهة التهديدات الخاصة بالجرائم الإلكترونية، ومدى تبني هؤلاء الأفراد سلوكاً وقائياً تجاه هذه الجرائم، من عدمه، ثم إنها تقدم إطاراً نظرياً وعملياً، للتنبؤ بسلوكيات التكيف مع المخاطر، ويشير هذا الإطار إلى أن دوافع الأفراد لحماية أنفسهم من تهديدات الجرائم الإلكترونية، ينبعمن تقييم هؤلاء الأفراد للتهديدات، مع الأخذ في الاعتبار حجم الضرر الناجم عن تلك التهديدات، واحتمالية تأثيراتِها السلبية، وفي حالة اعتقاد الأفراد أن إجراءات حمايتهم من الجريمة الإلكترونية ذات فعالية، ولديهم القدرة أو الثقة في ممارستها، فقد يهتمون بهذه الإجراءات، ثم إن التوعية الأمنية بمخاطر الجرائم الإلكترونية تساعد في إثراء تقييمات الأفراد للتهديدات الإلكترونية، وزيادة قدرتهم على التعامل معها، وعلى النقيض، فإن نقص المعلومات والمعرفة حول التهديدات الإلكترونية، يؤدي إلى التعامل معها بشكل غير ملائم.

إن مستوى دافعية الأفراد لحماية أنفسهم من الجرائم الإلكترونية ومخاطرها، يعتمد على تقييم خطورة الجرائم والكفاءة الذاتية للأفراد في مواجهتها وفعالية الاستجابة لديهم، فيما يتعلق بالمواجهة لتلك الجرائم، فإذا اعتبر الأفراد التهديد غير خطير، فلن يكون هناك إجراء فعلي للمواجهة، وإذا شكّ الفرد في قدرته على التعامل مع الخطر، فلن يكون لديه دافع للحماية، لذلك ينبغي أن يكون للوعي بالأمن السيبراني تأثير مباشر على دافع اتخاذ إجراءات الحماية.

- **المدخل الثاني :** نظرية **" الأنشطة الروتينية لأسلوب الحياة "**

(LRAT) (Lifestyle Routine Activities theory)

ترتبط هذه النظرية بأعمال **"هيندیلانج، وكوهين، وفيلسون"**، وتتضمن عدداً من المفاهيم، والمسلمات، وبعض القضايا النظرية التي طرحتها، والتي جاءت على النحو التالي:

أ- المفاهيم :

1 Dien Van Tran and Others, Unraveling Influential Factors Shaping Employee Cybersecurity Behaviors: an Empirical Investigation of Public Servants in Vietnam, Journal of Asia Business Studies, Vol 18, No 6, United Kingdom, 2024, p 1949.

تشتمل نظرية "الأنشطة الروتينية لأسلوب الحياة" على عدد من المفاهيم، يتمثل أهمها في:

1- ملاءمة الهدف : Target Suitability

يشير مصطلح ملاءمة الهدف إلى كون الشخص عرضة للهجوم، أو عرضة لأفعال الجناة، وملاءمة الهدف لها بُعدان هما:

– البُعد الأول: الأنشطة الروتينية التي تجعل الأفراد أو الأشياء أهدافاً مناسبة.

– البُعد الثاني: سمات الأفراد أو الأشياء التي تجعلهم أهدافاً جذابة.[1]

2- الوصاية : Guardianship

ينطوي مفهوم الوصاية على وجود بشري، ولكن وجود شخص آخر، أي لا يمكن أن يكون الفرد هدفاً للجريمة ووصياً في الوقت نفسه، وبالتالي يشترط أن يكون الوصيُّ شخصاً آخر غير الهدف (في الحالات التي يكون فيها الهدف بشرياً على وجه التحديد)، فالوجود الفعلي ووهم وجود شخص وصيّ أو يراقب، يكفيان لردع النشاط الإجرامي، ومع ذلك فإن عدم وجود وصيّ قادر على حماية شخص آخر، لا يعني بالضرورة أن الشخص المستهدف عاجز أمام الجاني، أو أنه لا يمكنه فعل أي شيء لتحسين فرص منع وقوعه ضحية في غياب "الوصيّ"، فالأفراد قادرون على حماية أنفسهم، أو تطبيق "وصاية تقنية"، هذا يعني أن استخدام الشخص للتكنولوجيا يشكل وصاية، وأن التكنولوجيا نفسها تصبح هي الوصيّ.[2]

ب- المسلمات :

تعتمد نظرية "الأنشطة الروتينية لأسلوب الحياة" على عدد من المسلمات، تتمثل في:

1- الأنشطة الروتينية للأفراد تتيح فرصاً لارتكاب الجريمة.

2- أفعال الأفراد التي تعزز تعرضهم للمجرمين المحتملين تساهم في زيادة فرص أن يصبحوا هدفاً لهؤلاء المجرمين.

3- الأفراد يسهلون وقوعهم ضحايا للجرائم الإلكترونية من خلال أنشطتهم الروتينية على الإنترنت وأنماط حياتهم.

1 Naci Akdemir and Christopher James Lawless, Exploring The human factor in Cyber-enabled and Cyber-dependent Crime Victimization: a Lifestyle Routine Activities Approach, OP Cit, p 1667.

2 Kristjan Kikerpill, The Individual's Role in Cybercrime Prevention: Internal Spheres of Protection and our Ability to Safe Guard Them, Op Cit, p 1017.

4- تقوم الجريمة الإلكترونية على (الفرص)، فهي تركز على الفرص الإجرامية التي تتيحها الأنشطة اليومية الروتينية للأفراد.[1]

5- الإدارة الفعالة لأمن شبكات التواصل الاجتماعي، يمكن أن تقلل من احتمالية وقوع مستخدمي وسائل التواصل الاجتماعي ضحية للجرائم الإلكترونية، خاصة ضحايا التصيد الاحتيالي.

6- ما يفعله الفرد، وكيف يتصرف، وأين يذهب، ومن يتفاعل معه يزيد أو يقلل من احتمالية وقوعه ضحية.[2]

جـ - القضايا النظرية :

تقوم نظرية "الأنشطة الروتينية لأسلوب الحياة" على عدد من القضايا النظرية، يتمثل أهمها في:

1- التباين في أنماط الحياة يؤثر على خطر التعرض للمجرمين:

الإيذاء لا يتوزع عشوائيا عبر الزمان والمكان، فكلما زاد الوقت الذي يقضيه الأفراد خارج المنزل، زاد احتمال تعرضهم للوقوع ضحية، نظرا لزيادة فرص تفاعلهم مع المجرمين في أماكن محفوفة بالمخاطر، كما أن التعرض أو القرب من مرتكبي الجرائم عبر الانترنت، يزيد من احتمال الوقوع ضحية.[3]

2- العلاقة بين ارتكاب الجريمة الإلكترونية و"المجرم المُحَفَّز"، و"الأهداف المناسبة"، و"غياب الوصاية المؤهلة":

هناك ثلاث عناصر رئيسة يتوقف عليها مدى التعرض للهجمات الإلكترونية، وهي:

– المجرم المُحَفَّز: فقرب الضحية من المجرم تحفز من ارتكاب الجريمة.

– الهدف المُؤهَّل: رؤية الضحايا من خلال أنواع الأنشطة التي يشاركون فيها، تسهم في مدى كون الضحية هدفاً مؤهلاً من منظور المجرم المحتمل.

1 Naci Akdemir and Christopher James Lawless, Exploring The human factor in Cyber-enabled and Cyber-dependent Crime Victimization: a Lifestyle Routine Activities Approach, OP Cit, p 1666.

2 Jacqueline M. Drew, A Study of Cybercrime Victimization and Prevention: Exploring The use of Online Crime Prevention Behaviors and Strategies, OP Cit, p 19.

3 Naci Akdemir and Christopher James Lawless, Exploring The human factor in Cyber-enabled and Cyber-dependent Crime Victimization: a Lifestyle Routine Activities Approach, OP Cit, p 1666.

- الوصاية المُؤهَّلة: وتشير إلى إدارة الأمن الإلكتروني، وهنا عندما يلتقي "المجرم المُحَفَّز"، و"الهدف المناسب"، و"غياب وصي قادر"، تقع الضحية والجريمة، وفي حال غياب أحد هذه العناصر يمكن التهرب من الوقوع ضحية لجرائم الانترنت.[1]

إن قضاء مستخدمي الإنترنت وقتاً في التواصل الاجتماعي عبر الانترنت (مثل الأنشطة اليومية)، قد يزيد من احتمالية تعرضهم لتهديدات الجرائم الإلكترونية، وخاصة الوقوع لهجمات التصيد الاحتيالي، كما أن التغييرات في الروتين اليومي للأفراد، مثل زيادة الوقت الذي يقضونه على الإنترنت، سيؤدي إلى زيادة احتمالية أن يصبحوا ضحايا للجرائم الإلكترونية، فالمجرمون يوفرون فرصاً مغرية للإيقاع بالضحايا من خلال التقرب منهم، وعدم وجود حماية كافية، في الوقت نفسه قد يسهل مستخدمو الإنترنت من وقوعهم ضحايا للجرائم الإلكترونية من خلال أنشطتهم على الإنترنت، واستخدام تكنولوجيا الإنترنت غير الآمنة.

7- الإستراتيجية المنهجية للبحث:

تحدد طبيعة موضوع البحث نوعه والمجتمع الأصلي للبحث والعينات وطرق البحث الاجتماعي وأدوات جمع البيانات، وسيتم عرضها على النحو التالي :

أ – نوع البحث :

ينتمي هذا البحث إلى البحوث الوصفية، حيث يحاول وصف طبيعة الجريمة الإلكترونية ومدى انعكاسها على الأمن الاجتماعي للأفراد ، من خلال التعرف على أهم أسباب ودوافع الجريمة الإلكترونية ، وأكثر الجرائم الإلكترونية انتشاراً ، وكيف تؤثر الجرائم الإلكترونية على الأمن الاجتماعي للأفراد ، وأهم إستراتيجيات مواجهة تلك الجرائم والوقاية منها.

ب – طرق البحث :

اعتمد البحث على كلٍ من تحليل البيانات الجاهزة ، والمسح الاجتماعي، وذلك على النحو التالي :

- تحليل البيانات الجاهزة

1 Yi Yong Lee and Others, Phishing Victimization Among Malaysian Young Adults: Cyber Routine Activities Theory and Attitude in Information Sharing Online, The Journal of Adult Protection, Vol 24, No 3/4, United Kingdom, 2022, p 183.

تم الاعتماد على البيانات الجاهزة من دراسات سابقة وتقارير وإحصائيات وكتابات نظرية خاصة بالجريمة الإلكترونية .

- المسح الاجتماعي

اعتمد البحث على (المسح الاجتماعي بالعينة)، حيث يساعد المسح الاجتماعي في التعرف على العلاقات الارتباطية بين الخصائص الاجتماعية لأفراد العينة البحثية ومدى تقيمهم لتأثير الجرائم الإلكترونية على الأمن الاجتماعي ، وذلك من خلال المسح الاجتماعي لعينة من أفراد المجتمع المصري الذين تعرضوا لجرائم إلكترونية .

جـ – أدوات البحث :

تم الاعتماد على (الاستبيان) كأداة لجمع البيانات، وتم التطبيق على مجموعة من الأفراد في المجتمع المصري من فئات اجتماعية واقتصادية مختلفة، للتعرف على الرؤى المختلفة لطبيعة الجرائم الإلكترونية ، وتأثيراتها على الأمن الاجتماعي ، وقد تم تقسيم الاستبيان إلى عدة محاور هي (**البيانات الأولية، بيانات حول أسباب ودوافع الجرائم الإلكترونية، بيانات حول نماذج الجرائم الإلكترونية الأكثر انتشاراً، بيانات حول مواجهة الجرائم الإلكترونية والوقاية منها**).

ثبات وصدق استمارة الاستبيان :

وقد تم التأكد من ثبات الاستبيان من خلال استخدام (معامل ألفا – كرونباخ) للاتساق الداخلي لمحاور الاستبيان من خلال جمع درجات الأبعاد الفرعية للمحاور الرئيسة للاستبيان، وهذا ما يوضحه الجدول التالي :

جدول رقم(1) : يوضح ثبات الاستبيان

محاور الاستبيان	معامل الثبات (ألفا – كرونباخ)
أسباب ودوافع الجريمة الإلكترونية	0.898
نماذج الجرائم الإلكترونية الأكثر انتشاراً	0.910
انعكاس الجريمة الإلكترونية على الأمن الاجتماعي	0.912

مواجهة الجريمة الإلكترونية	0.917

نستخلص من الجدول السابق ثبات أداة الاستبيان في قياس ما وضعت لقياسه، حيث إن الاستبيان ثابت بدرجة معقولة نظراً لزيادة قيمة معامل ألفا عن 0.85، وهي القيمة التي تدل على الثبات، مما يؤهلها لتكون أداة قياس مناسبة .

د- أساليب ومستويات التحليل:

- **أساليب التحليل :**

اعتمد البحث على أساليب التحليل المستخدمة في علم الاجتماع والتي تنوعت ما بين التحليل الكمي، الذي تشير إليه الأرقام والنسب المئوية، والتحليل الكيفي الذي يشير إلى الخصائص وتفسير هذه البيانات الإحصائية لموضوع البحث .

- **مستويات التحليل :**

تحددت مستويات التحليل في البحث في المجتمع المصري، متضمنةً مستويات التحليل الكبرى والصغرى ، حيث تم تحليل البيانات على مستوى الوحدات الكبرى (Macro) المتمثلة في المجتمع المصري، ومستوى الوحدات الصغرى (Micro) المتمثلة في عينة من أفراد المجتمع المصري من فئات اجتماعية واقتصادية مختلفة .

هـ- مجتمع البحث والعينات :

- **مجتمع البحث :** يتمثل مجتمع البحث في المجتمع المصري .

- **عينة البحث :** تشتمل عينة البحث على عينة من أفراد المجتمع المصري، وقد بلغ حجم عينة البحث **(186)** مبحوثاً ، ممن تعرضوا لجرائم إلكترونية ، وتم الوصول إلى هذه العينة عن طريق (كرة الثلج).

- **خصائص عينة البحث :** سوف نتناول عينة البحث من خلال عدد من المؤشرات الرئيسة التي تتمثل في (النوع – السن – الحالة الاجتماعية –المستوى التعليمي – المهنة – محل الإقامة)، وهي على النحو التالي :

جدول رقم(2) : يوضح النوع

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
ذكر	129	69.4	0.694	0.462	186	100
أنثى	57	30.6				

يتضح من بيانات الجدول السابق أن: أغلب المبحوثين ممن تعرضوا لجرائم إلكترونية (ذكور) بنسبة 69.4%، ويبلغ عددهم 129 مبحوثاً، في حين أن 30.6% من المبحوثين (إناث) ممن تعرضن لجرائم إلكترونية، وعددهن 57 مبحوثة، وذلك بمتوسط حسابي يُقدر بحوالي ٠.٦٩٤، وانحراف معياري ٠.٤٦٢، ويتبين من ذلك أن الذكور أكثر تعرضاً للجرائم الإلكترونية، وقد يرتبط ذلك بشكلٍ كبيرٍ بالاستخدام المتزايد للذكور لتكنولوجيا الاتصالات والمعلومات أو الإنترنت بشكلٍ عامٍ مقارنة بالإناث.

جدول رقم(3) : يوضح السن

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
15 إلى أقل من 25 عاماً	93	50	1.785	0.957	186	100
25 إلى أقل من 35 عاماً	56	30.1				
35 إلى أقل من 45 عاماً	21	11.3				

45 إلى أقل من 55 عاماً	16	8.6				
55 عاماً فأكثر	-	-				

يتضح من بيانات الجدول السابق أن: أغلب المبحوثين ممن تعرضوا لجرائم إلكترونية في الفئة العمرية (15 إلى 25 عاماً) بنسبة 50%، ويبلغ عددهم 93 مبحوثاً، و30.1% من المبحوثين ممن تعرضوا لجرائم إلكترونية في الفئة العمرية (25 إلى 35 عاماً)، ويبلغ عددهم 56 مبحوثاً، و11.3% من المبحوثين في الفئة العمرية (35 إلى 45 عاماً)، ويبلغ عددهم 21 مبحوثاً، و8.6% من المبحوثين أعمارهم تقع في الفئة العمرية (45 إلى 55 عاماً)، وعددهم 16 مبحوثاً، في حين أن عينة البحث لم تشتمل على مبحوثين في الفئة العمرية (55 عاماً فأكثر)، وذلك بمتوسط حسابي يُقدر بحوالي ١.٧٨٥، وانحراف معياري ٠.٩٥٧، ويتبين من ذلك أن أغلب الأفراد ممن يتعرضون للجرائم الإلكترونية من فئة (الشباب)، لأنهم أكثر الفئات استخداماً لتكنولوجيا الاتصالات والمعلومات، وفي المقابل (الفئات الأكبر سناً) أقل استخداماً لتلك التكنولوجيا، وبالتالي أقل تعرضاً لمخاطرها وجرائمها.

جدول رقم(4) : يوضح الحالة الاجتماعية

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
لم يتزوج	140	75.3	0.753	0.433	186	100
متـزوج	46	24.7				

يتضح من بيانات الجدول السابق أن: أغلب عينة البحث ممن تعرضوا لجرائم إلكترونية (لم يتزوجوا) بنسبة 75.3% من إجمالي عدد المبحوثين وعددهم 140 مبحوثاً، في حين أن 24.7% (متزوجون) وعددهم 46 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.753، وانحراف معياري 0.433، ويشير ذلك إلى أن الجرائم الإلكترونية تتركز بشكلٍ أكبر بين الفئات غير المتزوجة نظراً لأن تلك الفئات قد يكون لديها وقت أطول لاستخدام تكنولوجيا الاتصالات والمعلومات، وفي نفس الوقت مسئوليات أقل تسمح

لهم بالمشاركة بشكلٍ أكبر في استخدام تكنولوجيا الإنترنت، وبالتالي تكون الفرصة أكبر لتعرضهم للجرائم الإلكترونية.

