



## The Social Dimensions of Cybercrime and Strategies for Combating It

Sawsan Ali Salem Hanish \*

Department of Social Work, Faculty of Arts and Languages, University of Tripoli, Libya

الأبعاد الاجتماعية للجريمة الإلكترونية واستراتيجيات مواجهتها

سوسن علي سالم حنيش \*

قسم الخدمة الاجتماعية، كلية الآداب واللغات، جامعة طرابلس، ليبيا.

\*Corresponding author: [sa.hanish@uot.edu.ly](mailto:sa.hanish@uot.edu.ly)

Received: October 17, 2025

Accepted: November 29, 2025

Published: December 04, 2025

### Abstract:

This study explores the social dimensions of cybercrime and strategies for its confrontation, noting its increasing prevalence in the Libyan society due to rapid technological advancement. Cybercrime differs from traditional crimes as it requires a minimum level of technical culture, involves the intent to harm others, and is often difficult to detect due to the lack of physical evidence, relying only on digital information traces. The research, utilizing a descriptive analytical method, aims to identify the social dimensions and causes of cybercrime, and their impacts on the victim and perpetrator, while proposing mechanisms for reduction. The findings indicate that cybercrime is often linked to factors such as unemployment and difficult economic and social pressures, which drive some individuals, particularly those with low self-control, to engage in criminal activities as a low-risk, high-return path to achieving desired goals, as explained by the Anomie theory. The study concludes with a set of strategies for prevention and confrontation, including enacting deterrent legislation, strengthening electronic police units, raising community awareness, and adopting strong individual protective measures.

**Keywords:** Cybercrime, Social Dimensions, Social Control, Anomie Theory, Counter Strategies.

### المخلص

تستكشف هذه الدراسة الأبعاد الاجتماعية للجريمة الإلكترونية واستراتيجيات مواجهتها، مشيرة إلى تنامي انتشارها في المجتمع الليبي نتيجة التطور التقني المتسارع. وتختلف الجريمة الإلكترونية عن الجرائم التقليدية كونها تتطلب حداً أدنى من الثقافة التقنية، وتتضمن الإرادة في إلحاق الضرر بالآخرين، وغالباً ما يصعب اكتشافها لغياب الآثار المادية، واقتصارها على الآثار المعلوماتية الرقمية. وتهدف الدراسة، باستخدام المنهج الوصفي التحليلي، إلى تحديد الأبعاد والمسببات الاجتماعية للجريمة الإلكترونية وتأثيراتها

على الضحية والمركب، واقتراح آليات للحد منها. وتبين النتائج أن الجريمة الإلكترونية ترتبط بعوامل مثل البطالة والضغط الاقتصادي والاجتماعية الصعبة، التي تدفع بعض الأفراد، خاصة ممن يتسمون بضبط ذاتي منخفض، للانخراط في الأنشطة الإجرامية كمسار قليل المخاطر وسريع المردود لتحقيق أهداف مرغوبة، كما تفسره نظرية اللامعيارية. وتختتم الدراسة بمجموعة من الاستراتيجيات للوقاية والمواجهة، تشمل سن تشريعات رادعة، وتفعيل وحدات الشرطة الإلكترونية، وزيادة الوعي المجتمعي، واعتماد تدابير وقائية فردية قوية.