جدول رقم(5) : يوضح المستوى التعليمي

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
يقرأ ويكتب	3	1.6	4.591	0.860	186	100
ابتدائي	3	1.6				
إعدادي	10	5.4				
ثانوي	44	23.7				
جامعي	117	62.9				
فوق جامعي	9	4.8				

يتضح من بيانات الجدول السابق أن: أغلب العينة ممن تعرضوا للجرائم الإلكترونية بنسبة 62.9% من إجمالي عدد المبحوثين مستواهم التعليمي (جامعي)، ويبلغ عددهم 117 مبحوثاً، و23.7% مستواهم التعليمي (ثانوي)، ويبلغ عددهم 44 مبحوثاً، و5.4% مستواهم التعليم (إعدادي)، ويبلغ عددهم 10 مبحوثين، و4.8% مستواهم التعليمي (فوق جامعي)، وعددهم 9 مبحوثين، وأقل عدد من المبحوثين مستواهم التعليمي (ابتدائي، ويعرفون القراءة والكتابة)، وذلك بمتوسط حسابي يُقدر بحوالي4.591، وانحراف معياري 0.860، ويشير ذلك إلى أن أكثر مستخدمي تكنولوجيا الاتصالات والمعلومات، مستواهم التعليمي (جامعي)، نظراً لأنهم أكثر تطلعا للتطور التكنولوجي، الأمر الذي يعرضهم بشكلٍ أكبر للجرائم الإلكترونية، ومن ثم تتركز الجرائم الإلكترونية لدى هذه الفئة التعليمية بمستوى أعلى من الفئات التعليمية الاخرى.

جدول رقم(6) : يوضح المهنة

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة

مـــوظـــف	49	26.4	0.264	0.442	186	100
أعمال تجارية	25	13.4	0.134	0.342		
أعمال فنـيـــة	20	10.8	0.108	0.317		
أعمال زراعية	9	4.8	0.048	0.215		
عـامـل خدمات	10	5.4	0.054	0.226		
طـــالـــب	32	17.2	0.172	0.378		
لا يعـمـــــل	41	22	0.220	0.416		

يتضح من بيانات الجدول السابق أن: أغلب المبحوثين ممن تعرضوا لجرائم إلكترونية (موظفون) بنسبة 26.4%، ويبلغ عددهم49 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي0.264، وانحراف معياري 0.442، و22% (لا يعملون)، وذلك بمتوسط حسابي يُقدر بحوالي0.220، وانحراف معياري0.416، وعددهم41مبحوثاً، و17.2% (طلاب)، وعددهم32 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي0.172، وانحراف معياري 0.378، و13.4% يعملون(بالأعمال التجارية)، وعددهم25 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي0.134، وانحراف معياري0.342، و10.8% يعملون (بالأعمال الفنية) وعددهم20 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي0.108، وانحراف معياري 0.317، و5.4% يعملون(بمجال الخدمات)، وعددهم 10 مبحوثين، و4.8% يعملون (بالأعمال الزراعية)، ويشير ذلك إلى أن أغلب الأفراد ممن يتعرضون للجرائم الإلكترونية (موظفون) نظراً لأن طبيعة بعض الأعمال في العصر الحالي تتطلب التعامل مع تكنولوجيا الاتصالات والمعلومات، كما أن طلاب الجامعات أيضاً يستخدمون تكنولوجيا الاتصالات والمعلومات بشكلٍ كبيرٍ، مما يعرضهم للجرائم الإلكترونية، في ظل عدم الوعي والأمان الكافي للحماية من الجرائم الإلكترونية.

جدول رقم(7) : يوضح محل الإقامة

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
حضـــر	167	89.8	0.898	0.304	186	100
ريـــف	19	10.2				

يتضح من بيانات الجدول السابق أن: أغلب المبحوثين الذين تعرضوا لجرائم الإلكترونية مقيمون في (الحضر) بنسبة 89.8% من إجمالي عدد المبحوثين ويبلغ عددهم167 مبحوثاً، في حين أن10.2% مقيمون في(الريف) ويبلغ عددهم 19 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي0.898، وانحراف معياري0.304، ويشير ذلك إلى تركز الجرائم الإلكترونية بشكلٍ أكبر لدى المقيمين في الحضر، ويرجع ذلك إلى أنهم أكثر اهتماماً باستخدام تكنولوجيا الإنترنت، إلى جانب أن غالبية وظائفهم تحتم عليهم التعامل مع تكنولوجيا الاتصالات والمعلومات، وهو ما يتيح الفرصة بشكلٍ أكبر للتعرض للجرائم الإلكترونية، بالمقارنة بالمقيمين في الريف.

ثانياً : أسباب ودوافع الجريمة الإلكترونية

تشهد البيئة الإلكترونية تغيراً وتطوراً مستمراً، نظراً لسرعة التقدم التقني، ومع تزايد توافر شبكات الحاسوب، استغل المخترقون الخدمات الشبكية لتحقيق مكاسب شخصية، وشهرة واسعة في بيئة محفوفة بالمخاطر، حيث أصبحت الجريمة الإلكترونية مرتبطة بالتكنولوجيا المتقدمة، واستخدام مواقع التواصل الاجتماعي، والأنماط الحديثة نسبياً في الاتصالات سريعة النمو، وجميعها تحت سيطرة المنظمات الإجرامية، وللحفاظ على تفوق مجرمي الإنترنت وقدراتهم التنافسية، يُعد اتباع إستراتيجية ذكية واستباقية ومتطورة لتكنولوجيا المعلومات أمراً بالغ الأهمية.[1]

وقد تطورت الجريمة الإلكترونية وتعددت هجماتها، وأصبحت أكثر انتشاراً وأوسع نطاقا، وبشكل يختلف عن بداية ظهور هذه الجرائم، فالجريمة الإلكترونية تطورت من خلال عدة مراحل هي:

- المرحلة الأولى:

بظهور الكمبيوتر وربطه بشبكة الإنترنت في الستينيات والسبعينيات، وظهرت أول معالجة لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي، وبدأ التساؤل هل هذه الجرائم مجرد حالة عابرة أم ظاهرة إجرامية مستجدة ؟ .

- المرحلة الثانية:

في بداية الثمانينيات، حيث بدأت أنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بتدمير كلي للملفات والبرامج، وشاع مصطلح "الهاكرز" المعبر عن مقتحمي النظم والمجرم المعلوماتي.

- المرحلة الثالثة:

1 Kuldeep Singh Kaswan and Others, Cybersecurity Law-Based Insurance Market, Op Cit, p 305.

وتبدأ من التسعينيات، حيث تزايدت الجرائم الإلكترونية بشكل هائل، وحدث تغير في نطاقها ومفهومها، وساعد على ذلك نمو الإنترنت، دون مراعاة تحديات أمن المعلومات.[1]

ووفقاً للأرقام العالمية للجرائم الإلكترونية لعام 2018 فيقرب من 700 مليون شخص كانوا ضحايا لنوع من أنواع الجرائم الإلكترونية، ويحقق مجرمو الإنترنت إيرادات قد تصل إلى 1,5 تريليون دولار سنوياً، مع الوضع في الاعتبار أن جميع الجرائم الإلكترونية لا يتم التبليغ عنها.[2]

لقد فتح تطور الإنترنت بيئة غير آمنة للاستغلال الإجرامي في ظل الاعتماد المتزايد للأفراد على التكنولوجيا، لتلبية احتياجاتهم اليومية من التجارة إلى التفاعل الاجتماعي، ورغم تباين الإحصاءات، ففي عام 2019 قُدر عدد مستخدمي الإنترنت حول العالم بنحو 4,48 مليار مستخدم.[3]

وتزامنت طبيعة الفرص التي تتيحها التطورات التكنولوجية مع تزايد حالات الجرائم الإلكترونية، وأصبحت حالات تسريب كلمات المرور وأسماء المستخدمين على الإنترنت أمرا شائعا للغاية في العالم الحديث، كما يفقد الملايين من الأشخاص حول العالم بياناتهم الخاصة واستثماراتهم المالية على يد القراصنة ومجرمي الإنترنت، وقد صنف " تقرير المخاطر العالمية " الصادر عن المنتدى الاقتصادي العالمي، عمليات الاحتيال والنصب الضخمة في البيانات في "المرتبة الرابعة"، والهجمات الإلكترونية في "المرتبة الخامسة" ضمن المخاطر العالمية في عام 2019.[4]

ويمكن أن يُعزى نمو الجرائم الإلكترونية إلى:

1- النمو والتطور السريع للتكنولوجيا التي يشهدها العالم، والذي عمل على خلق مسافات وتحديات كبيرة، لم يستطع العالم معها إيجاد وسائل للتحكم والسيطرة بشكل كامل عليها، فكلما زادت التكنولوجيا زادت الجرائم الإلكترونية والضحايا.

---

[1] لامية طالة، كهيذة سلام، الجريمة الإلكترونية: بُعد جديد لمفهوم الإجرام عبر منصات التواصل الاجتماعي، مرجع سابق، ص 70.

2 Mahmood Hussain Shah and Others, Cybercrimes Prevention: Promising Organizational Practices, Information Technology and People, Vol 32, No 5, United Kingdom, 2019, p 1125.

3 Jacqueline M. Drew, A Study of Cybercrime Victimization and Prevention: Exploring The use of Online Crime Prevention Behaviors and Strategies, Op Cit, p 17.

4 Hassan Younies and Tareq Na›el Al-Tawil, Effect of Cybercrime Laws on Protecting Citizens and Businesses in The United Arab Emirates, Journal of Financial Crime, Vol. 27, No. 4, United Kingdom, 2020, p 1091.

2- التحولات التي أحدثتها العولمة في عالم الجريمة الإلكترونية وانعكاساتها على الأمن الاجتماعي وحماية المجتمع، حيث ساعدت العولمة على اختراق الحواجز والتوغل في معظم دول العالم، خاصة دول العالم الثالث، وبالتالي تُعد العولمة من العوامل التي ساعدت على انتشار الجرائم الإلكترونية.[1]

3- انتشار شبكات الإنترنت المظلمة التي تستخدم مجموعات معقدة من المعاملات التي تشمل وسطاء آخرين في الأسواق السوداء.

4- زيادة أعداد مستخدمي الإنترنت الجدد من الاقتصادات منخفضة الدخل ذات الأمن السيبراني الضعيف.

5- سرعة تبني مجرمي الإنترنت للتقنيات الجديدة.

6- تطور مهارات كبار مجرمي الإنترنت في تبسيط عمليات الربح مع تزايد استخدام العملات الرقمية.[2]

7- ضعف تنفيذ القانون وتطبيقه في الجريمة الإلكترونية فهناك الكثير من الدول التي لم تطور تشريعاتها وأجهزة العدالة بها لكي تتمكن من مواكبة التقدم في مكافحة الجرائم الإلكترونية وأساليبها.[3]

وقد كشفت نتائج البحث الميداني أن هناك بعض الأسباب التي تزيد من وقوع الأفراد ضحايا للجرائم الإلكترونية ، كما توضحها بيانات الجدول التالي :

جدول رقم(8) : يوضح سبب تعرض الأفراد للجرائم الإلكترونية

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
عدم الوعي بكيفية استخدام الإنترنت	95	51.1	0.510	0.501	186	100
قضاء أوقات طويلة على الإنترنت	29	15.6	0.156	0.364		

[1] مهنا بن يوسف بن مهناء المخايطة، العوامل الاجتماعية لوقوع الشباب ضحايا للجرائم الإلكترونية: دراسة ميدانية بمدينة الهفوف، مجلة الخدمة الاجتماعية، المجلد 1، العدد 70، الجمعية المصرية للأخصائيين الاجتماعيين، مصر، 2021، ص ص 276، 277.

[2] Peter Yeoh, Artificial Intelligence: Accelerator or Panacea for Financial Crime?, Journal of Financial Crime, Vol 26, No 2, United Kingdom, 2019, p 637.

3 نوال قادة بن عبد الله، محمد بن حمو، الجريمة الإلكترونية: قراءة سوسيولوجية لأهم النظريات المفسرة للسلوم الإجرامي، مجلة روافد للدراسات والأبحاث العلمية في العلوم الاجتماعية والإنسانية، المجلد 6، العدد 3، المركز الجامعي بلحاج بوشعيب، الجزائر، 2022، ص 669.

تزايد إفصاح الأفراد عن معلوماتهم الشخصية	62	33.3	0.333	0.471		

يتضح من بيانات الجدول السابق أن: الغالبية من المبحوثين ممن تعرضوا لجرائم إلكترونية بنسبة 51.1%، يرون أن سبب التعرض للجرائم الإلكترونية عدم الوعي بكيفية استخدام الإنترنت، ويبلغ عددهم 95 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.510، وانحراف معياري 0.501، و33.3% يرون أن تزايد إفصاح الأفراد عن معلوماتهم الشخصية يُعد أحد أسباب التعرض للجرائم الإلكترونية، ويبلغ عددهم 62 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.333، وانحراف معياري 0.471، في حين أن 15.6% يرون السبب قضاء أوقات طويلة على الإنترنت، ويبلغ عددهم 29 مبحوثاً، ويتبين من ذلك أن التعرض للجرائم الإلكترونية يرجع بشكل كبير إلى عدم وعي غالبية الأفراد بكيفية استخدام الإنترنت، إلى جانب تزايد إفصاحهم عن معلوماتهم الشخصية.

إلى جانب الأسباب التي يرجع إليها نمو الجرائم الإلكترونية، هناك مجموعة من الدوافع لارتكاب تلك الجرائم، وهي:

- الكسب المالي: يهدف مرتكبو الجرائم الإلكترونية إلى الكسب المالي كما هو الحال في الجرائم التقليدية.
- الدوافع السياسية: تستخدم المنظمات المتطرفة الإنترنت لنشر الدعاية لتدمير المواقع الإلكترونية المنافسة وشبكاتها.
- الدوافع الجنسية: تعتبر الجرائم الإلكترونية المتعلقة بالمحتوى والأنشطة الجنسية غير مشروعة، ويستغل الناس المواقع الإباحية لإشباع رغباتهم، والقيام بأعمال غير أخلاقية.
- الترفيه: على عكس الجرائم الإلكترونية التي يستخدم فيها الإنترنت كوسيلة لتحقيق غاية، ترتكب بعض الجرائم الإلكترونية لمجرد التسلية والمتعة، وهنا تعد التسلية دافعاً ونتيجة في آنٍ واحد.

– الدوافع العاطفية: يندفع بعض مجرمي الإنترنت بدوافع عاطفية قوية، وخاصة الانتقام، قد يكون هؤلاء الأفراد قد تعرضوا للخداع من قبل شركاء عاطفيين، أو أزواج، أو زملاء، أو شركاء عمل، أو غيرهم، ويمنحهم السعي للانتقام فرصة للتخطيط لأعمالهم، وتقل احتمالية كشف هويتهم.[1]

– الانبهار بالتقنية المعلوماتية: مع ظهور التقنية المعلوماتية، وانتشارها سواء تعلق الأمر بالمعلومات أو أجهزة الحاسب، فإن الأمر في النهاية يؤدي إلى انبهار المجرمين بهذه التقنية الحديثة، وفي هذه الحالة فإن مرتكبي الجرائم الإلكترونية يفضلون تحقيق انتصارات تقنية.[2]

وقد كشفت نتائج البحث الميداني أن الدافع الأكثر انتشاراً وراء ارتكاب الجرائم الإلكترونية هو سعي مرتكبيها إلى الكسب المادي ، كما توضح بيانات الجدول التالي :

جدول رقم(9) : يوضح أسباب ودوافع الجرائم الإلكترونية

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
الكسب المادي	120	64.5	0.645	0.480	186	100
الترفيه	29	15.6	0.156	0.364		
دوافع عاطفية (الانتقام)	37	19.9	0.199	0.400		
دوافع سياسية	-	-	-	-		

يتضح من بيانات الجدول السابق أن: الغالبية من المبحوثين ممن تعرضوا لجرائم إلكترونية بنسبة 64.5%، يرون أن أهم أسباب ودوافع ارتكاب تلك الجرائم هو الكسب المادي، ويبلغ عددهم 120 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.645، وانحراف معياري 0.480، و19.9% من المبحوثين يرون أن الدوافع العاطفية مثل الانتقام تُعد أحد أسباب الجرائم الإلكترونية، ويبلغ عددهم 37 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.199، وانحراف معياري 0.400، و15.6% يرون الترفيه هو الدافع

1 Kiran Joshi and Priyanka Kaushik, An Analysis of Perception and Awareness of Undergraduate Youth Towards Cybercrime, Advanced Series in Management, Vol 34A, Emerald Publishing Limited, United Kingdom, 2024, p 105.

2 فيصل كامل نجم الدين، واقع الجريمة الإلكترونية في مواقع التواصل الاجتماعي: الحماية النظامية في دول مجلس التعاون الخليجي، المجلة الدولية للاتصال الاجتماعي، المجلد 5، العدد 4، كلية العلوم الإنسانية والاجتماعية، جامعة عبد الحميد بن باديس مستغانم، الجزائر، 2018، ص 15.

لارتكاب الجريمة الإلكترونية ، وعددهم 29 مبحوثاً، ويتبين من ذلك أن مرتكبي الجرائم الإلكترونية يكون الدافع الأساس لديهم لارتكابهم تلك الجرائم هو الكسب المادي إلى جانب الانتقام من الضحايا.

ومن ثم تتمثل طبيعة الجرائم الإلكترونية في :

- الجريمة الإلكترونية سلاحها التكنولوجيا ، إنها العمل مع التكنولوجيا، مما يجعل مجرمي الإنترنت خبراء تقنيين ذوي معرفة عميقة بمجال الحواسيب والإنترنت والشبكات.
- تحدث الجرائم الإلكترونية في الوقت الفعلي، وهو ما يجعلها فعالة للغاية، ولا تستغرق سوى لحظات لاختراق مواقع الويب، أو القيام بعمليات احتيال إلكتروني.
- لا حدود جغرافية لها ولا مسافات، لذا يمكن لمجرمي الإنترنت ارتكاب جرائمهم على جهاز كمبيوتر، أو بواسطته من أي مكان في العالم.
- تتم جميع عمليات التحضير والتنفيذ للجرائم الإلكترونية في الفضاء الإلكتروني، مما يجعل مجرمي الإنترنت متورطين فعليا في الجريمة.
- يُعد جمع الأدلة على الجرائم الإلكترونية مهمة صعبة للغاية ويصعب إثباتها قانوناً.[1]
- الجرائم الإلكترونية جرائم ناعمة لا تتطلب أي نوع من المجهودات العضلية، مثل الجرائم التقليدية.
- تتم بتعاون أكثر من شخص على ارتكابها.
- تقع الجريمة الإلكترونية في أحيان كثيرة أثناء المعالجة الآلية للبيانات.[2]
- تتسم الجرائم الإلكترونية بالجاذبية، نظراً لما يمثله سوق الحاسب والإنترنت من ثروة كبيرة للمجرمين أو للإجرام المنظم، فقد أصبحت أكثر جذباً لاستثمار الأموال وغسيلها، والتوظيف منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات، وسرقة المعلومات.[3]

---

1 Kiran Joshi and Priyanka Kaushik, An Analysis of Perception and Awareness of Undergraduate Youth Towards Cybercrime, Op Cit, p 103.

2 محمود صالح محمد مثنى، الجريمة الإلكترونية ومراحل تطورها، التواصل، العدد 52، جامعة عدن- نيابة الدراسات العليا والبحث العلمي، عدن، اليمن، 2024، ص ص 169، 170.

3 Fatima Al- Zahra Qamqani ، مفهوم وتطور الجريمة الإلكترونية، مرجع سابق ، ص 63.

ومن خلال الأسباب والدوافع الخاصة بالجريمة الإلكترونية وطبيعتها، يمكن التوصل إلى بعض خصائص مرتكبي الجرائم الإلكترونية، وهي:

- مجرم يمتلك المعرفة والمهارة: المعرفة بالوسائل الإلكترونية، مثل الحاسب الآلي والإنترنت، والتي تُعد أدوات ارتكاب الجريمة الإلكترونية هذا من جهة، ومن جهة أخرى العلم بكيفية التعامل مع المواقع الإلكترونية.
- مجرم غير عنيف: فهو مجرم ذكي يستعين بالحاسوب والإنترنت لحل المشكلات التي تواجهه، مثل الاستعانة بالفيروسات لتدمير موقع إلكتروني ما.
- مجرم اجتماعي: فمرتكب الجرائم الإلكترونية إلى جانب أنه شخص ذكي، فهو شخص اجتماعي بطبيعته مع الآخرين، لأنه في الغالب ليس لديه ميول عدوانية ظاهرة تجاه المحيط الاجتماعي الذي يعيش فيه، فالذكاء سمة من سمات التكيف الاجتماعي، لذلك نجد أن بعض الجرائم الإلكترونية يكون مجرموها على علاقة اجتماعية سابقة بالضحايا، أو تربطهم علاقة عمل مع المؤسسات المجني عليها.[1]

وتبين من نتائج البحث أن مرتكبي الجرائم الإلكترونية غالباً أشخاص مجهولو الهوية وغير معروفين ، كما تشير بيانات الجدول التالي :

جدول رقم(10) : يوضح مرتكبي الجريمة

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
صديق	.12	6.5	0.065	0.246	186	100
شخص لا أعرفه	172	92.5	0.925	0.265		
زميل عمل	2	1.1	0.011	0.103		
أحد الأقارب	-	-	-	-		

[1] دلال لطيف مطشر الزبيدي، جريمة الاعتداء على المواقع الإلكترونية، مجلة جامعة بابل- العلوم الإنسانية، المجلد 26، العدد 9، جامعة بابل، العراق، 2018، ص 397.

يتضح من بيانات الجدول السابق أن: الغالبية من المبحوثين ممن تعرضوا لجرائم إلكترونية بنسبة 92.5% تعرضوا لتلك الجرائم من أشخاص غير معروفين، ويبلغ عددهم 172 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.925 ، وانحراف معياري 0.265، و6.5% من المبحوثين تعرضوا لجرائم إلكترونية من قبل أصدقائهم، ويبلغ عددهم 12 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.065، وانحراف معياري0.265، و1.1% تعرضوا لجرائم إلكترونية من قِبل زميل في العمل وعددهم مبحوثان، ويتبين من ذلك أن أغلب الجرائم الإلكترونية يتم ارتكابها من قِبل أشخاص غير معروفين للضحايا.

وقد أكدت نتائج البحث أن الشباب هم الفئة الأكثر عرضة للجرائم الإلكترونية ، كما يتضح ذلك من بيانات الجدول التالي:

جدول رقم(11) : يوضح الفئات الأكثر عرضة للجرائم الإلكترونية

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
الفئات الأصغر سناً	63	33.9	0.339	0.475	186	100
الشباب	87	46.8	0.467	0.500		
الفئات الأكبر سناً	36	19.3	0.193	0.396		

يتضح من بيانات الجدول السابق أن: الغالبية ممن تعرضوا للجرائم الإلكترونية بنسبة 46.8%، يرون أن أكثر الفئات عرضة للجرائم الإلكترونية (الشباب)، ويبلغ عددهم 87 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.467،وانحراف معياري 0.5، و33.9% من المبحوثين يرون أن (الفئات الأصغر سناً) أكثر عرضة للجرائم الإلكترونية، ويبلغ عددهم 63 مبحوثاً، وذلك بمتوسط حسابي 0.339، وانحراف معياري 0.475، في حين أن 19.3% يرون (الفئات الأكبر سناً)، ويبلغ عددهم 36 مبحوثاً، ويتبين من ذلك أن فئة الشباب هم الأكثر عرضة للجرائم الإلكترونية، نظرا لأن هذه الفئة أكثر استخداماً للإنترنت وبرامجه وتطبيقاته.

ثالثاً : نماذج الجرائم الإلكترونية الأكثر انتشاراً

تشهد الجرائم الإلكترونية معدلات تنذر بالخطر، حيث يتم الإبلاغ يومياً عن حوالي (80 مليار) عملية احتيال ضارة، و(300 ألف) برنامج خبيث جديد، و(33 ألف) عملية تصيد احتيالي، و(4 آلاف) عملية فدية، و(780 ألف) سجل مفقود، بسبب عمليات الاختراق، ومن المتوقع أن تشهد الجرائم الإلكترونية مزيداً من النمو، حيث استغل المخترقون بشكلٍ متزايد أجهزة الإنترنت ضعيفة الحماية، من خلال نشر أدوات الذكاء الاصطناعي المحسنة، التي تُنشئ برامج ضارة، يتم من خلالها ارتكاب الجرائم الإلكترونية.[1]

وهناك بعض الوسائل التي يتم استخدامها من قِبل مرتكبي الجريمة الإلكترونية لممارسة جرائمهم، يتمثل أهمها في :

- برنامج فلام : Flame

وهو برنامج تجسس حاسوبي وُجد عام 2012، كفيروس يصيب أنظمة تشغيل الحاسوب، ويستخدمه مرتكبو الجرائم الإلكترونية، وغالباً ما يُستخدم هذا البرنامج للتجسس عبر الشبكة المحلية (LAN)، أو ذاكرة (USB)، مصيباً آلاف الأجهزة المتصلة من أفراد ومدارس وجامعات وهيئات حكومية.[2]

- الألعاب الإلكترونية : Video Games

تكتسب ألعاب تقمص الأدوار الجماعية عبر الإنترنت شعبية متزايدة بسرعة، لذلك تنشأ مشاكل متنوعة، مثل سرقة الحسابات والتحويلات غير القانونية للأموال، والسلع الافتراضية، أو المشاكل المادية الناجمة عن الإفراط في ممارسة الألعاب، كما تتزايد حصة ألعاب الهاتف المحمول في تطبيقات الهاتف المحمول يوماً بعد يوم في هذا العصر، وتعتمد التأثيرات السلبية لألعاب الهاتف المحمول على مدة الاستخدام ومحتوى اللعبة ونوعها، لذلك قد تشكل ألعاب الهاتف المحمول والكمبيوتر سبباً للوقوع ضحية للجرائم الإلكترونية.[3]

- البرمجيات الخبيثة : Malware

تغطي البرمجيات الخبيثة مجموعة واسعة من التهديدات الإلكترونية القائمة على الأكواد، مثل فيروسات الحاسوب، وبرامج تسجيل ضغطات المفاتيح، وتُستخدم الملفات المصابة أو البرامج أو مواقع

1 Peter Yeoh, Artificial Intelligence: Accelerator or Panacea for Financial Crime?, Op Cit, p 637.

2 Kuldeep Singh Kaswan and Others, Cybersecurity Law-Based Insurance Market, Op Cit, p 307.

3 Vasileios Vlachos and Others, The Landscape of Cybercrime in Greece, Information Management and Computer Security, Vol 19, No 2, Emerald Group Publishing Limited, United Kingdom, 2011, p 117.

الويب الموزعة مجاناً لإصابة الأجهزة الإلكترونية المستهدفة، وتُشكل الإصابة بالبرمجيات الخبيثة تهديداً كبيراً لأمن الأجهزة الإلكترونية، بالإضافة إلى المعلومات الشخصية لمستخدمي الإنترنت وخصوصيتهم.[1]

كما تستخدم البرمجيات الخبيثة لتعديل البرامج، أو التلاعب في البرامج الإلكترونية، ويكون تعديل البرامج غالباً بهدف الاختلاس، في حين أن التلاعب في البرامج يكون من خلال التدخل في برنامج أصلي يُزرع فيه برنامجٌ فرعيٌ دقيقٌ، بحيث يتمكن هذا البرنامج من الدخول غير المشروع لأي نظام معلوماتي.[2]

- الهندسة الاجتماعية : Social Engineering

يستخدم مرتكبو الجرائم الإلكترونية هجمات الهندسة الاجتماعية عن طريق أشكال مختلفة من الاتصالات عبر الإنترنت والتكنولوجيا، من خلال استهداف الأفراد الذين قد لا يدركون غالباً قيمة المعلومات التي يقدمونها، حيث تستغل هجمات الهندسة الاجتماعية الثقة البشرية لإقناع الضحية بالكشف عن معلومات حساسة عن غير قصد، وتدور هذه الهجمات حول لحظة اتخاذ القرار بشأن الثقة في إجراء ما، بفتح رابط أو النقر عليه.[3]

- حصان طروادة : Trojan Horse

هو عبارة عن برنامج مخفي في نظام الحاسوب، يتم إدخاله بواسطة برنامج أو نظام موثوق الاستعمال، ويهدف إلى تغيير أو تبديل أو حذف البرامج والمعلومات داخل الحاسوب، وقد يكون على شكل برنامج عادي، مما يشجع المستخدم على تشغيله وعند فتح البرنامج يتبين أنه حصان طروادة، وأنه مسئول عن تدمير العديد من البرامج، وقد تظهر الرسالة "أمسكت بك" وأحصنة طروادة يمكن أن تكون خطيرة، وصعبه الاكتشاف، فأحياناً يقوم البرنامج بتدمير نفسه بعد اتمام العملية، وسُمِّي حصان طروادة (لأنه يقوم بمقام الحصان الخشبي الشهير في الأسطورة المعروفة، الذي تُرك أمام الحصن، وحين أدخله إليه الناس، خرج من داخله الغزاة، فتمكنوا من السيطرة والاستيلاء على الحصن)، هذا الملف الصغير الفتاك يدخل لجهاز الضحية، يُغير من هيئته، ويصعب اكتشافه في حالة عدم وجود برنامج جيد مضاد للفيروسات،

1 Naci Akdemir and Christopher James Lawless, Exploring The human factor in Cyber-enabled and Cyber-dependent Crime Victimization: a Lifestyle Routine Activities Approach, OP Cit, p 1669.

2 إبراهيم حسن عبد الرحيم الملا، الذكاء الاصطناعي والجريمة الإلكترونية، مجلة الأمن والقانون، المجلد 26، العدد 1، دبي، الإمارات، 2018، ص 127.

3 Curtis C. Campbell, Solutions for Counteracting Human Deception in Social Engineering Attacks, Information Technology and People, United Kingdom. Vol 32, No 5, United Kingdom, 2019, p 1130.

وبالتالي تُعد أحصنة طروادة بالمقام الاول ملفات تجسس، يمكن أن تسيطر سيطرة تامة على الضحية، وتكمن خطورتها في أنها لا تصدر أي علامات تدل على وجودها بجهاز الضحية.[1]

- الشبكات الاجتماعية : Social Networks

تُعد الشبكات الاجتماعية بمثابة فضاء إلكتروني، يؤثر تلقائياً على المشاعر، والأفكار، والميول، والعلاقات الإنسانية، والتفاعلات الاجتماعية، ويرتبط الأفراد على هذه الشبكات باهتمامات وميول مشتركة، ويسبب الاستخدام غير السليم للشبكات الاجتماعية انعداماً للأمن النفسي والاجتماعي، مما قد يُخلِف أثاراً لا يمكن إصلاحها على المجتمع والأفراد، وتعتمد التأثيرات السلبية للشبكات الاجتماعية بشكلٍ كبير على مدة الاستخدام، والمحتوى المرغوب، والصفحات المتابعة.[2]

- برامج الفدية : Ransomware

وهي برمجيات حاسوبية خبيثة تمنع وصول الضحية إلى البيانات على أنظمه حاسوبه، ويتم ذلك عادة بتشفير البيانات ومطالبة الضحية بدفع فدية، غالبا ما تكون على شكل عملة افتراضية يصعب تتبعها، ومن أمثلة برامج الفدية (فيروس WannaCry).[3]

وتتمثل أهم نماذج الجرائم الإلكترونية الأكثر انتشاراً التي تمارس ضد الأفراد في:

1- <u>التصيد الاحتيالي:</u>

في هذا النوع من الجرائم أو الخداع، يحصل مرتكبو هذه الجرائم على معلومات، مثل بيانات تسجيل الدخول، أو تفاصيل الدفع من خلال انتحال شخصية فرد، أو كيان قانوني عبر قنوات متعددة .[4]

حيث يقوم مجرمو الإنترنت بالحصول على معلومات حساسة، من خلال انتحال شخصية أفراد موثوق بهم، لخداع الضحايا ودفعهم إلى الكشف عن معلومات حساسة، والتي سيستخدمونها لاحقاً

---

[1] فريحة محمد كريم، الجريمة الإلكترونية، شئون اجتماعية، المجلد 28، العدد 110، جمعية الاجتماعيين في الشارقة، الجزائر، 2011، ص 144.

2 Yang Li and Others, Cybercrime's Tendencies of The Teenagers in The COVID-19 Era: Assesssing. The Influence of Mobile Games, Social Networks and Religious Attitudes, Journal of Kubernetes Emerald Publishing Limited, United Kingdom, 2021, p K.

3 Eileen M. Decker and Others, Bots, Bytes, and Briefs: Cyber Investigations and Prosecutions Community, Environment and Disaster Risk Management, Vol. 24, United Kingdom, 2021, p 36.

4 Kuldeep Singh Kaswan and Others, Cybersecurity Law-Based Insurance Market, Op Cit, p 312.

لأغراض احتيالية وعديمة الضمير، أو الضغط على الضحية للقيام بسلوك يفيد المجرم، مثل تحويل أموال، أو الكشف عن معلومات سرية.[1]

كما أن التصيد الاحتيالي يتضمن الاحتيال المالي، وهنا تكون عمليات الاحتيال ذات دوافع مالية، ويمكن أن يمتد من هجمات التصيد الاحتيالي البسيطة، إلى مخططات أكثر تعقيداً باستخدام أساليب استغلال الأموال.[2]

ويُعد هجوم التصيد الاحتيالي من أكثر الهجمات شيوعاً، وتُحقق أعلى معدل نجاح، وكلما زادت المعلومات المُفصح عنها من قبل الأفراد، زادت فرص وقوع الأفراد في هجوم التصيد الاحتيالي، وفي هذه الحالة سيفقد الأشخاص خصوصية هويتهم، بسبب انتهاك مهاجمي التصيد الاحتيالي لخصوصيتهم.[3]

وهناك عدة أنواع للتصيد الاحتيالي يتعرض لها الأفراد، يتمثل اهمها في:

- انتحال البريد الإلكتروني:

ويشير إلى إنشاء رسائل بريد الكتروني، تحمل عنوان بريد الكتروني مزيف للمُرسِل، حيث يخدع محتوى البريد الالكتروني المستلم لفتحه، وهنا يقع المستلمون ضحية للتهديدات عند قراءتهم، أو النقر على البريد الالكتروني.

- التصيد الاحتيالي عبر الرسائل النصية القصيرة :

هو نوع آخر من هجمات التصيد الاحتيالي، وتُرسل فيه رسائل التصيد الاحتيالي عبر الرسائل النصية، أو خدمات الرسائل القصيرة (SMS)، وعادة ما يتم مهاجمة الضحايا عن طريق إرسال رسائل نصية، تنتحل هوية محددة، وتُبلغ متلقي الرسائل بحساباتهم.

- التصيد الصوتي:

حيث يجري المخادع هجوماً عبر المكالمات الهاتفية، ويتم استخدام خدمات الهاتف لدفع الضحايا إلى تسليم معلومات وبيانات شخصية للمهاجمين، فيتصل المخادعون بالضحايا متظاهرين بأنهم من جهات رسمية، مثل (الشرطة، الجمارك، البنوك، هيئات قانونية، وغيرها...)، وعادة ما يتبع الضحايا جميع التعليمات، ثم يقعون في فخ التصيد الاحتيالي.

---

1 Yi Yong Lee and Others, Phishing Victimization Among Malaysians Young Adults: Cyber Routine Activities Theory and Attitude in Information Sharing Online, Op Cit, p 179.