**الكلمات المفتاحية:** الجريمة الإلكترونية، الأبعاد الاجتماعية، الضبط الاجتماعي، نظرية الأنومي، استراتيجيات المواجهة.

#### المقدمة:

شهد المجتمع الليبي في العقد الأخير تنامي وظهور جرائم مستحدثة، نتيجة للتطور والتغير المتسارعين ودخول الوسائل التقنية في مختلف جوانب الحياة. وقد ترتب على ذلك ارتكاب الجرائم إلكترونياً من قبل الشباب من الجنسين. ومن المؤكد أن الإقبال على ارتكاب هذا النوع من الجرائم يعد أمراً خطيراً وينطوي على قدر بالغ من الخطورة والتهديد للأسرة والمجتمع، لاسيما أن هذه الظاهرة تبرز كما لو كانت متعلقة بردود أفعال أو تصفية حسابات أو انتهاك حرمان الآخرين (الرومي، 2003، ص. 121). وتعتبر الجريمة الإلكترونية إحدى الجرائم المستحدثة التي دخلت على مجتمعاتنا العربية وأصبحت تؤرق حياة الفرد وأمن المجتمع؛ إذ أثر التطور التقني الواسع النطاق بشكل كبير في أمن واستقرار المجتمعات من ناحية، كما أدت تبعات الموجة التطورية التقنية العارمة إلى التدخل في أدق خصوصيات الفرد من ناحية أخرى (عبدالمطلب، 2001، ص. 87). وقد سعت بعض الدول إلى سن تشريعات قانونية لمواجهة هذه الجرائم. وفي المجتمع الليبي، زاد وتنامي انتشار التطور التقني في كافة المستويات والمجالات، مما بدأ يُشكل خطراً على أمن المجتمع سياسياً واقتصادياً وثقافياً، وعلى استقرار بناء الحياة الاجتماعية وتركيباتها. وتختلف طبيعة الجريمة الإلكترونية عن الجرائم التقليدية وفقاً للوسط الذي تُرتكب فيه والوسيلة التي استُخدمت في ارتكابها. وهذا يتطلب توفر الحد الأدنى من الثقافة التقنية لدى مرتكب الجريمة، والإرادة في إلحاق الضرر بالآخرين، ووجود نص قانوني يُجرّم هذا السلوك الإجرامي. فالجريمة الإلكترونية تُرتكب باستخدام الحاسب الآلي كأداة وتُستخدم شبكة الإنترنت كوسيلة. وفي الغالب، لا يتم التبليغ عن هذه الجرائم، خاصة إذا تعلق الأمر بالمؤسسات والشركات التجارية اللامعة، تجنباً للإساءة للسمعة وزعزعة ثقة الزبائن والعملاء. وهي جرائم صعبة الاكتشاف لعدم تركها آثار مادية يمكن تتبع الأدلة التابعة لها، وتقتصر فقط على الآثار المعلوماتية الرقمية؛ وذلك بسبب غياب الدليل المرئي ولأن أغلب البيانات عبارة عن رموز لا يمكن قراءتها وفهمها إلا من قبل شخص ذي معرفة تقنية وخبرة فائقة في مجال الحاسب الآلي. وقد حاولت الباحثة في هذه الدراسة التركيز على الجوانب الاجتماعية لهذه الجرائم.

#### مشكلة الدراسة:

تنتشر الجريمة الإلكترونية على نطاق عالمي واسع، وتتخطى الحدود الإقليمية وتلحق أضراراً جسيمة. هذه الجرائم لا تمتاز بالعنف ولا يستخدم مرتكبوها القوة الجسدية أو العضلية للقيام بها. وقد لاحظت الباحثة من خلال عملها كأستاذ جامعي وتعاملها مع طلابها تزايد وتفاقم هذه المشكلة، سواء من خلال الواقع المعاش أو من خلال ما يتناقله الطلاب من خبراتهم اليومية. وبهذا أدركت الباحثة اختلاف أثر التحولات التقنية في انتشار الجرائم المعلوماتية في المجتمع الليبي من حيث الحجم والخصائص والتطور والثقافات الفرعية للأسرة الليبية التي تسهم بشكل كبير في انتشار هذه الجرائم، مما يعكس الأبعاد الاجتماعية لها. ومن خلال الاطلاع على بعض الدراسات السابقة، أظهرت نتائجها تطور حجم الجرائم المعلوماتية على المستوي المحلي والعربي والعالمي منذ عام (2001 حتى 2005)، فظهرت حالات للنشهر بسمعة الأفراد والمؤسسات، والدخول غير المشروع على البريد الإلكتروني، واختراق المواقع الخاصة على شبكة الإنترنت. وقد توصلت دراسات كل من (النفيعي، 2002)، (المنشاي، 2003)، (عبد، 2006)، (محمد، 2021)، (موسى وأبو عكير، 2023) إلى أن الجريمة الإلكترونية تتمثل في كل سلوك غير قانوني مرتبط