2 Vasileios Vlachos and Others, The Landscape of Cybercrime in Greece, Op Cit, p 117.

3 Yi Yong Lee and Others, Phishing Victimization Among Malaysians Young Adults: Cyber Routine Activities Theory and Attitude in Information Sharing Online, Op Cit, p 179.

- التصيد الاحتيالي عبر الرسائل الفورية:

أشارت الأبحاث الحديثة إلى أن مستخدمي الهواتف المحمولة أكثر عرضة لهجمات التصيد الاحتيالي، وحوالي ثلاثة أضعاف من هجمات التصيد الاحتيالي العامة، غالباً ما يرسل المهاجمون رسائل احتيالية عبر الأجهزة المحمولة إلى الضحايا المستهدفين لسببين:

- الأول: انتشار الأجهزة المحمولة على نطاق واسع.
- الثاني: برامج تطبيقات الهواتف المحمولة، بما في ذلك وسائل التواصل الاجتماعي، والرسائل النصية القصيرة، وواتساب، وسكاي بي، والتي عادة ما تمتلك مصادر، أو ميزات أقل تدقيقاً، للتحقق من المصادر الشرعية لرسائل معينة.[1]

وتُعد عمليات الاحتيال المصرفي عبر الإنترنت من أشكال التصيد الاحتيالي، حيث يُشكل الاحتيال المصرفي تهديداً متزايداً للأفراد، وينطوي هذا النوع من الاحتيال على وصول المجرمين إلى الأموال، وتحويلها من الحسابات المصرفية الإلكترونية للأفراد، وغالباً ما يجد الضحايا صعوبة في استرداد الأموال بعد وقوع الاحتيال، الأمر الذي يؤدي إلى الخوف والقلق من الخدمات المصرفية عبر الإنترنت، وعدم الثقة في تلك الخدمات، نظراً للمخاطر المحتملة المرتبطة بالمعاملات المالية عبر الإنترنت، مقارنة بالطرق المصرفية التقليدية.[2]

والجدير بالذكر أن التصيد الاحتيالي (الاحتيال الإلكتروني) يكون غالبا بسبب:

- عدم وعي الأفراد بكيفية استخدام وسائل التواصل الاجتماعي والمواقع الإلكترونية المختلفة.
- إساءة الاستخدام للمواقع الإلكترونية والوصول إلى مواقع غير آمنة.
- نقاط الضعف الموجودة بالأنظمة الإلكترونية، التي تُؤدي إلى سرقة المعلومات وابتزاز الآخرين.[3]

2- الرسائل غير المرغوب فيها:

تتضمن الرسائل غير المرغوب فيها أنواع السلوكيات العدوانية، التي تُمارس عبر الرسائل الإلكترونية، حيث يُعتبر أي سلوك عدواني أو تهديد مباشر، أو غير مباشر، يحدث عبر البريد

1 Yi Yong Lee and Others, Phishing Victimization Among Malaysians Young Adults: Cyber Routine Activities Theory and Attitude in Information Sharing Online, Op Cit, pp 181, 182.

2 Sri Lestari and Others, Navigating Perilous seas: Unmasking Online Banking Frauds, Perceived Usefulness Fear of Cybercrime and Distrust in Online Banking, Safer Communities, Vol 23, No 4, Emerald Publishing Limited, United Kingdom, 2024, p 447.

3 حياة هراكي، واقع جريمة الاحتيال الإلكتروني في التجارة الإلكترونية، مجلة التغير الاجتماعي، المجلد 8، العدد 2، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خيضر ، بسكرة، الجزائر، 2023، ص 52.

الالكتروني، أو الرسائل الفورية، أو شبكات التواصل الاجتماعي، أو المدونات، وما إلى ذلك، سلوك تنمرٍ إلكتروني.[1]

وفي الغالب يتم إرسال الرسائل غير المرغوب فيها عبر منصات التواصل الاجتماعي، وتأخذ أشكالاً منها:

- التهديد بالكتابة: حيث يظهر رسالة إلكترونية مكتوبة ومرسلة من الجاني إلى المجني عليهم مباشرة، تتضمن عبارات تبث الخوف، وعدم الشعور بالأمان، للحصول على مقابل مادي، أو معنوي، وقد تحمل هذه الرسائل تهديداً بإفشاء معلومات وأسرار خاصة.
- التهديد بالقول: وذلك من خلال إرسال رسائل صوتية لنشر الخوف في نفس الضحية، وذلك للحصول على مكاسب مادية أو معنوية.
- التهديد بالصور والفيديوهات: وتكون هذه الصور والفيديوهات تمس جانب من جوانب الحياة الشخصية للضحية، وقد يكون حصول الجاني على هذه الصور والفيديوهات عن طريق كسب ثقة الضحية، أو اختراق أحد حساباته.[2]

3- البريد الإلكتروني:

وهي عباره عن تزييف لعنوان بريد إلكتروني، وهذا يعني أن الرسالة تبدو وكأنها مستلمة من شخص أو مكان آخر، غير المصدر الأصلي أو الفعلي، وتستخدم هذه الإستراتيجيات بشكل شائع في رسائل البريد العشوائي، أو الاحتيال، نظراً لأن المستهلكين يميلون إلى فتح الرسائل المشفرة، أو رسائل البريد الإلكتروني، إذا اعتقدوا أنها مرسلة من قبل جهة موثوقة.[3]

ويمكن استخدام رسائل البريد الالكتروني العشوائية للوصول غير المصرح به للحسابات، ونشر كميات هائلة من البرامج الضارة، على شكل فيروسات حاسوبية، وأحصنة طروادة، وغيرها من البرامج الضارة، وعندما يحصل مجرم على معلومات عن شخص ما، يمكنه انتحال هويته لارتكاب مجموعة واسعة من الجرائم، مثل طلبات القروض، وبطاقات الائتمان المزيفة، وعمليات السحب

1 Vasileios Vlachos and Others, The Landscape of Cybercrime in Greece, Op Cit, p 117.

2 أحلام بو خميس، ندى بوالزيت، الآليات القانونية لحماية سرية المراسلات الإلكترونية في سبيل تعزيز الحق في الخصوصية الرقمية، مجلة الحقوق والحريات، المجلد 12، العدد 1، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2024، ص ص 252، 253.

3 Kuldeep Singh Kaswan and Others, Cybersecurity Law-Based Insurance Market, Op Cit, p 312.

الاحتيالية من الحسابات المصرفية، والاستخدام الاحتيالي لبطاقات الاتصالات الهاتفية، ومن الإستراتيجيات التي يستخدمها المجرمون، الوصول إلى بطاقات الائتمان، وكشوف الحسابات المصرفية، بشكل زائف، للوصول غير المصرح به إلى حسابات الضحايا بطريقة خداعية، لضمان عدم علم الضحايا بما يحدث، حتى يكون المجرم قد نقل الأصول المسروقة إلى ولاية قضائية أخرى، وغالباً ما يستخدم أسماء مستعارة.[1]

ويتم انتحال رسائل البريد الالكتروني، من خلال إنشاء رسائل بريد الكتروني تحمل عنوان مزيف للمُرسِل، ويرسل المحتالون رسائل بريد إلكتروني إلى الضحايا المستهدفين عبر (Outlook أو Gmail)، حيث يخدع محتوى البريد الالكتروني المستلم لفتحه، وقد يقع المستلمون ضحية لتهديدات الخداع عند قراءتهم، أو النقر على البريد الإلكتروني، وعادة ما يستخدم المحتالون أساليب عرض أسماء مؤسسات، أو أفراد موثوق بهم، وإرسال رسائل بريد الكتروني للإيقاع بالضحايا من خلالها.[2]

4- <u>الابتزاز و التشهير الإلكتروني:</u>

يُرتكب الابتزاز الإلكتروني عادة من خلال هجمات حجب الخدمة (إضعاف أو تعطيل إرسال أو استقبال الاتصالات)، وبرامج الفدية التي تستخدم لتشفير بيانات الضحية، ثم يطلب المبتز الإلكتروني المال مقابل فك التشفير، ويميل مرتكب الابتزاز الإلكتروني إلى العمل من دول غير دول ضحاياهم، ويستخدمون حسابات مجهولة، وعناوين بريد إلكتروني مزيفة، وهذا يجعل الابتزاز الإلكتروني خطيراً للغاية، نظراً لانخفاض احتمالية تحديد هوية مجرمي الإنترنت واعتقالهم ومحاكمتهم.[3]

وفي بعض الأحيان يكون الابتزاز جنسياً، وفي هذه الحالة ينتحل الجناة هوية مزيفة على الإنترنت، لحث الضحية على بناء علاقة مع الجاني، ثم يستغل الجاني هذه العلاقة لحث الضحية على إرسال صور فاضحة، لابتزاز الضحية لإرسال أموال، أو المشاركة في أنشطة أخرى غير مشروعة نيابة عنه.

ويتضمن التشهير الإلكتروني جمع ونشر معلومات حساسة عن شخص محدد عبر الإنترنت، مما يُعرض هذا الشخص لمضايقات من قبل الآخرين، ويمكن أن تشمل أنواع المعلومات الشخصية المستخدمة فيها هجمات التشهير(العناوين، وتواريخ الميلاد، وأرقام الضمان الاجتماعي، وأرقام

1 Norman Mugarura and Emma Ssali, Intricacies of Anti-Money Laundering and Cyber-Crimes Regulation in a Fluid Global System, Journal of Money Laundering, Vol 24, No 1, United Kingdom, 2021, p 12.

2 Yi Yong Lee and Others, Phishing Victimization Among Malaysians Young Adults: Cyber Routine Activities Theory and Attitude in Information Sharing Online, Op Cit, p 181.

3 Norman Mugarura and Emma Ssali, Intricacies of Anti-Money Laundering and Cyber-Crimes Regulation in a Fluid Global System, Op Cit, p 12.

الهواتف، وعناوين البريد الإلكتروني، ومعلومات بطاقات الائتمان، وأصحاب العمل، وتفاصيل عن أفراد العائلة..... وغيرها)، ويكون الضحية أحيانا شخصية مشهورة، أو شخصاً يسعى المتصل للانتقام منه.[1]

5- انتهاك حقوق الطبع والنشر والملكية الفكرية:

يشير انتهاك حقوق الطبع والنشر إلى انتهاكات ممتلكات الشخص، وهو الاستخدام غير القانوني لمواد محمية بحقوق الطبع والنشر، مثل المؤلفات.[2]

فالملكية الفكرية هي إبداعات العقل من اختراعات ومصنفات أدبية وفنية وتصاميم وشعارات وأسماء وصور مستخدمة في التجارة، والملكية الفكرية محمية قانونياً بحقوق منها (البراءات، وحق المؤلف، والعلامات التجارية) التي تمكن الأشخاص من كسب الاعتراف أو فائدة مالية من ابتكاراتهم أو اختراعاتهم وبالتالي فإن الملكية الفكرية لم تسلم من استهداف واعتداء مرتكبي الجرائم الإلكترونية ويتم ذلك بقيام الجاني بالاستحواذ على أحد الملكيات الفكرية والاستفادة منها وحرمان المالك من المنفعة أو الفائدة المالية لهذه الملكية.[3]

وبالتالي فان أحد المتضررين من إساءة استخدام شبكة المعلومات أصحاب الملكية الفكرية، سواء ما يتعلق منها بحقوق المؤلف، أو الحقوق المجاورة والمتعلقة بالبرامج، والإصدارات الخاصة بنظم المعلومات، أو بالمصنفات الفكرية، أو الأدبية، أو الأبحاث العلمية، التي أصبحت متاحة على شبكة المعلومات، ويتم نسخها وتداولها دون أن تنسب إلى صاحبها الأصلي، وهو ما يلحق ضرراً بالغاً بهذه الطائفة من الحقوق، التي تعرف بالحقوق الفكرية.[4]

وقد أوضحت نتائج البحث الميداني أن هناك مجموعة من نماذج الجرائم الإلكترونية والتهديدات، تكون أكثر انتشاراً، ويتعرض لها الأفراد بشكل أكبر ، ويتبين ذلك من الجدول التالي :

جدول رقم(12) : يوضح نوع الجريمة التي تم التعرض لها

المتغيرات	التكرار	النسبة	المتوسط	الانحراف	الإجمالي

1 Eileen M. Decker and Others, Bo$_{ts}$, Bytes, and Briefs: Cyber Investigations and Prosecutions Community, Environment and Disaster Risk Management, O$_{p\ Cit}$, pp 34, 35.

2 Kuldeep Singh Kaswan and Others, Cybersecurity Law-Based Insurance Market, O$_{p\ Cit}$, p 312.

3 محمود صالح محمد مثنى، الجريمة الإلكترونية ومراحل تطورها، مرجع سابق، ص 167.

4 لامية طالة، كهيذة سلام، الجريمة الإلكترونية: بُعد جديد لمفهوم الإجرام عبر منصات التواصل الاجتماعي، مرجع سابق، ص 81..

			الحسابي	المعياري	التكرار	النسبة
انتحال البريد الإلكتروني	28	15.1	0.151	0.359	186	100
احتيال مالي	12	6.4	0.065	0.246		
رسائل غير مرغوب فيها	67	36	0.360	0.481		
سرقة معلومات وبيانات شخصية	8	4.3	0.043	0.203		
انتهاك لحقوق الملكية الفكرية	5	2.7	0.027	0.162		
فيرسة تطبيقات وبرامج	28	15.1	0.151	0.359		
إغلاق حساب أو موقع اجتماعي	38	20.4	0.204	0.404		

يتضح من بيانات الجدول السابق أن: أغلب المبحوثين ممن تعرضوا لجرائم إلكترونية بنسبة 36% يشيرون إلى أنهم تعرضوا لرسائل غير مرغوب فيها وعددهم 67 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.360، وانحراف معياري 0.481، و20.4% كانت الجرائم الإلكترونية التي تعرضوا لها إغلاق حساب أو موقع اجتماعي، ويبلغ عددهم 38 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.204، وانحراف معياري 0.404، و15.1% من المبحوثين تعرضوا لفيرسة تطبيقات وبرامج، ويبلغ عددهم 28 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.151، وانحراف معياري 0.359، و15.1% أيضاً تعرضوا لانتحال بريد إلكتروني ويبلغ عددهم 28 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي0.151، وانحراف معياري 0.359،كما أن 6.4% من المبحوثين تعرضوا لاحتيال مالي، ويبلغ عددهم 12 مبحوثاً، و4.3% تعرضوا لسرقة معلومات وبيانات شخصية، وعددهم 8 مبحوثين، و2.7% تعرضوا لانتهاك لحقوق الملكية الفكرية، وعددهم 5 مبحوثين، ويتبين من ذلك أن أكثر نماذج الجرائم الإلكترونية انتشاراً هي الرسائل غير المرغوب فيها، وإغلاق حسابات ومواقع اجتماعية، وانتحال بريد إلكتروني، وفيرسة التطبيقات والبرامج.

ورغم خطورة الجريمة الإلكترونية، فقد كشفت نتائج البحث أن الغالبية ممن تعرضوا لهذه الجرائم لم يقوموا بالإبلاغ عنها ، كما يتضح ذلك من بيانات الجدول التالي :

جدول رقم(13): يوضح مدى الإبلاغ عن الجريمة

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
نعم	19	10.2	0.102	0.304	186	100
لا	167	89.8				

يتبين من بيانات الجدول السابق أن: الغالبية من المبحوثين ممن تعرضوا لجرائم إلكترونية بنسبة 89.8% لم يقوموا بالإبلاغ عن الجريمة التي تعرضوا لها، ويبلغ عددهم 167 مبحوثاً، في حين أن 10.2% من المبحوثين فقط ممن تعرضوا لجرائم إلكترونية قاموا بالإبلاغ عن الجريمة التي تعرضوا لها، ويبلغ عددهم 19 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.102، وانحراف معياري 0.304، ويتبين من ذلك أن غالبية الأفراد الذين يتعرضون لجرائم إلكترونية لا يقومون بالإبلاغ عن تلك الجرائم.

كما أوضحت نتائج البحث أنه حتى في حالة إبلاغ بعض الأفراد عن الجرائم التي تعرضوا لها ، فإنه لم يتم الوصول إلى مرتكبيها ، وهو ما تشير إليه بيانات الجدول التالي :

جدول رقم(14) : يوضح نتائج الإبلاغ عن الجريمة

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
تم القبض على مرتكبي الجريمة	2	10.5	0.105	0.103	186	100
تم أخذ تعويض من مرتكبي الجريمة	1	5.2	0.052	0.073		
لم يتم الوصول إلى مرتكبي الجريمة	12	63.2	0.632	0.237		

عدم الاهتمام من قبل الجهات الأمنية	4	21.1	0.211	0.145		

يتضح من بيانات الجدول السابق أن: الغالبية من المبحوثين ممن قاموا بالإبلاغ عن الجريمة التي تعرضوا لها بنسبة 63.2%، ويبلغ عددهم 12 مبحوثاً، كانت نتائج الابلاغ عدم الوصول إلى مرتكبي الجريمة، وذلك بمتوسط حسابي يُقدر بحوالي 0.632، وانحراف معياري 0.237، و21.1% من المبحوثين وعددهم 4 مبحوثين، كانت نتيجة إبلاغهم عدم الاهتمام من قبل الجهات الأمنية، وذلك بمتوسط حسابي يُقدر بحوالي 0.211، وانحراف معياري 0.145، و10.5% كانت نتيجة إبلاغهم القبض على مرتكب الجريمة، ويبلغ عددهم مبحوثين اثنين، في حين أن مبحوثاً واحداً ممن قاموا بالإبلاغ، كانت نتيجة الإبلاغ أخذ تعويض من مرتكبي الجريمة، ويتبين من ذلك أن الأفراد الذين يتعرضون لجرائم إلكترونية في حالة إبلاغهم بالجريمة التي تعرضوا لها، غالباً لا يتم الوصول إلى مرتكبي تلك الجرائم، نظرا لأن أهم خصائص الجرائم الإلكترونية صعوبة الوصول لمرتكبي تلك الجرائم، لأنها تتم في الفضاء الالكتروني.

كما يؤكد الواقع الاجتماعي أن الغالبية من الأفراد ممن يتعرضون لجرائم إلكترونية، لايقومون بالإبلاغ لعدة أسباب، توضحها بيانات الجدول التالي:

جدول رقم(15): يوضح سبب عدم إبلاغ الأفراد عن الجرائم الإلكترونية

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
الخوف	4	2.2	0.022	0.145	186	100
المكانة الاجتماعية	16	8.6	0.086	0.281		
صعوبة الوصول إلى الجاني	77	41.4	0414.	0.493		
الاعتقاد بأن الإبلاغ لا يفيد	89	47.8	0.478	0.501		

يتضح من بيانات الجدول السابق أن: غالبية المبحوثين ممن تعرضوا لجرائم إلكترونية بنسبة 47.8%، يرون أن سبب عدم إبلاغ الأفراد عن الجرائم التي يتعرضون لها هو الاعتقاد أن الإبلاغ لا يفيد،

ويبلغ عددهم 89 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.478، وانحراف معياري 0.501، و41.4% من المبحوثين يرون أن صعوبة الوصول إلى الجاني أحد أسباب عدم إبلاغ الأفراد عن الجرائم التي يتعرضون لها، ويبلغ عددهم 77 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.414، وانحراف معياري 0.493، و8.6% يرون أن سبب عدم إبلاغ الأفراد المكانة الاجتماعية لهم، ويبلغ عددهم 16 مبحوثاً، في حين أن 2.2% من المبحوثين، يرون أن سبب عدم الإبلاغ هو الخوف، ويتبين من ذلك أن الأفراد الذين يتعرضون لجرائم إلكترونية لا يقومون بالإبلاغ عن تلك الجرائم، بسبب الاعتقاد بأن الإبلاغ لا يفيد، نظرا لصعوبة الوصول إلى مرتكبي تلك الجرائم.

ويجدر الإشارة إلى أن هذه النماذج من الجرائم الإلكترونية ترتكب من قِبل مجموعة من الطوائف تتمثل في:

- أولا: المخترقون أو المتطفلون (الهاكرز Hackers - الكريكرز Crackers)

يُعَدُّ (الهاكرز) متطفلين يتخذون إجراءات أمن النظم والشبكات، لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية، وإنما ينطلقون من دوافع التحدي وإثبات المقدرة، أما (الكريكرز) فإن اعتداءاتهم تعكس ميولاً إجرامية خطيرة، ناتجة عن رغباتهم في إحداث التخريب، فمصطلح (الكريكرز) مرادف للهجمات الحاقدة والمؤذية، في حين أن مصطلح (الهاكرز) مرادف لهجمات التحدي.

- ثانيا: مجرمو الكومبيوتر المحترفون

تتميز هذه الطائفة بسعة الخبرة والإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم والتخطيط للأنشطة التي ترتكب من قبل أفرادها، لذلك تُعد هذه الطائفة الأخطر من بين مجرمي التقنية، حيث تهدف اعتداءاتهم إلى تحقيق مكاسب مادية، سواء لهم أو للجهات التي تقوم بتكليفهم.

- ثالثا: الحاقدون

هذه الطائفة غالباً لا تتوافر لديها أهداف وأغراض للجريمة، فهم لا يسعون إلا لإثبات قدرات تقنية أو مهارية، ولا يسعون إلى مكاسب مادية، وإنما يحرك أنشطتهم الرغبة في الانتقام، ولا يمتلكون المعرفة التقنية الاحترافية، ويستخدمون تقنيات زراعة الفيروسات، والبرامج الضارة، وتخريب النظام، أو إتلاف البيانات، أو تعطيل بعض الأنظمة.

- رابعا: طائفه صغار السن

يطلق عليهم البعض (صغار نوابغ المعلوماتية)، فهم الشباب المفتون بالمعلوماتية، والحاسبات الآلية، ومن بينهم فئة لا تزال دون سن الأهلية، مولعون بالحوسبة والاتصال، دافعهم التحدي لبرامج ورموز الحاسوب.

- خامسا: محترفو الإجرام

يتمتعون بقدره عالية من الذكاء الإلكتروني، ولديهم إلمام جيد بالتقنيات، ويُعَدُّون مستخدمين مثاليين من قبل الجهات العاملين لديها.[1]

وقد أكدت نتائج البحث أن الأشخاص الذين يتعرضون لهذه الأنواع من الجرائم الإلكترونية ، لا يعرفون مرتكبيها ، وإلى أي نوع ينتمون إلى الطوائف السابقة، وهو ما تشير إليه بيانات الجدول التالي :

جدول رقم(16): يوضح مدى معرفة مرتكبي الجريمة

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
نعم	34	18.3	0.183	0.388	186	100
لا	152	81.7				

يتضح من بيانات الجدول السابق أن: الغالبية من المبحوثين ممن تعرضوا لجرائم إلكترونية بنسبة 81.7% ويبلغ عددهم 152 مبحوثاً، لا يستطيعون معرفة مرتكبي الجريمة، في حين أن 18.3% من المبحوثين، ويبلغ عددهم 34 مبحوثاً، تمكنوا من معرفة مرتكبي الجريمة، وذلك بمتوسط حسابي يُقدر بحوالي 0.183، وانحراف معياري 0.388، ويتبين من ذلك أن هناك تفاوتاً واضحاً بين الأفراد في معرفة مرتكبي الجريمة، وأن الغالبية من الأفراد لا يستطيعون معرفة مرتكبي الجرائم الإلكترونية.

رابعاً : الجريمة الإلكترونية وانعكاسها على الأمن الاجتماعي للأفراد

[1] سمير شعبان، الجريمة الإلكترونية: مقارنة تحليلية لتحديد مفهوم الجريمة والمجرم، مجلة دراسات وأبحاث، العدد 1، الجزائر، 2009، ص 124: 127.

يشير الواقع الاجتماعي إلى أن الجرائم الإلكترونية لها انعكاسات وتأثيرات سلبية على الأمن الاجتماعي للأفراد، ومن المتعارف عليه أن المُشَرع في كل النظم القانونية يضع القوانين بغرض حماية الأفراد من كل اعتداء قد يتعرضون إليه، ومع الانتشار الواسع للتكنولوجيا وظهور العالم الإلكتروني، أصبحت الحياة الشخصية للأفراد وأمنهم في خطورة، نتيجة وجود إمكانية الوقوع ضحية للجرائم الإلكترونية، مثل الانتحال والسرقة والاطلاع على أدق البيانات والمعلومات الخاصة بالأفراد، والاستعمال السيء لها، إلى جانب السب وتشويه السمعة وغيرها من الأفعال اللاأخلاقية، بغرض المساس بشرف الشخص أو النيل من كرامته.[1]

وقد يعاني ضحايا الجرائم الإلكترونية من اضطرابات، وعدم القدرة على التكيف الاجتماعي، والخوف وعدم الثقة من إقامة علاقات اجتماعية، والشعور بالعزلة، وصعوبة التعامل مع الآخرين، وضعف الثقة بالنفس، وكثرة الشك وفقدان للأمن الاجتماعي، نتيجة الترهيب النفسي والقلق والتوتر، وتكون هذه التأثيرات أكثر حدة على الأفراد الذين يستخدمون تكنولوجيا المعلومات والاتصالات بدون خبرة كافية، ويفتقرون إلى الممارسات والمهارات الرقمية والقدرات التي تقيس سلامة المحتوى عبر الإنترنت، مما يجعلهم أكثر عرضة للتهديدات والمخاطر التكنولوجية، خاصة الابتزاز الالكتروني.[2]

ويقوم الأمن الاجتماعي على عدة مقومات تُعد الأساس الذي ينشئ عملية الأمن، وأهمها:

1- إشباع الحاجات

يتميز السلوك الإنساني بأن وراءه دافعاً معيناً، ويسعى لتحقيق هدف أو إشباع حاجة، لذلك يكون هناك سبب وراء ذلك السلوك، وفي حالة إشباع الحاجة أو تحقيق الهدف، يشعر الفرد بحالة من التوازن والراحة، وفي حالة الإخفاق في تحقيق الهدف، يشعر الفرد بعدم الراحة، وعدم التوازن وافتقارٍ للأمن الاجتماعي.[3]

2- القيم والمعايير الاجتماعية

يرى علماء الاجتماع أن القيم تعبر عن الواقع، بصفتها حقائق واقعية توجد في المجتمع، وتعمل على توجيه سلوك الأفراد، ولا ينفصل وجودها عن معايير الجماعة، وترتبط بجوانب الحياة الاجتماعية والثقافية والنفسية، فالقيم تمارس دوراً في تحقيق الضبط الاجتماعي، لأن المجتمع يتمكن من خلالها التمييز بين

---

[1] أمينة إبراهيم الأميري، أحمد فلاح العموش، أثر استخدام التكنولوجيا كنشاط روتيني في زيادة معدلات الجريمة، مجلة كلية الآداب، العدد 143، جامعة بغداد، العراق، 2022، ص ص 308، 309.

[2] شريف محمد السويدي، زيزت مصطفى عبده نوفل، دور الأسرة في تدعيم الأمن السيبراني لمواجهة الابتزاز الإلكتروني: دراسة كيفية، مجلة كلية الآداب، العدد 147، جامعة بغداد، العراق، 2023، ص 433.

[3] أحمد حسن عبد الله، الأمن الاجتماعي ومقوماته: دراسة نظرية تحليلية ، مرجع سابق ، ص 10.

السلوك السوي والسلوك غير السوي، ولذلك فالقيم لها دورٌ هامٌ في تنظيم الحياة الاجتماعية، وفي حالة عدم التزام بعض الأفراد بالقيم الرئيسة للمجتمع، تظهر سلوكيات غير سوية، ينتج عنها شعور الأفراد بانعدام الأمن الاجتماعي.[1]

3- الاستقرار السياسي وتوافر الأجهزة المختصة القادرة على تحقيق الأمن

وهذا من المقومات الرئيسة لتحقيق الأمن الاجتماعي، وذلك من خلال تحقيق الحقوق الدستورية الشرعية للفرد عبر حكم رادع يراعي شئون المواطنين، ويعمل على توفير أسباب الطمأنينة لهم، حيث يتطلب الاستقرار السياسي دعائم تحقق الحقوق الرئيسة للمواطنين، في ظل أنظمة ومؤسسات مختصة قادرة على تأمين المجتمع، وتتمثل في:

- جهاز أمني قوي وفعال ومستعد للتدخل دائما لرعاية الأمن بوجه عام.
- جهاز قضائي عادل وحاسم يضمن حقوق الجميع، ويفصل في الأحكام بسرعة وحسم.
- تخطيط متكامل وسياسة جنائية سليمة وتعاون وثيق بين كافة المؤسسات لتوفير مقومات الأمن الاجتماعي للأفراد.[2]

وقد أكدت نتائج البحث مدى خطورة الجرائم الإلكترونية على الأمن الاجتماعي ، كما يتضح ذلك من الجدول التالي :

جدول رقم(17) : يوضح مدى خطورة الجرائم الإلكترونية على الأمن الاجتماعي للأفراد

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
مرتفع	155	83.4	1.172	0.392	186	100
متوسط	30	16.1				
منخفض	1	0.5				

يتضح من بيانات الجدول السابق أن: الغالبية من المبحوثين ممن تعرضوا لجرائم إلكترونية بنسبة 83.4%، يرون أن الجرائم الإلكترونية ذات خطورة (مرتفعة) على الأمن الاجتماعي للأفراد، ويبلغ عددهم

[1] المرجع السابق ، ص ص 11، 12.
[2] إبراهيم بن مبارك بن موسى الجوير، تحقيق الأمن الاجتماعي، مرجع سابق، ص ص 159، 160.

155 مبحوثاً، و16.1% من المبحوثين يرون أن مستوى خطورة الجرائم الإلكترونية على الأمن الاجتماعي للأفراد (متوسط)، ويبلغ عددهم 30 مبحوثاً، وأن مبحوثاً واحداً فقط يرى أن مستوى الخطورة (منخفض)، وذلك بمتوسط حسابي يُقدر بحوالي 1.172، وانحراف معياري 0.392، ويشير ذلك إلى أن مستوى خطورة الجرائم الإلكترونية على الأمن الاجتماعي للأفراد مرتفع بشكلٍ كبير.

كما أوضحت نتائج البحث أن للجرائم الإلكترونية تأثيرات سلبية على الأمن الاجتماعي للأفراد، كما يتبين ذلك من الجدول التالي:

جدول رقم(18): يوضح كيفية تأثير الجرائم الإلكترونية على الأمن الاجتماعي للأفراد

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
عدم الثقة في استخدام تكنولوجيا الاتصالات والمعلومات	70	37.6	0.376	0.486	186	100
الخوف من أي معاملات عبر الإنترنت	65	34.9	0.449	0.471		
تجنب إقامة علاقات اجتماعية عبر وسائل التواصل الاجتماعي	23	12.4	0.124	0.330		
الإصابة بالقلق والتوتر	28	15.1	0.150	0.359		

يتضح من بيانات الجدول السابق أن: الغالبية من المبحوثين ممن تعرضوا لجرائم إلكترونية بنسبة 37.6%، وعددهم 70 مبحوثاً، يرون أن الجرائم الإلكترونية تؤثر على الأمن الاجتماعي للأفراد من خلال عدم الثقة من جانب الأفراد في استخدام تكنولوجيا الاتصالات والمعلومات، وذلك بمتوسط حسابي يُقدر بحوالي 0.376، وانحراف معياري 0.486، و34.9% من المبحوثين يرون أن تأثير الجرائم الإلكترونية على الأمن الاجتماعي للأفراد يتمثل في الخوف من أي معاملات عبر الإنترنت، ويبلغ عددهم 65 مبحوثاً،

وذلك بمتوسط حسابي يُقدر بحوالي 0.449، وانحرف معياري 0.471، و15.1% يرون أن التأثير يكون في الإصابة بالقلق والتوتر ، وعددهم 28 مبحوثاً، و12.4% يرون تجنب إقامة علاقات اجتماعية عبر وسائل التواصل الاجتماعي، وعددهم 23 مبحوثاً، ويتبين من ذلك أن هناك تأثيرات مختلفة للجرائم الإلكترونية على الأمن الاجتماعي للأفراد، أهمها أنها تخلق نوعاً من عدم الثقة لدى الأفراد في استخدام تكنولوجيا الاتصالات والمعلومات، إلى جانب الخوف من التعامل عبر الإنترنت.

جدول رقم(19): يوضح العلاقة بين الخصائص الاجتماعية للمبحوثين وتقييمهم لخطورة الجرائم الإلكترونية على الأمن الاجتماعي للأفراد

المتغيرات		مرتفع		متوسط		منخفض		الإجمالي		قيمة مربع كاي	درجات الحرية	قيمة معامل كيندل
		ع = 155		ع = 30		ع = 1		ع = 186				
		العدد	%	العدد	%	العدد	%	العدد	%			
النوع	ذكر	105	56.5	23	12.4	1	0.5	129	69.4	1.386	2	0.079
	أنثي	50	26.9	7	3.8	-	-	57	30.6			

السن	15 : 25 عاماً	73	39.2	19	10.2	1	0.5	93	50	4.357	6	-0.104
	25 : 35 عاماً	50	26.9	6	3.2	-	-	56	30.1			
	35 : 45 عاماً	19	10.2	2	1.1	-	-	21	11.3			
	45 : 55 عاماً	13	7	3	1.6	-	-	16	8.6			
المستوى التعليمي	يقرأ ويكتب	3	1.6	-	-	-	-	3	1.6	4.759	10	-0.004
	ابتدائي	3	1.6	-	-	-	-	3	1.6			
	إعدادي	8	4.3	2	1.1	-	-	10	5.4			
	ثانوي	36	19.4	7	3.8	1	0.5	44	23.7			
	جامعي	97	52.2	20	10.8	-	-	117	62.9			
	فوق جامعي	8	4.3	1	0.5	-	-	9	4.8			
محل الإقامة	حضر	137	73.7	29	15.6	1	0.5	167	89.8	1.993	2	0.103
	ريف	18	9.7	1	0.5	-	-	19	10.2			

- توضح بيانات الجدول السابق العلاقة بين الخصائص الاجتماعية للمبحوثين، ورؤيتهم لمستوى خطورة الجرائم الإلكترونية على الأمن الاجتماعي للأفراد، حيث تبين أن 56.5% تقريباً من المبحوثين (الذكور) يرون أن مستوى خطورة الجرائم الإلكترونية على الأمن الاجتماعي للأفراد مرتفع، و12.4%منهم يرون أن مستوى خطورة الجرائم الإلكترونية على الأمن الاجتماعي متوسط، و0.5% فقط يرون أن مستوى الخطورة منخفض، في حين أن 26.9% من المبحوثين (الإناث) يرون أن مستوى خطورة الجرائم الإلكترونية على الأمن الاجتماعي للأفراد مرتفع، و3.8% يرون أن مستوى الخطورة متوسط، وقد بلغت

قيمة مربع كاي 1.386، وهي قيمة غير معنوية، حيث بلغت قيمة معامل كندل 0.079، ويشير ذلك إلى عدم وجود علاقة بين النوع ورؤية مدى خطورة الجريمة الإلكترونية على الأمن الاجتماعي للأفراد، فكلٌ من الذكور والإناث يشيرون الى خطورة الجريمة الإلكترونية بشكلٍ كبير.