بأي شكل بالأجهزة الإلكترونية، ويتسبب في حصول المجرم على فوائد مع تحميل الضحية خسارة. ويكون هدف هذه الجرائم دائماً هو سرقة وقرصنة المعلومات الموجودة في الأجهزة، أو ابتزاز الأشخاص بمعلوماتهم المخزنة على أجهزتهم. وعلى الرغم من أن شبكة المعلومات لها وجه يعود بالخير على الإنسان ومنافعها لا تحصى، إلا أنه إلى جانب هذا الخير، لها آثار مدمرة عندما يساء استخدامها، حيث يتم من خلالها ارتكاب جرائم متعددة كسرقة المستندات وتزويرها، وتدمير مواقع المعلومات، ونشر الإشاعات وتشويه سمعة الأشخاص والشركات، والاستيلاء على الإنتاج الفكري والعلمي للآخرين، بل ونشر الفساد والفجور. ومن هذا المنطلق انبثقت الدراسة الحالية لتجيب على تساؤل عام يتمثل في: ما هي الأبعاد الاجتماعية للجريمة الإلكترونية واستراتيجيات مواجهتها؟

### أهمية الدراسة:

- تساعد دراسة الجريمة الإلكترونية في تحديد أنواعها والمخاطر المرتبطة بها كاختراق الحسابات والابتزاز ونشر المحتوى غير الأخلاقي.
- يساعد فهم الجريمة الإلكترونية في تطوير آليات وقائية وعلاجية للحد من أثارها على الفرد والمجتمع.
- يمكن من خلال هذه الدراسة تحديد الأبعاد الاجتماعية للجريمة الإلكترونية وبالتالي تلافي الهوة الثقافية والاجتماعية التي من شأنها أن تزيد من حدة آثار هذه الجرائم.

### أهداف الدراسة:

- تحديد الأبعاد الاجتماعية للجريمة الإلكترونية وتأثيراتها على البناء الاجتماعي للمجتمع.
- الكشف عن المسببات الاجتماعية للجريمة الإلكترونية وآثارها على كل من الضحية ومرتكب الجريمة.
- اقتراح بعض الاستراتيجيات والآليات للحد من الجريمة الإلكترونية.

### تساؤلات الدراسة:

- ما هي أهم الأبعاد الاجتماعية للجريمة الإلكترونية وتأثيراتها على البناء الاجتماعي للمجتمع؟
- ما هي المسببات الاجتماعية للجريمة الإلكترونية وآثارها على كل من الضحية ومرتكب الجريمة؟
- ما هي أهم الاستراتيجيات والآليات للحد من الجريمة الإلكترونية؟

**حدود الدراسة:** تحددت الدراسة بالحد الموضوعي الذي يتناول الأبعاد الاجتماعية للجريمة الإلكترونية واستراتيجيات مواجهتها.

### مصطلحات الدراسة:

- **الأبعاد الاجتماعية للجريمة الإلكترونية:** وهي الآثار والتغيرات السلبية التي تحدثها الجريمة الإلكترونية على البنية والقيم والتفاعلات الاجتماعية للأفراد والأسر والمجتمع.
- **الجريمة الإلكترونية (تعريف إجرائي مستند إلى المراجع):** أي نشاط يتم تنفيذه عبر الكمبيوتر والأجهزة الرقمية والشبكات المستخدمة في عالم الإنترنت، ويتم تسهيله من خلال وسيط الإنترنت. يمكن أن يشمل السرقة البعيدة للمعلومات التي تنتمي إلى قطاع فردي أو حكومي أو شركة من خلال المرور الجنائي إلى جهاز تحكم عن بعد غير مصرح به أنظمة حول العالم. ويشمل ذلك سرقة ملايين الروبيات من البنوك عبر الإنترنت وصولاً إلى المضايقة والمطاردة لمستخدمي الإنترنت (محمد، 2020، ص. 440).

**منهج الدراسة:** استخدمت الباحثة المنهج الوصفي التحليلي لملاءمته لطبيعة الدراسة الحالية، حيث يقوم على وصف الظاهرة وتحليلها تحليلًا دقيقًا من خلال جمع المعلومات والعمل على تصنيفها والتعبير عنها وصفيًا (كيفيًا)، وذلك للوصول إلى استنتاجات حول موضوع الدراسة.

## الإطار النظري:

### مفهوم الجريمة الإلكترونية:

تبرز الجريمة الإلكترونية في الأفعال الضارة التي يقوم بها الفرد أو الجماعة من خلال أجهزة الحواسيب أو الهواتف المحمولة لإلحاق الضرر بالآخرين. يُعرفها (توبة، 2008) بأنها تصرف غير مشروع يؤثر في الأجهزة والمعلومات الموجودة عليها. يُعتبر هذا التعريف جامعاً مانعاً من الناحية الفنية للجريمة الإلكترونية؛ حيث إن ارتكاب الجريمة يتطلب وجود أجهزة كمبيوتر بالإضافة إلى ربطها بشبكة معلوماتية ضخمة (توبة، 2008، ص. 189). كما أوردت (محمد، 2021) تعريف الدكتور عبد الفتاح مراد لجرائم الإنترنت على أنها: "جميع الأفعال المخالفة للقانون والشرعية والتي تُرتكب بواسطة الحاسب الآلي من خلال شبكة الإنترنت، وهي تتطلب إلماماً خاصاً بتقنيات الحاسب الآلي ونظم المعلومات، سواء لارتكابها أو للتحقيق فيها. ويُقصد بها أيضاً أي نشاط غير مشروع ناشئ في مكون أو أكثر من مكونات الإنترنت مثل مواقع الإنترنت وغرف المحادثة أو البريد الإلكتروني، كما تُسمى كذلك في هذا الإطار بالجرائم السيبرانية أو السيبرية لتعلقها بالعالم الافتراضي" (محمد، 2021، ص. 439). ويشير (الديربي، 2013) إلى الجريمة الإلكترونية بأنها نشاط يتم تنفيذه عبر الكمبيوتر والأجهزة الرقمية والشبكات المستخدمة في عالم الإنترنت، ويتم تسهيله من خلال وسيط الإنترنت. قد تكون في شكل السرقة البعيدة للمعلومات التي تنتمي إلى قطاع فردي أو حكومي أو شركة من خلال المرور الجنائي إلى جهاز تحكم عن بعد غير مصرح به أنظمة حول العالم، وكذلك سرقة الملايين من المصارف عبر الإنترنت، كما قد تصل أيضاً إلى مضايقة ومطاردة مستخدمي الإنترنت (الديربي، 2013، ص. 87). وتعرفها الباحثة إجرائياً في هذه الدراسة بأنها جرائم تُرتكب ممن يتقنون استخدام الحواسيب والأجهزة المعلوماتية، فيسيئون استخدامها ويوظفونها لأنشطة إجرامية تُرتكب ضد الأفراد والمجتمع ككل.