- ويشير الجدول إلى أن 39.2% من المبحوثين الذين تقع أعمارهم في الفئة العمرية (15 إلى 25 عاماً)، يرون أن مستوى خطورة الجرائم الإلكترونية على الأمن الاجتماعي للأفراد مرتفع، و10.2% من نفس الفئة العمرية يرون أن مستوى الخطورة متوسط، و0.5% فقط بمعدل مبحوث واحد، يرى أن مستوى الخطورة منخفض، و26.9% من المبحوثين في الفئة العمرية (25 إلى 35 عاماً)، يرون أن مستوى خطورة الجرائم الإلكترونية مرتفع، و3.2% من نفس الفئة يرون أن المستوى متوسط، و10.2% في الفئة العمرية (35 إلى 45 عاماً)، يرون أن مستوى الخطورة مرتفع، و1.1% يرون أن المستوى متوسط، و7% من المبحوثين في الفئة العمرية (45 إلى 55عاماً)، يرون أن مستوى الخطورة مرتفع، و1.6% يرون أنه متوسط ، وقد بلغت قيمة مربع كاي 4.357، وهي قيمة تشير إلى وجود فروق بين الفئات العمرية، وتقييم خطورة الجرائم الإلكترونية على الأمن الاجتماعي، حيث بلغت قيمة معامل كندل - 0.104، ويشير ذلك إلى وجود ارتباط سلبي بين السن ورؤية المبحوثين لمستوى خطورة الجرائم الإلكترونية، فكلما زاد السن قلّت رؤية المبحوثين لمستوى خطورة الجرائم، وكلما قل السن كانت رؤية المبحوثين للجرائم أكثر خطورة، نظراً لأن تلك الفئة هي الأكثر استخداماً لتكنولوجيا الاتصالات والمعلومات، وبالتالي أكثر عرضة للجرائم وإدراك مدى خطورتها.
- كما يتبين من الجدول السابق أن 52.2% من المبحوثين من ذوي التعليم (الجامعي)، يرون أن مستوى خطورة الجرائم الإلكترونية على الأمن الاجتماعي مرتفع، و10.8% من نفس المستوى التعليمي يرون أن مستوى الخطورة متوسط، و19.4% من ذوي التعليم (الثانوي)، يرون أن مستوى خطورة الجرائم الإلكترونية مرتفع، و3.8% من المبحوثين من نفس المستوى التعليمي، يرون أن مستوى الخطورة متوسط، و0.5% فقط بواقع مبحوث واحد، يرى أن مستوى الخطورة منخفض، كما أن 4.3% من المبحوثين من ذوي التعليم (الإعدادي) يرون أن مستوى الخطورة مرتفع، و1.1% يرون المستوى متوسط ، و1.6% من ذوي التعليم (الابتدائي) يرون الخطورة مرتفعةً، ونفس النسبة ممن (يعرفون القراءة والكتابة) يرون أن مستوى الخطورة مرتفع، وقد بلغت قيمة مربع كاي 4.759، وهي قيمة تشير إلى وجود فروق بين الفئات التعليمية وتقييم خطورة الجرائم الإلكترونية على الأمن الاجتماعي للأفراد، حيث بلغت قيمة معامل كندل -0.004، ويتبين من ذلك أن المستويات التعليمية الأعلى أكثر إدراكاً لخطورة الجرائم الإلكترونية .

- وأيضاً يتضح من الجدول السابق أن 73.7% من المبحوثين المقيمين في (الحضر) يرون أن مستوى خطورة الجرائم الإلكترونية على الأمن الاجتماعي مرتفع، و15.6% منهم يرون مستوى الخطورة متوسط، و0.5% فقط بواقع مبحوث واحد يرى مستوى الخطورة منخفض، في حين أن 9.7% من المبحوثين المقيمين في (الريف) يرون مستوى الخطورة مرتفعاً، و0.5% ويمثل مبحوثاً واحداً يرى مستوى الخطورة متوسطاً، وقد بلغت قيمة مربع كاي 1.993، وهي قيمة غير دالة إحصائياً، حيث بلغت قيمة معامل كندل 0.103، ويشير ذلك إلى أن محل الإقامة (الحضر – الريف) ليس له تأثير كبير على رؤية المبحوثين لمستوى خطورة الجرائم الإلكترونية، فكلٌ من المقيمين في الحضر والريف ممن تعرضوا لجرائم إلكترونية تقييمهم لهذه الجرائم أنها تشكل خطورة كبيرة على الأمن الاجتماعي للأفراد.

خامساً : إستراتيجيات الأمن السيبراني لمواجهة الجريمة الإلكترونية

تواجه الأساليب التقليدية لمكافحة الجريمة صعوبات في عالم التكنولوجيا المترابط الذي نعيش فيه الآن، ووكالات إنفاذ القانون التي تقع على عاتقها المهمة الرئيسة لمكافحة الجريمة، وتلعب دوراً مهماً في منعها ، تعمل إلى حدٍ كبيرٍ في سياق تحديد هوية المجرمين والقبض عليهم، وغالباً ما تُضعف أساليب عمل مجرمي الإنترنت أساليب الشرطة التقليدية، فإن إخفاء الهوية الذي يوفره الإنترنت للمجرمين، والتشتت الجغرافي للمجرمين والضحايا، وتواجد المجرمين عادةً خارج نطاق السلطة القضائية التي تقع فيها الجريمة، وبالتالي خارج نطاق سلطات إنفاذ القانون المحلية، يجعل الجريمة الإلكترونية مشكلة صعبة على سلطات إنفاذ القانون، ولذلك ثمة حاجة ماسة وملحة لابتكار طرق مختلفة لمكافحة الجريمة الإلكترونية.[1]

وتُعد الجرائم الإلكترونية من أكبر التهديدات للاستقرار العالمي، من حيث أمن البنية التحتية الوطنية الحيوية، وسلامة الفضاء الإلكتروني، والتنمية الاقتصادية الرقمية، بالإضافة إلى حماية البيانات الشخصية الخاصة والسرية، خاصة في ظل التكلفة المرتفعة لتلك الجرائم، حيث كلفت الجرائم الإلكترونية العالم حوالي تريليوني دولار أمريكي اعتباراً من عام 2020، وهي تُهدد بارتفاع هذا الرقم إلى ثلاثة تريليونات دولار أمريكي بحلول عام 2030، وقد استلزمت طبيعة الجرائم الإلكترونية التي تستحوذ على مبالغ طائلة من المال في جميع أنحاء العالم السعي نحو تحقيق أمن سيبراني فعَّال على الصعيدين الوطني والدولي، من خلال تحديد مواطن الضعف المحتملة، والمهاجمين المشتبه بهم الذين يجب منعهم من الوصول إلى البيانات، أو مهاجمة أجهزة الكمبيوتر وغيرها من الأدوات التي تمكنهم من تكبيد أضرار.[2]

1 Jacqueline M. Drew, A Study of Cybercrime Victimization and Prevention: Exploring The use of Online Crime Prevention Behaviors and Strategies, Op Cit, p 18.

2 Babayo sule and Others, Countering CyberCrimes as The Strategy of Enhancing Sustainable Digital Economy in Nigeria, Op Cit, p 1558.

ورغم ما يشهده العالم من تزايد لمعدلات الجريمة الإلكترونية، لا زال هناك الكثير من الدول لم تطور أنظمتها التشريعية وقوانينها الرادعة وأجهزتها، بما يمكّنها من مواكبة التقدم في مجال الجريمة الإلكترونية وأساليبها، وهذا الضعف يُعد عاملاً حاسماً في التشجيع على ارتكاب الجرائم الإلكترونية، دون خوف من الإدانة أو العقاب، وبالتالي لا بُد من تدعيم المنظومة التشريعية والأمنية بشكلٍ يتجاوب مع تطورات الجريمة الإلكترونية وتعقيداتها.[1]

وهنا يظهر دور الأمن السيبراني كإستراتيجية لمواجهة الجريمة الإلكترونية، وقد ظهر الأمن السيبراني كخطاب أمني في ستينيات القرن الماضي، بعد النجاح في اختراع الحاسوب الرئيس، وكان هذا أول نموذج للابتكار الحاسوبي، لتسهيل الأنشطة والعمليات التجارية، وفي تلك الفترة كانت أجهزة الكمبيوتر محمية أو مؤمنة بحُراس ماديين (عصر الأمن السيبراني المادي)، وكان مديرو أجهزة الكمبيوتر من هذا النوع على دراية تامة بالمخاطر الأمنية، لكن مستوى السرية والسلامة وتوافر المعلومات لم يكن يرقى إلى المستوى المطلوب، وفي الفترة ما بين سبعينيات وثمانينيات القرن الماضي ازدادت الثورة التكنولوجية، مما أدى إلى إنتاج أجهزة الكمبيوتر الصغيرة، ومع ذلك فإن طبيعة الأمن هي الحماية المادية، وتم تمكين الانتقال من الأمن المادي إلى الأمن السيبراني في أواخر التسعينيات، عندما تم إدخال الاتصالات عبر الإنترنت، مما أدى إلى هجمات الفيروسات والقرصنة وسرقة البيانات عبر الإنترنت، وتفاقم الوضع مع تطور الهواتف المحمولة وأجهزة الكمبيوتر الشخصية الصغيرة، الأمر الذي أصبحت معه جميع دول العالم والمنظمات الوطنية والدولية والأفراد والمؤسسات أهدافاً محتملة لمجرمي الإنترنت، مما يستلزم اتخاذ تدابير لمواجهة هذه الهجمات، وبالتالي بذل جهود لتعزيز الأمن السيبراني.[2]

وهناك مجموعه من المبادئ الإستراتيجية للأمن السيبراني، أهمها:

1- السرية: الخصوصية والأمان هما القدرة على إخفاء المعلومات عن غير المسموح لهم بالاطلاع عليها، وبالتالي حماية الأفراد من الوصول غير القانوني، حيث يُعد إخفاء الهوية سمة أمنية رئيسة، وفي معظم السياقات والظروف يجب الحفاظ على المعلومات المهمة، مثل البيانات الطبية، والخاصة، وحماية الهويات، والوصول غير المرغوب فيه.

2- النزاهة: يشير الحفاظ على السرية إلى حماية المعلومات من التغيير غير القانوني، أو غير المتوقع، أو غير المقصود، فالنزاهة سمة أمنية ضرورية لتقديم خدمات موثوقة لمستخدمي إنترنت الأشياء.

---

[1] العمري عيسات، عبد الرؤوف بوعزة، الجريمة الإلكترونية لدى المراهقين: دوافع الإقبال وآليات الضبط الاجتماعي، مجلة علوم الإنسان والمجتمع، المجلد 11، العدد 1، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خيضر بسكرة، الجزائر، 2022، ص 142.

2 Babayo sule and Others, Countering Cybercrimes as The Strategy of Enhancing Sustainable Digital Economy in Nigeria, Op Cit, p 1559.

3- التوافر: يتمثل في إمكانية وصول جهاز الكمبيوتر المستخدم إلى المعلومات في أي وقت مطلوب، لذلك أصبحت أموال إنترنت الأشياء متاحة بشكل روتيني لتلبية المتطلبات، أو منع الخسائر.[1]

ويتم الاعتماد على نظرية (دوافع الحماية) (Protection Motivation Theory) (PMT) في أبحاث الأمن السيبراني لتفسير سبب عدم تبني الأفراد دائماً لسلوك الامتثال الأمني، وقد مثل نموذج (دوافع الحماية) (PMT) إطاراً مفيداً في دراسة العمليات المعرفية عند مواجهة الأفراد للتهديدات الإلكترونية، كما يحدد نموذج (دوافع الحماية) أسباب فشل الأفراد في حماية أنظمتهم وشبكاتهم، حتى في حالة امتلاكهم معرفة واسعة بأمن المعلومات، على سبيل المثال، غالباً ما يدرك الأفراد أن التهديدات ليست خطيرة، ولن تسبب أي ضرر، وبالتالي يكون إدراك بعض الأفراد لشدة التهديد المدركة ضعيفة.[2]

فالمشكلة الرئيسة تكمن في عدم فهم خطورة الهجمات الإلكترونية من جانب الأفراد، كما لا يتبنى العديد من الأفراد ممارسات الأمن السيبراني المناسبة، إلا بعد أن يكونوا قد تعرضوا بالفعل لجرائم إلكترونية، مثل تغيير كلمات المرور بانتظام، وكلمات المرور القوية، وتحديث البرامج، وغيرها من التدابير الوقائية، حتى في حالة الوعي بالتهديدات لا يعني فهم النتائج المحتملة للجرائم الإلكترونية، وبالتالي من الضروري زيادة اهتمام الأفراد بالأمن السيبراني، وتوعيه الأفراد بالمخاطر والعواقب الحقيقية للجرائم الإلكترونية، وهو ما يؤدي إلى تعزيز الأمن الانساني والاجتماعي للأفراد، نظراً لأن مجال الأمن السيبراني يُمكن من منع الجرائم الإلكترونية، من خلال تبني ممارسات أمنية تساعد على جعل البيئة الرقمية والمجتمع المعلوماتي أكثر أماناً.[3]

ومن الجدير بالذكر أنه قد يكون لشبكات التواصل الاجتماعي دورٌ في الامتثال للأمن السيبراني، حيث تُعد منصات التواصل الاجتماعي وسيلة لتثقيف المستخدمين حول تعزيز استعدادهم للمخاطر، ويمكن للأفراد تقييم مدى نجاح استخدام الاستجابات الدفاعية، بالاعتماد على المعرفة التي يكتسبونها من وسائل التواصل الاجتماعي، مما يزيد من إدراكهم للتهديد.[4]

---

1 Kuldeep Singh Kaswan and Others, Cybersecurity Law-Based Insurance Market, Op Cit, p 308.

2 Hassan Jamil and Others, Human-Centric Cyber Security: Applying Protection Motivation Theory to Analyze Micro Business Owners' Security Behaviors, Op Cit, p 51.

3 Ines Gil Costa, Ameacas Ciberneticas Os Seeus Impactos an Seguranca Humana, Grau de Mastre em Relacoes Internacionis, Universidade Autonoma de Lisboa, Portuguesa, 2023, pp 84, 85.

4 Dien Van Tran and Others, Exploring The Influence of Government Social Media on Cybersecurity Compliance: Employee Attitudes, Motivation and Behaviors, Journal of Asia Business Studies, Vol 18, No 1, United Kingdom, 2024, p 208.

ومن ثم يُعد الأمن السيبراني هو الحل الأمثل لمتابعة الاستخدام الواسع للإنترنت وتطبيقاته وأنظمته المختلفة، للتقليل من المخاطر التي تنشأ من سوء الاستخدام، وعدم المعرفة الجيدة بكيفية التعامل مع تكنولوجيا المعلومات، فالأمن السيبراني يحمي الأفراد من التعرض لأي أذى على شبكة الإنترنت، وبالتالي يمثل الأمن السيبراني أحد الركائز الرئيسة للتصدي للهجمات الإلكترونية، والحد من مخاطرها، من خلال المحافظة على أمن بيئة الاتصالات، وتأمين الأجهزة التقنية بكافة أشكالها وأنواعها، وبما تحتويه من أنظمة وبرامج وبيانات ومعلومات، يتم تداولها عبر الإنترنت، والحفاظ على سريتها.[1]

كما يستطيع الأفراد حماية أنفسهم من بعض مخاطر الجرائم الإلكترونية من خلال:

- الاسعافات الأولية: تتمثل الاسعافات الأولية في إعداد نسخ احتياطية من البيانات والبرامج.
- إجراءات فنية: كعدم استخدام البرامج المسروقة، للتقليل من احتمالات العدوى من الفيروسات، وحماية البرامج الأصلية، وعدم استخدام البرامج المجانية.[2]
- تأمين الأجهزة الإلكترونية: كل مستخدم للإنترنت يجب أن يحتوي جهازه الشخصي على برامج خاصة بالحماية، وبرامج لمقاومة الفيروسات والرسائل الإلكترونية الخادعة، لحماية الأفراد منها وتأمين حساباتهم الشخصية أثناء استخدام الإنترنت.[3]

وقد أشارت نتائج البحث أنه يمكن للأفراد حماية أنفسهم من الوقوع ضحايا للجريمة الإلكترونية من خلال عدة أساليب، أهمها تجنب فتح الرسائل غير المعروفة، كما تشير بيانات الجدول التالي :

جدول رقم(20) : يوضح كيفية حماية الأفراد أنفسَهم من الجريمة الإلكترونية

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
تشفير المعلومات	29	15.6	0.156	0.364	186	100

[1] شريف محمد السويدي، زيزت مصطفى عبده نوفل، دور الأسرة في تدعيم الأمن السيبراني لمواجهة الابتزاز الإلكتروني: دراسة كيفية، مرجع سابق، ص 434.

[2] ليندة شرابية، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية: الاتجاهات الدولية في مكافحة الجريمة الإلكترونية، مجلة دراسات وأبحاث، العدد 1، جامعة الجلفة، الجزائر، 2009، ص 249.

[3] ريهام رمضان سيد، إستراتيجية مقترحة لتجنب الجريمة المعلوماتية على المستوى العربي: بشكل عام وفي مصر بشكل خاص، المجلة العلمية ملحق، كلية الآداب، جامعة أسيوط، 2015، ص 83.

استخدام برامج وقاية من الفيروسات	28	15.1	0.150	0.359		
تجنب فتح الرسائل غير المعروفة	65	34.9	0.349	0.478		
عمل نسخ احتياطية من البيانات والبرامج	8	4.3	0.43	0.203		
عدم نشر معلومات شخصية	56	30.1	0.301	0.460		

يتضح من بيانات الجدول السابق أن: الغالبية من المبحوثين ممن تعرضوا لجرائم إلكترونية بنسبة 34.9%، ويبلغ عددهم 65 مبحوثاً، يرون أن الأفراد يمكن أن يحموا أنفسهم من الجرائم الإلكترونية من خلال تجنب فتح الرسائل غير المعروفة، وذلك بمتوسط حسابي يُقدر بحوالي 0.349، وانحراف معياري 0.478، و30.1% من المبحوثين، يرون عدم نشر معلومات شخصية قد يحمي الأفراد من الجريمة الإلكترونية، ويبلغ عددهم 56 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.301، وانحراف معياري 0.460، و15.6% يرون تشفير المعلومات وسيلة للحماية من الجريمة الإلكترونية، ويبلغ عددهم 29 مبحوثاً، و15.1% يرون استخدام برامج وقاية من الفيروسات، ويبلغ عددهم 28 مبحوثاً، و4.3% يرون عمل نسخ احتياطية من البيانات والبرامج، ويتبين من ذلك أن أهم الأساليب التي يمكن أن يتخذها الأفراد لحماية أنفسهم من الجرائم الإلكترونية، تتمثل في تجنب فتح الرسائل غير المعروفة، وعدم نشر معلومات شخصية .