### أهداف الجرائم الإلكترونية:

بينت (سلامة، 2023) أهداف الجريمة الإلكترونية وتلخصت في التالي:

1. يمكن لمرتكبيها الوصول إلى المعلومات بطرق غير قانونية والاطلاع عليها أو حذفها أو تعديلها أو سرقتها بما يحقق أهدافهم المرجوة.
2. يمكن من خلال مستخدمي الإنترنت من ذوي المهارة والتقنية العالية الوصول والاختراق للأجهزة الموفرة للمعلومات وتعطيلها أو الحصول على معلومات سرية للأفراد أو المؤسسات والمصارف وابتزازهم بواسطتها مما يحقق الكسب المادي أو المعنوي أو السياسي غير المشروع.
3. يمكن لمرتكب الجريمة الإلكترونية الانتقام من أشخاص أو مؤسسات ألحقت به الضرر مسبقاً، فتنولد لديه الشعور بالحرمان من بعض الحقوق المهنية أو العاطفية أو الاجتماعية، فيلجأ إلى التلاعب بالبرامج المعلوماتية إما بالتشهير والفضح أو الحذف والإلغاء والتخريب والتحريف أو بالابتزاز والاستغلال وإساءة استخدامها أو بالسرقة والاستيلاء عليها.
4. تزوير معلومات وقواعد بيانات النظام التعليمي وتغيير المعلومات وتحريفها كتغيير نتائج الطلاب أو إصدار شهادات علمية مزورة أو التشهير ببعض المؤسسات التعليمية لإلحاق الخسائر المادية بها أو سرقة الإنتاج العلمي والبحوث والكتب أو الإبداعات والاختراعات للباحثين في الجامعات.
5. التصنت والتجسس والدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف واعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.
6. الإرهاب الإلكتروني والقنابل البريدية والمتمثلة في إرسال فيروسات لتدمير البيانات من خلال رسالة إلكترونية، أو قرصنة البرمجيات وبيعها مرة أخرى، وقرصنة البيانات والمعلومات واعتراضها وخطفها بقصد الاستفادة منها، وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.

7. إفشاء الأسرار والحصول على معلومات خاصة جداً ونشرها على الأفراد، وكذلك سرقة الأرقام والمتاجرة بها وخاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقات الانتماء.

8. التحرش الجنسي ويقصد به مضايقة الأفراد من الجنسين من خلال المراسلة أو المهاتفة، أو المحادثة والمطاردة والملاحقة والابتزاز والتتبع بقصد فرض إقامة علاقة، كما تتجسّد بعض الجرائم الإلكترونية إلى نشر صور خاصة للأطفال "الجنس السياحي" للأطفال ونشر الجنس التخلي من خلال استخدام البريد الإلكتروني وإرسال الرسائل (سلامة، 2023، ص. 405).

#### أنماط مرتكبي الجريمة الإلكترونية:

تتعدد شخصيات مرتكبي الجريمة الإلكترونية كما أوضحها (عبد، 2006) لأنماط هي:

1. **شخص متخصص:** يتسم بقدرة ومهارة في استخدام التقنية ويستغل مداركه ومهاراته في اختراق الشبكات وكسر كلمات المرور أو الشفرات ويسبج في عالم الشبكات ليحصل على البيانات والمعلومات الهامة في أجهزة الحواسيب ومن خلال الشبكات.
2. **شخصية إجرامية:** يتسم فيها المجرم المعلوماتي بأنه يعود للجريمة دائماً فيوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به، لأنه يقوم بالاختراق نتيجة شعوره بقدرة ومهارته في الاختراق.
3. **شخص احترافي:** يتسم بامتلاك القدرات والمهارات التقنية ما يؤهله لوظيفة تمكنه من الاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية مقابل المكاسب المالية.
4. **شخص ذكي:** يتسم هذا الشخص بالمهارات التي تؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب.
5. **الهاكرز:** هو المتسلل المحترف الذي يستغل خبراته وإمكاناته في هذا المجال للتسلل إلى مواقع معينة للحصول على معلومات سرية أو تخريب وإتلاف نظام معين وإلحاق الخسائر به بقصد الانتقام أو الابتزاز.
6. **الكرارز:** هو الهاوي أو المحترف الذي يستخدم قدراته الفنية في اختراق الأنظمة والأجهزة تحقيقاً لأهداف غير قانونية كالحصول على معلومات سرية أو القيام بأعمال تخريبية والعبث بالشفرات وتآليف الفيروسات (عبد، 2006، ص. 250).

وتؤكد الباحثة في هذه الدراسة من خلال ما سبق ذكره أن الجريمة الإلكترونية المعلوماتية هي جرائم ذكاء ولا تحتاج لاستخدام القوة والعنف، حيث يلجأ مرتكبوها إلى استخدام ذكائهم لاكتشاف الثغرات واختراق البرامج المحصنة. وعادة ما تتراوح أعمار هذه الفئة من (18-45 سنة)، ويمتلكون المهارة والإلمام الكامل والقدرة الفنية الهائلة في مجال نظم المعلومات، وأغلبهم من الطبقة المتعلمة والمتقنة والمتخصصة في مجال الحاسب الآلي ولديهم القدرة على اختراق التحصين والحماية. كما أن مرتكبي الجريمة الإلكترونية يتمتعون بالثقة الزائدة بالنفس والإحساس بإمكانية ارتكابهم للجرائم دون افتضاح أمرهم، مع إلمامهم التام بأدوات ارتكابها وبما يجنبهم المواقف المفاجئة التي تؤدي إلى إفشالهم وافتضاح أمرهم.

#### النظريات المفسرة لموضوع الدراسة:

– **نظرية التقليد:** يرى أنصار هذه النظرية أن الجريمة حقيقة اجتماعية، حيث تنشأ وتتكون وتتطور وفق قوانين أساسية يخضع لها جميع أفراد المجتمع. وكما ترى النظرية، فإن الأفراد يقلد بعضهم بعضاً بدرجة تتفاوت طردياً بحسب شدة الاختلاط، فالتقليد في المدينة يزيد عنه في القرية. وينشأ المجرم مجرماً عندما يعيش داخل مجتمع إجرامي، فالجريمة مهنة يتعلمها الطفل من البيئة التي يعيش بها؛ حيث يقلد المجرمين من أسرته وأصدقائه. أي أن السلوك الإجرامي مكتسب نتيجة الاحتكاك بالمجتمع وتقليد أفراد بعضهم بعضاً، حيث إن التقليد والمحاكاة هما الأساس في تفسير تعميم السلوك وبالتالي تفسير الجريمة. فلا بد من وجود قدوة لأي نمط سلوكي، فالمجرم يقلد في فعله مجرماً آخر، وأن التقليد ينتقل من الطبقات العليا إلى السفلى ويتأثر بالعادة والذاكرة والفضول والاختلاط (سلامة، 2023، ص. 406).

- **نظرية اللامعيارية أو الأنومي:** لـ إميل دوركايم، تنطبق هذه النظرية بحسب ما جاء به من أنه نتيجة اختلال التركيب الاجتماعي تضعف القيم والأعراف والمعتقدات، الأمر الذي يؤدي إلى حالة اللانظام (الأنومي)، فتختفي المعايير والقيم والقواعد، بحيث لا يمكن قياس سلوك ما عليها لتصنيفه باعتباره سلوكاً سوياً أو غير سوي، مما يعني زوال الوسائل المتبعة في الضبط الاجتماعي. وقد يواجه الأسوياء نتيجة ذلك صعوبة في تلبية احتياجاتهم، فيحدث قلق وتوتر لدى الفرد، وبالتالي ارتباك أو عزلة عن المجتمع، وقد يصبح معادياً وغير مكترث بوسائل الضبط الاجتماعي، مما ينعكس على القيم التي تسنها المجتمعات لإشباع الأفراد متطلباتهم بطرق مشروعة. فينتج عن ذلك محاولة الأفراد تحقيق أكبر قدر ممكن من رغباتهم والوصول إلى أهدافهم دون وجه حق، مما لا يستطيعون تحقيقه بالوسائل القانونية التي تحددها قيم المجتمع (محمد، 2021، ص. 453).