وفي ظل التكنولوجيا والانتشار الإلكتروني أصبحت الجرائم الإلكترونية تتطلب المزيد من الجهود للمواجهة، الأمر الذي يجعل من الضروري وجود تعاون دولي أكثر فعالية، ورغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة الإلكترونية، إلا أن هناك عوائق وتحديات تحول دون ذلك، وتجعل هذا التعاون صعباً، وتتمثل أهم هذه العوائق في:

1- عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي، إلى جانب عدم اتفاق النظم القانونية في بلدان العالم على صور محددة يندرج ضمنها ما يسمى بإساءة استخدام نظم المعلومات.

2- عدم وجود معاهدات بين الدول كافية وذات فعالية لمواجهة الجريمة الإلكترونية، وحتى في حالة وجودها، فإنها تبقى قاصرة عن تحقيق الحماية المطلوبة، في ظل التقدم السريع لنظم الحاسب الآلي والإنترنت.

3- عدم وجود تنسيق بين الدول فيما يتعلق بالإجراءات الجنائية للجريمة الإلكترونية، لا سيما أن الحصول على أدلة جنائية لهذه الجرائم خارج حدود الدولة أمرٌ صعبٌ.[1]

4- إن الضُباط المختصين في التحقيق بالجرائم الإلكترونية يصطدمون بالتعقيدات الخاصة بالقوانين والأحكام، واختلافها بين الدول، ومرتكبو الجرائم الإلكترونية يستغلون هذه الثغرة القانونية المتمثلة في الاختلافات الإجرائية والقانونية بين البلدان، فيما يتعلق بالجرائم الإلكترونية، مما يجعل مهمة محاربة الجرائم التي تشمل أكثر من بلد صعبة للغاية.

5- وجود تنظيمات ترتكب الجرائم المعلوماتية لأهداف سياسية، أو اقتصادية، أو مساندة أفكار متطرفة، إلى جانب الجرائم التي يرتكبها الأفراد عبر الانترنت، والتي قد لا تختلف دوافعها وأهدافها، وإن اختلف حجم تأثيرها.[2]

وقد تبين من نتائج البحث أنه بشكل عام يوجد مجموعة من المعوقات التي تحد من مواجهة الجريمة الإلكترونية، كما يتضح من بيانات الجدول التالي:

جدول رقم(21) : يوضح معوقات مواجهة الجريمة الإلكترونية

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
عدم وجود أدلة قانونية	29	15.6	0.156	0.364	186	100
عدم وعي الأفراد بالجرائم الإلكترونية	72	38.7	0.387	0.488		
خوف الأفراد من الإبلاغ عن الجرائم الإلكترونية	15	8.1	0.081	0.273		
عدم وجود مهارات وتقنيات كافية لمواجهة الجرائم الإلكترونية	26	14	0.140	0.348		

[1] ليندة شرابية، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية: الاتجاهات الدولية في مكافحة الجريمة الإلكترونية، مرجع سابق، ص ص 250، 251.

[2] سامي يس خالد، الجهود الدولية لمكافحة الجرائم الإلكترونية، مجلة الدراسات العليا، المجلد 4، العدد 14، كلية الدراسات العليا، جامعة النيلين، السودان، 2016، ص ص 20، 21.

عدم وجود تشريعات قانونية قادرة على مواجهة الجرائم الإلكترونية	22	11.8	0.118	0.324		
سهولة ارتكابها	22	11.8	0.118	0.324		

يتضح من بيانات الجدول السابق أن: أغلب المبحوثين ممن تعرضوا لجرائم إلكترونية بنسبة 38.7%، وعددهم 72 مبحوثاً، يرون أن أهم معوقات مواجهة الجرائم الإلكترونية يتمثل في عدم وعي الأفراد بالجرائم الإلكترونية، وذلك بمتوسط حسابي يُقدر بحوالي 0.387، وانحراف معياري 0.488، و15.6% من المبحوثين يرون أن معوقات مواجهة الجريمة الإلكترونية عدم وجود أدلة قانونية، ويبلغ عددهم 29 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.156، وانحراف معياري 0.364، و14% يرون عدم وجود مهارات وتقنيات كافية لمواجهة الجرائم الإلكترونية وعددهم 26 مبحوثاً، وذلك بمتوسط حسابي 0.140، وانحراف معياري 0.348، و11.8% يرون عدم وجود تشريعات قانونية قادرة على مواجهة الجرائم الإلكترونية وعددهم 22 مبحوثاً، ونفس العدد من المبحوثين يرون سهولة ارتكابها، ويشير ذلك إلى وجود نوعٍ من الاتفاق على أن أهم معوقات مواجهة الجريمة الإلكترونية يتمثل في عدم وعي الأفراد بتلك الجرائم، إلى جانب عدم وجود أدلة قانونية ضد مرتكبيها.

والجدير بالذكر أن القانون المصري في البداية لم يعالج أو يتدخل بنصٍ صريح حول جرائم الإنترنت، بل اعتمد في ذلك على قانون العقوبات، ولكن بعد ذلك أُنشئ في وزارة الداخلية المصرية مكتب إداري لمكافحة جرائم الحاسب الآلي وشبكة المعلومات عام 2002، وقد اعتمد التشريع المصري على قانون العقوبات فيما يتعلق بجزئية السب والقذف، سواء كانت بالنشر عبر الوسائل المقروءة، أو الإلكترونية، كذلك اعتمد على قانون حقوق الملكية رقم (82) لسنة 2002 ، وبعد ذلك أُصدر القانون رقم (10) لسنة 2003 الخاص بتنظيم الاتصالات، ثم عقبه قانون رقم (10) لسنة 2004 الخاص بالتوقيع الإلكتروني.[1]

ومع تزايد معدلات الجريمة الإلكترونية، ومنها قرصنة البريد الإلكتروني، جعل المشرِّع المصري البريد الالكتروني من وسائل الاتصال المحمية دستورياً، وذلك بنص المادة رقم (57) من دستور مصر عام 2014 على أن "الحياة الخاصة حرمة، وهي مصونة لا تُمس، وللمراسلات البريدية والبرقية

[1] سعاد طعبة، الجريمة الإلكترونية: تفعيل لآليات القانون من أجل تحقيق العدالة، مجلة الحقوق والعلوم الإنسانية، المجلد 15، العدد 3، جامعة زيان عاشور بالحلفة، الجزائر، 2022، ص 236.

والإلكترونية والمحادثات الهاتفية وغيرها من وسائل الاتصال، حرمة، وسريتها مكفولة، ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها، إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون، كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها بشكل تعسفي، وينظم القانون ذلك" .[1]

ورغم أهمية المسئولية العامة للدولة، والجهات الخاصة بالحماية من الجرائم الإلكترونية، فهناك أيضا مسئولية شخصية على الأفراد، فمع تنامي حجم "مجتمعاتنا" بالتزامن مع استخدام الموارد الإلكترونية، تعرضت فعالية الجهات الحمائية التقليدية، أي مؤسسات إنفاذ القانون لضغوط شديدة، ففي الوقت الذي تتزايد حالات الجرائم الإلكترونية والأضرار الناجمة عنها، لم تتمكن وكالات إنفاذ القانون من مواكبة هذا التزايد، خاصة وأن جرائم الإنترنت لم تعد تقتصر على المجرمين المحترفين، أو الجماعات الإجرامية، بل يستغل الناس العاديون الفرص المتاحة عبر الانترنت بنفس الطريقة، ونظرا لأن سُبل عيش الفرد وأمنه الشخصي قد تعرضا لضغوط هائلة ولم تستطيع السلطات العامة مواجهة هذه الضغوط، أصبح الأمر متروكاً للأفراد، وتقع المسئولية الشخصية عليهم، لحماية ما يعتبرونه قيماً بالنسبة لهم شخصيا.[2]

وقد كشفت نتائج البحث أنه يمكن مواجهة الجريمة الإلكترونية من خلال عدة أساليب، كما يتبين من الجدول التالي:

جدول رقم (22) : يوضح مقترحات مواجهة الجريمة الإلكترونية

المتغيرات	التكرار	النسبة	المتوسط الحسابي	الانحراف المعياري	الإجمالي	
					التكرار	النسبة
توعية المستخدمين بمخاطر الجريمة الإلكترونية	69	37.1	0.371	0.484	186	100
تنظيم برامج تثقيفية في المدارس والجامعات حول الأمن الإلكتروني	39	21	0.209	0.408		

[1] أنسام سمير طاهر الحجامي، جريمة السرقة الإلكترونية، مجلة جامعة بابل – العلوم الإنسانية، المجلد 27، العدد 5، جامعة بابل، العراق، 2019، ص 137.

2 Kristjan Kikerpill, The Individual's Role in Cybercrime Prevention: Internal Spheres of Protection and our Ability to Safe Guard Them, Kubernetes, Op Cit, pp 1018, 1019.

تحديث البرامج الإلكترونية	9	4.8	0.048	0.215		
التعاون الدولي لمكافحة الجريمة الإلكترونية	13	7	0.070	0.256		
تطبيق القوانين بشكل صارم على مرتكبي الجريمة الإلكترونية	36	19.3	0.193	0.396		
تدريب كوادر فنية وأمنية على مواجهة الجريمة الإلكترونية	5	2.7	0.027	0.162		
سرعة الاستجابة لشكاوي المواطنين	15	8.1	0.081	0.273		

يتضح من بيانات الجدول السابق أن: الغالبية من المبحوثين ممن تعرضوا لجرائم إلكترونية بنسبة 37.1% يرون أنه يمكن مواجهة الجريمة الإلكترونية من خلال توعية المستخدمين للإنترنت بمخاطر تلك الجرائم، ويبلغ عددهم 69 مبحوثاً، وذلك بمتوسط حسابي يُقدر بحوالي 0.371، وانحراف معياري 0.484، و21% من المبحوثين ويُقدر عددهم 39 مبحوثاً، يرون أن مواجهة الجريمة تكون عن طريق تنظيم برامج تثقيفية في المدارس والجامعات حول الأمن الإلكتروني، وذلك بمتوسط حسابي يُقدر بحوالي 0.209، وانحراف معياري 0.408، في حين أن 19.3% من المبحوثين، ويبلغ عددهم 36 مبحوثاً، يرون أن المواجهة تكون من خلال تطبيق القوانين بشكلٍ صارم على مرتكبي تلك الجرائم، وذلك بمتوسط حسابي يُقدر بحوالي 0.193، وانحراف معياري 0.396، و8.1% يرون أن المواجهة تكون من خلال سرعة الاستجابة لشكاوى المواطنين ويبلغ عددهم 15 مبحوثاً، وذلك بمتوسط حسابي0.081، وانحراف معياري 0.273، و7% يرون التعاون الدولي ، ويبلغ عددهم 13 مبحوثاً، و4.8% يرون تحديث البرامج الإلكترونية، وعددهم 9 مبحوثين، و2.7% يرون تدريب كوادر فنية وأمنية على مواجهة الجريمة الإلكترونية، ويتبين من ذلك أنه يمكن مواجهة الجريمة الإلكترونية من خلال عدة آليات، أهمها توعية المستخدمين بمخاطر الجريمة الإلكترونية، وتنظيم برامج تثقيفية حول الأمن الإلكتروني، وتطبيق القوانين بشكلٍ صارم على مرتكبي تلك الجرائم.

ويتضح مما سبق أن مواجهة الجرائم الإلكترونية بشكلٍ عام، يتم من خلال طريقين:

- الأول (الطريق الوقائي): ويتمثل في غلق كل الأبواب والمنافذ، التي قد تؤدي إلى اقتراف الجرائم الإلكترونية، وهو ما نطلق عليه وسائل الوقاية من الوقوع ضحايا للجرائم الإلكترونية.
- الثاني (الطريق العلاجي): ويتضمن العقوبات لمرتكبي الجرائم الإلكترونية، وتبني الطرق والوسائل الأكثر فعالية في التعامل مع تلك الجرائم.[1]

النتائج العامة وتفسيرها

من خلال الأدب النظري والبحث الميداني، وما توصل إليه من استنتاجات، يمكن مناقشة النتائج العامة وتفسيرها من خلال إلقاء الضوء على:

أ – النتائج العامة في ضوء الهدف من البحث .

ب – الدلالات التطبيقية لنتائج البحث .

أ - النتائج العامة في ضوء الهدف من البحث :

حاول هذا البحث وصف الجريمة الإلكترونية في عصر تكنولوجيا الاتصالات والمعلومات، وانعكاسها على الأمن الاجتماعي للأفراد، وتم تحقيق هذا الهدف من خلال عده محاور، تمثلت في:

- **أسباب ودوافع الجريمة الإلكترونية :**

– تطورت الجريمة الإلكترونية وتعددت هجماتها، وأصبحت أكثر انتشاراً وأوسع نطاقاً، في ظل النمو السريع لتكنولوجيا الاتصالات والمعلومات، والتحولات التي أحدثتها العولمة، وتطور مهارات مجرمي الإنترنت، وتبنيهم للتقنيات الجديدة.

– يرجع تعرض الأفراد للجرائم الإلكترونية إلى عدم وعي الغالبية بكيفية استخدام الإنترنت، وتزايد الإفصاح عن المعلومات الشخصية، وتُعد فئة الشباب هي الفئة الأكثر عرضة للجرائم الإلكترونية، نظراً لأنها الفئة الأكثر استخداماً لتكنولوجيا الاتصالات والمعلومات، ويقضون وقتاً

[1] رفعت عمر عزوز وآخرون، الجريمة الإلكترونية ومتطلبات مواجهتها، مجلة كلية التربية، المجلد 10، العدد 31، كلية التربية، جامعة العريش، مصر، 2022، ص 244.

في التواصل عبر الإنترنت، وتؤكد ذلك نظرية "الأنشطة الروتينية لأسلوب الحياة" حيث أشارت إلى أن قضاء أوقات أطول في استخدام الإنترنت كنشاط يومي، يزيد من احتمالية التعرض لتهديدات الجرائم الإلكترونية.

- من أهم أسباب ودوافع الجرائم الإلكترونية الكسب المادي الذي يسعى إليه مرتكبو تلك الجرائم، إلى جانب الدوافع العاطفية، التي قد تتمثل في الانتقام من الضحايا، وفي بعض الأحيان يكون ارتكاب تلك الجرائم بدافع الترفيه.

- **نماذج الجرائم الإلكترونية الأكثر انتشاراً :**

- تشهد الجرائم الإلكترونية معدلات تنذر بالخطر، في ظل تزايد الوسائل المستخدمة في ارتكاب تلك الجرائم، مثل برامج التجسس والبرمجيات الخبيثة القائمة على الأكواد، والهندسة الاجتماعية، والاتصالات عبر الإنترنت، وأحصنة طروادة (التي تعمل على تغيير أو حذف البرامج والمعلومات داخل الحاسوب)، وبرامج الفدية، إلى جانب الألعاب الإلكترونية والشبكات الاجتماعية.
- تُعد الرسائل غير المرغوب فيها، وإغلاق حسابات ومواقع اجتماعية، وانتحال البريد الإلكتروني، وفيرسة التطبيقات والبرامج، وسرقة معلومات وبيانات شخصية، من أكثر نماذج الجرائم الإلكترونية انتشاراً.
- يتعرض الأفراد للجرائم الإلكترونية من قِبل أشخاص غير معروفين، لذلك لا يلجئون في الغالب للإبلاغ عن الجريمة التي تعرضوا لها، لاعتقادهم أن الإبلاغ لا يفيد، نظراً لصعوبة الوصول إلى مرتكبي تلك الجرائم.

- **الجريمة الإلكترونية وانعكاسها على الأمن الاجتماعي للأفراد :**

- الجرائم الإلكترونية لها انعكاسات وتأثيرات سلبية، وتشكل خطورة كبيرة على الأمن الاجتماعي للأفراد، خاصة في ظل ظهور العالم الإلكتروني، الذي أصبح معه أمن الأفراد وحياتهم الشخصية أكثر تهديداً وأكثر عرضة للوقوع ضحية للجرائم الإلكترونية.
- تؤثر الجرائم الإلكترونية على الأمن الاجتماعي للأفراد، من خلال خلق نوع من عدم الثقة لدى الأفراد في استخدام تكنولوجيا الاتصالات والمعلومات، والخوف من أي معاملات عبر الإنترنت، إلى جانب الإصابة بالاضطرابات النفسية، مثل (القلق، وعدم القدرة على التكيف الاجتماعي، وعدم إقامة علاقات اجتماعية).

- **إستراتيجيات مواجهة الجريمة الإلكترونية :**

- يُعد الأمن السيبراني أحد الركائز الرئيسة لمواجهة الجريمة الإلكترونية، والحد من مخاطرها، حيث تساعد إستراتيجيات الأمن السيبراني على حماية الأنظمة الرقمية والبيانات من الجرائم الإلكترونية، من خلال تعزيز الوعي بين المستخدمين بمخاطر الجريمة الإلكترونية، وكيفية الوقاية منها، واستخدام تقنيات مثل التشفير، وبرامج مكافحة الفيروسات، وتطبيق الجدران النارية، وتحديث الأنظمة والبرامج بانتظام، لسد الثغرات الأمنية، والتصدي للتهديدات الجديدة، وتعزيز التعاون الدولي لمكافحة تلك الجرائم.
- عدم وعي الأفراد بالجريمة الإلكترونية، وعدم وجود أدلة قانونية حول الجاني، وعدم وجود مهارات وتقنيات كافية لمواجهة تلك الجرائم، التي يسعى مرتكبوها إلى استخدام المزيد من التقنيات، تُعد أكثر معوقات مواجهة الجريمة الإلكترونية.
- يمكن أن يحمي الأفراد أنفسهم من الجريمة الإلكترونية، من خلال تجنب فتح الرسائل غير المعروفة، وعدم نشر معلومات شخصية، وتشفير البيانات والمعلومات، إلى جانب استخدام برامج وقاية من الفيروسات، حيث تشير نظرية "دوافع الحماية" إلى أن دوافع الأفراد لحماية أنفسهم من تهديدات الجرائم الإلكترونية، ينبع من تقييمهم لخطورة تلك الجرائم، وحجم الضرر الناتج عنها.