#### الدراسات السابقة:

- **دراسة (النفيعي، 2002):** هدفت التعرف على نوع الفئة المرتادة لمقاهي الإنترنت والعوامل التي تجذب المترددين التواجد في هذه المقاهي، كذلك التعرف على أثر التعامل مع الإنترنت في المقاهي على الانحراف السلوكي الجنائي للمترددين الكشف عن علاقة الخصائص الديموجرافية لمترادي مقاهي الإنترنت بأرائهم نحو مقاهي الإنترنت والانحراف إلى الجريمة بين مترادياها، وقد توصلت الدراسة إلى أن أغلب أفراد عينة الدراسة من الشباب ممن قلت أعمارهم عن 30 سنة وحوالي ثلثي أفراد عينة الدراسة من مستخدمي الإنترنت الموقوفين بإصلاحية الدمار ودار الملاحظة الاجتماعية بالدمام من الشباب ممن تقع في الفئة العمرية (أقل من 30 سنة)، وحوالي ثلثي عينة المترادين عزاب وحوالي ثلثي عينة الموقوفين عزاب، وأكثر عينة المترادين موظفين، ونصف عينة الموقوفين موظفين، وقد أظهرت النتائج ارتفاع المستوي التعليمي نسبياً لأكثر من ثلاثة أرباع عينة المترادين (ثانوي أو ما يعادل فأعلى)، والارتفاع النسبي للمستوي التعليمي لحوالي ثلثي عينة الموقوفين (ثانوي أو ما يعادل فأعلى)، وارتفاع الدخل الشهري نوعاً ما لأسر حوالي ثلثي عينة المترادين من (6000 ريال فأكثر)، والانخفاض النسبي للمستوي التعليمي لحوالي ثلثي عينة الموقوفين من (4000 ريال فأقل).
- **دراسة (المنشاوي، 2003):** هدفت هذه الدراسة إلى الكشف عن حجم ونمط أكثر الجرائم الجنسية والممارسات غير الأخلاقية، وجرائم الاختراقات، والجرائم المالية، وجرائم المواقع المعادية، وجرائم القرصنة الأكثر شيوعاً، والتي يرتكبها مستخدمي الإنترنت في المجتمع السعودي وتحديد أهم سمات وخصائص مرتكبها، وقد أظهرت نتائج الدراسة أن هناك الكثير من الجرائم والممارسات غير الأخلاقية التي يرتكبها مستخدمي شبكة الإنترنت في المجتمع السعودي، وقد اتضح من خلال إجراءات البحث الميداني، ومن نتائج الدراسة عدم وجود جهة أمنية متخصصة للتعامل مع جرائم وسلبات الإنترنت، كما أثبتت نتائج الدراسة أن (4.12%) من مستخدمي شبكة الإنترنت في المجتمع السعودي يستخدمون البروكسي للدخول إلى المواقع المحجوبة، ثبت من نتائج الدراسة أن احتمال ميل فئة الأطفال والمراهقين والشباب قوي لارتكاب حوالي نصف الجرائم والممارسات التي شملتها الدراسة، أثبتت الدراسة انعدام احتمال ميل الإناث وكذلك انعدام احتمال ميل ربات المنازل من مستخدمي شبكة الإنترنت في المجتمع السعودي لارتكاب الجرائم والممارسات التي شملتها الدراسة. وأتضح أن أكثر جرائم وممارسات الإنترنت شيوعاً في المجتمع السعودي هي جرائم الاختراقات يليها الجرائم المالية وجرائم المواقع المعادية كجرائم وممارسات متوسطة الشيع أما الجرائم والممارسات الأقل شيوعاً فأتضح أنها الجرائم الجنسية وممارسة الأفعال غير الأخلاقية.
- **دراسة (محمد، 2021):** هدف البحث إلى التعرف على الأسباب الكامنة وراء اقتراف الجريمة الإلكترونية وأشكال الجريمة الإلكترونية المرتكبة عبر مواقع التواصل الاجتماعي ومعرفة الأساليب المتاحة لاقتراح الجريمة الإلكترونية وتأثير الجريمة الإلكترونية المرتكبة عبر مواقع التواصل الاجتماعي على الأفراد. والتعرف على الأحكام الجنائية الصادرة للجرائم المرتكبة