ب - الدلالات التطبيقية لنتائج البحث

من خلال النتائج التي تم التوصل إليها يقترح البحث مجموعة من التوصيات التي يمكن أن يكون لها أهمية، وتساعد من الناحية العملية في وضع خطط وإستراتيجيات أكثر فعالية في مواجهة الجريمة الإلكترونية ، ومحاولة مواجهة المخاطر والتأثيرات السلبية لتلك الجريمة على الأمن الاجتماعي للأفراد، وتلك التوصيات تتوجب على كلٍ من:

- **<u>الحكومات</u>**

1- زيادة الاستثمار والدعم الموجه لتحقيق الأمن الإلكتروني.
2- وضع أساليب للرقابة الإلكترونية أكثر فعالية.
3- الاهتمام بالكفاءات التقنية، للتمكن من الكشف عن الجرائم الإلكترونية.
4- دعم البحث العلمي في مجال الجريمة الإلكترونية، وتطوير حلول لمواجهتها.

- **مالكي ومسئولي المواقع الإلكترونية**

1- مراقبة عمل المواقع والبحث عن أي خلل فيها.

2- وضع شروط وسياسات استخدام المواقع الإلكترونية لمنع الجرائم الإلكترونية.

3- استخدام برامج للأمن السيبراني.

- **الهيئات الدولية**

1- عمل مبادرة منسقة لجميع الدول، تشمل تطبيقاً موحداً لتدابير الأمن الرئيسة، والاستثمار في التقنيات الدفاعية ضد الجرائم الإلكترونية.

2- زيادة التعاون في إنفاذ القانون الدولي الخاص بالجرائم الإلكترونية.

3- توحيد وتنسيق متطلبات إستراتيجيات الأمن السيبراني.

4- فرض عقوبات مالية على الدول التي لا تتخذ إجراءات جادة وفعالة ضد الجرائم الإلكترونية.

- **الأفراد**

1- تعزيز المواقف الإيجابية تجاه السلوكيات الوقائية من الجرائم الإلكترونية، مثل(عدم مشاركة المعلومات الشخصية).

2- استخدام برامج مكافحة الفيروسات.

3- تجنب إرسال معلومات إلى أشخاص غير معروفين عبر الإنترنت.

4- التحديث المستمر لبرامج الحماية الخاصة بالأجهزة الإلكترونية.

5- استخدام برامج ونظم تشغيل آمنة.

- **وسائل الإعلام**

1- توعية وتثقيف مستخدمي الإنترنت بالسلامة المعلوماتية، وكيفية تجنب مخاطر الإنترنت.

2- تثقيف الأفراد حول كيفية التعرف على الجرائم الإلكترونية، والتعامل معها بشكل آمن.

3- نشر معلومات حول الجرائم الإلكترونية الجديدة، والأكثر انتشاراً، والطرق التي يستخدمها المجرمون.

4- نشر معلومات حول أفضل الممارسات الأمنية.

قائمة المصادر والمراجع

أولاً : المراجع العربية

- الجنيبي، خالد علي. (2015). الجريمة الإلكترونية بين تحديات الواقع واستشراق المستقبل، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية- ICACC، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، السعودية .
- الجوبر، إبراهيم بن مبارك بن موسى. (2024). تحقيق الأمن الاجتماعي، المجلة العربية للآداب والدراسات الإنسانية، المجلد 8، العدد 33، المؤسسة العربية للتربية والعلوم والآداب، مصر .
- الحجامي، أنسام سمير طاهر. (2019). جريمة السرقة الإلكترونية، مجلة جامعة بابل – العلوم الإنسانية، المجلد 27، العدد 5، جامعة بابل، العراق .
- الحيمودي، بدر. (2023). الأمن السيبراني وحماية الأنظمة المعلوماتية، مجلة المنارة للدراسات القانونية، العدد 46، المغرب .
- الزبيدي، دلال لطيف مطشر . (2018). جريمة الاعتداء على المواقع الإلكترونية، مجلة جامعة بابل- العلوم الإنسانية، المجلد 26، العدد 9، جامعة بابل، العراق .
- السويدي، شريف محمد، ونوفل، زيزت مصطفى عبده. (2023). دور الأسرة في تدعيم الأمن السيبراني لمواجهة الابتزاز الإلكتروني: دراسة كيفية، مجلة كلية الآداب، العدد 147، جامعة بغداد، العراق .
- العباس، بو مامي. (2015). الجريمة الإلكترونية نتاج أجهزة ومواقع تواصل اجتماعي، مجلة جيل العلوم الإنسانية والاجتماعية، العدد 12، مركز جيل البحث العلمي، الجزائر .
- الأميري، أمينة إبراهيم، والعموش، أحمد فلاح. (2022). أثر استخدام التكنولوجيا كنشاط روتيني في زيادة معدلات الجريمة، مجلة كلية الآداب، العدد 143، جامعة بغداد، العراق .
- المخايطة، مهنا بن يوسف بن مهناء. (2021|). العوامل الاجتماعية لوقوع الشباب ضحايا للجرائم الإلكترونية: دراسة ميدانية بمدينة الهفوف، مجلة الخدمة الاجتماعية، المجلد 1، العدد 70، الجمعية المصرية للأخصائيين الاجتماعيين، مصر .

- الملا، إبراهيم حسن عبد الرحيم . (2018). الذكاء الاصطناعي والجريمة الإلكترونية، مجلة الأمن والقانون، المجلد 26، العدد 1، دبي، الإمارات .
- بن عبد الله، نوال قادة ، وبن حمو محمد. (2022). الجريمة الإلكترونية: قراءة سوسيولوجية لأهم النظريات المفسرة للسلوم الإجرامي، مجلة روافد للدراسات والأبحاث العلمية في العلوم الاجتماعية والإنسانية، المجلد 6، العدد 3، المركز الجامعي بلحاج بوشعيب، الجزائر .
- بن عمروش، فريدة ، وجاب الله، حكيمة . (2023) . الجريمة الإلكترونية: المفهوم، الأشكال والآليات، المجلة العلمية للتكنولوجيا وعلوم الإعاقة، المجلد 5 ، العدد 4، المؤسسة العلمية للعلوم التربوية والتكنولوجية والتربية الخاصة، الجزائر.
- بو خميس، أحلام، وبوالزيت ندى. (2024). الآليات القانونية لحماية سرية المراسلات الإلكترونية في سبيل تعزيز الحق في الخصوصية الرقمية، مجلة الحقوق والحريات، المجلد 12، العدد 1، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر .
- خالد، سامي يس. (2016). الجهود الدولية لمكافحة الجرائم الإلكترونية، مجلة الدراسات العليا، المجلد 4، العدد 14، كلية الدراسات العليا، جامعة النيلين، السودان .
- سيد، ريهام رمضان. (2015). إستراتيجية مقترحة لتجنب الجريمة المعلوماتية على المستوى العربي: بشكل عام وفي مصر بشكل خاص، المجلة العلمية ملحق، كلية الآداب، جامعة أسيوط .
- شرابية، ليندة. (2009). السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية: الاتجاهات الدولية في مكافحة الجريمة الإلكترونية، مجلة دراسات وأبحاث، العدد 1، جامعة الجلفة، الجزائر .
- شعبان، سمير. (2009). الجريمة الإلكترونية: مقارنة تحليلية لتحديد مفهوم الجريمة والمجرم، مجلة دراسات وأبحاث، العدد 1، الجزائر .
- طالة، لامية، وسلام، كهيذة. (2020) . الجريمة الإلكترونية: بُعد جديد لمفهوم الإجرام عبر منصات التواصل الاجتماعي، مجلة الرواق للدراسات الاجتماعية والإنسانية، المجلد 6، العدد 2، المركز الجامعي أحمد زبانة غليزان، مخبر الدراسات الاجتماعية والنفسية والأنثروبولوجية، الجزائر .
- طعبة، سعاد. (2022). الجريمة الإلكترونية: تفعيل لآليات القانون من أجل تحقيق العدالة، مجلة الحقوق والعلوم الإنسانية، المجلد 15، العدد 3، جامعة زيان عاشور بالحلفة، الجزائر .

- عبد الله، أحمد حسن، وجواد، صفاء كريم. (2022). الأمن الاجتماعي ومقوماته: دراسة نظرية تحليلية، مجلة جامعة بابل- العلوم الإنسانية، المجلد 30، العدد 3، جامعة بابل، العراق .
- عزوز، رفعت عمر، وآخرون. (2022). الجريمة الإلكترونية ومتطلبات مواجهتها، مجلة كلية التربية، المجلد 10، العدد 31، كلية التربية، جامعة العريش، مصر .
- عيسات، العمري، وبوعزة، عبد الرؤوف. (2022). الجريمة الإلكترونية لدى المراهقين: دوافع الإقبال وآليات الضبط الاجتماعي، مجلة علوم الإنسان والمجتمع، المجلد 11، العدد 1، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خيضر بسكرة، الجزائر .
- كروش، نوال . (2021). بحث في إشكالات الجريمة الإلكترونية، المجلة الجزائرية للدراسات الإنسانية، المجلد 2، العدد 2، جامعة وهران أحمد بن بلة، الجزائر .
- كريم، فريحة محمد. (2011). الجريمة الإلكترونية، شئون اجتماعية، المجلد 28، العدد 110، جمعية الاجتماعيين في الشارقة، الجزائر .
- مثنى، محمود صالح محمد. (2024). الجريمة الإلكترونية ومراحل تطورها، التواصل، العدد 52، جامعة عدن- نيابة الدراسات العليا والبحث العلمي، عدن، اليمن .
- منصور، إبراهيم صالح . (2024) . مفهوم الجريمة الإلكترونية وأثرها السلبي على مستخدمي مواقع الت
- نجم الدين، فيصل كامل. (2018). واقع الجريمة الإلكترونية في مواقع التواصل الاجتماعي: الحماية النظامية في دول مجلس التعاون الخليجي، المجلة الدولية للاتصال الاجتماعي، المجلد 5، العدد 4، كلية العلوم الإنسانية والاجتماعية، جامعة عبد الحميد بن باديس مستغانم، الجزائر .
- هراكي، حياة. (2023). واقع جريمة الاحتيال الإلكتروني في التجارة الإلكترونية، مجلة التغير الاجتماعي، المجلد 8، العدد 2، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خيضر ، بسكرة، الجزائر .
- واصل الاجتماعي الإنترنت، مجلة ريحان للنشر العلمي، العدد 49، مركز فكر للدراسات والتطوير، سوريا .

ثانياً : المراجع الأجنبية

- Akdemir, Naci, and Lawless, Christopher James. (2020). Exploring The human factor in Cyber-enabled and Cyber-dependent Crime Victimization: a Lifestyle Routine Activities Approach, Internet Research, Vol 30, No 6, .United Kingdom

- Akinbowale, Oluwatoyin Esther, and Others.(2020). Analysis of Cyber-Crime Effects on The banking Sector Using The Balanced Score Card: a Survey of Literature, Journal of Financial Crime, Vol 27, No 3, United Kingdom .

- Campbell,Curtis C. (2019). Solutions for Counteracting Human Deception in Social Engineering Attacks, Information Technology and People, United Kingdom. Vol 32, No 5, United Kingdom .

- Chen, Hao, and Yuan, Yufei. (2023). The Impact of Ignorance and Bias on Information Security Protection Motivation: a Case of E-Waste Handling, Internet Research, vol 33, No 6, United Kingdom .

- Costa, Ines Gil. (2023). Ameacas Ciberneticas Os Seeus Impactos an Seguranca Humana, Grau de Mastre em Relacoes Internacionis, Universidade Autonoma de Lisboa, Portuguesa.

- Decker, Eileen M, and Others. (2021). Bots, Bytes, and Briefs: Cyber Investigations and Prosecutions Community, Environment and Disaster Risk Management, Vol. 24, United Kingdom .

Drew, Jacqueline M. (2020). A Study of Cybercrime Victimization and - Prevention: Exploring The use of Online Crime Prevention Behaviors and Strategies, Journal of Criminological Research, Policy and Practice, Vol 6, No 1, United Kingdom .

- Farooq, Nourin, and Others. (2024). Explanatory and Predictive Analysis of Smartphone Security Using Protection Motivation Theory: a Hybrid

SEM-Al Approach, Information Technology and People, ITP, United Kingdom .

- Gibbs, Tanya. (2020). Seeking Economic Cyber Security: a Middle Eastern Example, Journal of Money Laundering Control, Vol 23 No 2, United Kingdom .

- Good, Megan C, and Hyman, Michael R. (2020). Protection Motivation Theory and Brich-and-Mortar Sales People, International Journal of Retail and Distribution Management, Vol 48, No 8, United Kingdom .

- Igbinovia, Magnus Osahon, and Ishola, Bolan Le Clifford. (2023). Cyber Security in University Libraries and Implication for Library and Information. Science Education in Nigeria, Digital Library Perspectives, Vol 39, No 3, United Kingdom .

- Jamil, Hassan, and Others. (2025). Human-Centric Cyber Security: Applying Protection Motivation Theory to Analyze Micro Business Owners' Security Behaviors, Information and Computer Security, Vol 33, No 1, United Kingdom .

- Joshi, Kiran, and Kaushik, Priyanka. (2024). An Analysis of Perception and Awareness of Undergraduate Youth Towards Cybercrime, Advanced Series in Management, Vol 34A, Emerald Publishing Limited, United Kingdom .

- Kaswan, Kuldeep Singh, and Others.(2022). Cybersecurity Law-Based Insurance Market, Emerald Group Publishing Limited, United Kingdom .

- Kikerpill, Kristjan. (2021). The Individual's Role in Cybercrime Prevention: Internal Spheres of Protection and our Ability to Safe Guard Them, .Kubernetes, Vol 50, No 4, Emerald Publishing Limited, United Kingdom

- Lee, Yi Yong, and Others. (2022). Phishing Victimization Among Malaysian Young Adults: Cyber Routine Activities Theory and Attitude in

Information Sharing Online, The Journal of Adult Protection, Vol 24, No 3/4, United Kingdom .

- Lestari, Sri, and Others. (2024). Navigating Perilous seas: Unmasking Online Banking Frauds, Perceived Usefulness Fear of Cybercrime and Distrust in Online Banking, Safer Communities, Vol 23, No 4, Emerald Publishing Limited, United Kingdom .

- Li, Yang, and Others. (2021). Cybercrime's Tendencies of The Teenagers in The COVID-19 Era: Assesssing. The Influence of Mobile Games, Social Networks and Religious Attitudes, Journal of Kubernetes Emerald Publishing Limited, United Kingdom .

- Mugarura, Norman, and Ssali, Emma. (2021). Intricacies of Anti-Money Laundering and Cyber-Crimes Regulation in a Fluid Global System, Journal of Money Laundering, Vol 24, No 1,United Kingdom .

Ofori, Abel Yeboah, and Boateng, Francisca Afua Opoku. (2023). - Mitigating Cybercrimes in an Evolving Organizational Landscape, Continuity and Resilience Review, Vol 5, No 1, Emerald Publishing Limited, United Kingdom .

- Shah, Mahmood Hussain, and Others. (2019). Cybercrimes Prevention: Promising Organizational Practices, Information Technology and People, Vol 32, No 5, United Kingdom .

- Skalkos, Andreas, and Others. (2024). Exploring Users Attitude Towards Privacy-Preserving Search Engines: aprotection Motivation Theory Approach. Information and Computer Security, Vol 32, No 3, United Kingdom .

- Sule, Babayo, and Others. (2023). Countering Cybercrimes as The Strategy of Enhancing Sustainable Digital Economy in Nigeria, Journal of Financial Crime, vol 30, No 6, United Kingdom .

- Tran, Dien Van, and Others. (2024). Unraveling Influential Factors Shaping Employee Cybersecurity Behaviors: an Empirical Investigation of Public Servants in Vietnam, Journal of Asia Business Studies, Vol 18, No 6, United Kingdom .

- Tran, Dien Van, and Others.(2024). Exploring The Influence of Government Social Media on Cybersecurity Compliance: Employee Attitudes, Motivation and Behaviors, Journal of Asia Business Studies, Vol 18, No 1, United Kingdom .

- Vlachos, Vasileios, and Others. (2011). The Landscape of Cybercrime in Greece, Information Management and Computer Security, Vol 19, No 2, Emerald Group Publishing Limited, United Kingdom .

- Yeoh, Peter. (2019). Artificial Intelligence: Accelerator or Panacea for Financial Crime?, Journal of Financial Crime, Vol 26, No 2, United Kingdom .

- Younies, Hassan, and Al-Tawil, Tareq Na'el. (2020). Effect of Cybercrime Laws on Protecting Citizens and Businesses in The United Arab Emirates, Journal of Financial Crime, Vol. 27, No. 4, United Kingdom .

Abstract:

The aim of the research is to describe the nature of cybercrime in the era of information and communications technology and its impact on the social security of individuals. Cybercrime has become more widespread and broader in scope, and its causes and motives have multiplied. It is also witnessing alarming rates, in light of the multiplicity of means used by perpetrators of these crimes. Social reality indicates that the youth category is the most vulnerable to these crimes, as it is the category that uses information and communications technology the most, which provides a greater opportunity for them to fall victim to cybercrimes, such as phishing, blackmail, electronic defamation, email violations, copyright, and other crimes, which have negative repercussions and effects on the social security of individuals, and create a kind of lack of trust in the use of technology and dealing online, which requires effective strategies to confront it. Cybersecurity is one of the most important of these strategies, through the motives of individuals to protect their data and electronic systems, in addition to maintaining the security of the communications and information environment, and securing technical devices including it contains systems, programs, data and information that are traded over the Internet.

Keywords: Cybercrime, Social security, Models, Confrontation strategies.