ووضع حلول للحد من ظاهرة الجريمة الإلكترونية المرتكبة عبر مواقع التواصل الاجتماعي. تم الاعتماد على المنهج الوصفي، أداة البحث تم تصميم استمارة تحليل المضمون، تبين من نتائج الدراسة معظم المحاضر كان المجني عليهم من الإناث فيما عدا كان عدد (2) محضر كان المجني عليه (ذكر)، وتبين أن أسباب اقتراف الجريمة الإلكترونية يرجع إلى عوامل اجتماعية واقتصادية وعوامل أخرى منها سهولة الوصول للهدف (المجني عليه)، الانتقام والتحدي. وأن الشكل الغالب للجرائم الإلكترونية يتمثل في التعذيب الرقمي والمطاردة السيبرانية. وكان تأثير الجريمة الإلكترونية.

• **دراسة (موسى وأبو عكير، 2023):** هدفت هذه الدراسة إلى الكشف عن الخوف الإلكتروني وعلاقته بمستويات القلق الاجتماعي لدى عينة من الشباب بلغ عددهم (600) طالب وطالبة من طلاب الجامعة تم اختيارها بطريقة كرة الثلج، وتم الحصول على العينة من خلال مجموعات التواصل الاجتماعي عن طريق الفيس بوك. وكانت العينة المسحوبة للدراسة من البيئة المصرية والقطرية والأردنية. واستخدمت الدراسة مقياس الخوف من الجريمة الإلكترونية، ومقياس القلق الاجتماعي، وتم تقدير مؤشرات الصدق والثبات للعينة. وقد ثبت من النتائج وجود علاقات ارتباطية موجبة متوسطة (0.227-0.374) بين أبعاد الجريمة الإلكترونية والدرجة الكلية على المقياس مع القلق الاجتماعي كدرجة كلية، وقد أثبتت الدراسة تحيز النتائج وبررته من الاستحسان الاجتماعي، أو الرغبة في تحسين صورة الذات، وبخاصة للأفراد ممن تعرضوا لدرجة من الجرائم الإلكترونية الموجهة نحو الأفراد، أو الشعور بالخزي والوصم في الإبلاغ عن تعرضهم للجرائم الإلكترونية. وتوصي الدراسة بضرورة رفع الوعي الإلكتروني لدى الشباب لخفض سلوكيات القلق الاجتماعي وتنمية إدراك الشباب للخطر الوارد من الترويج، أو التداول أو الإنتاج، أو أي فعل يوقع الشباب كضحية لارتكاب جريمة إلكترونية.

#### مدى الاستفادة من الدراسات السابقة:

- تنوعت الدراسات السابقة وقد اعتمدت جميعها على المنهج الوصفي، عدا دراسة واحدة اعتمدت على المنهج التحليلي وهو ما اتبعته الباحثة في الدراسة الحالية.
- أسفرت النتائج في كل الدراسات السابقة على وجود آثار اجتماعية سلبية على مرتكبي الجريمة الإلكترونية وعلى المجتمع ككل وهذا ما ركزت عليه الباحثة في هذه الدراسة.
- استفادت الدراسة الحالية من الدراسات السابقة في توفير القاعدة المعلوماتية لصياغة مشكلة الدراسة والأهداف والإطار النظري.

#### مناقشة وتحليل النتائج:

إجابة السؤال الأول: ما هي أهم الأبعاد الاجتماعية للجريمة الإلكترونية وتأثيراتها على البناء الاجتماعي للمجتمع؟

تبين من خلال الاطلاع على الدراسات السابقة والأدبيات التي تناولت مجال الجريمة الإلكترونية ارتباطها بالبطالة والظروف الاقتصادية الصعبة، خاصة بين الشباب ممن يمتلكون المعرفة ويستثمرونها في النشاط الإجرامي الإلكتروني. كما تُعد الضغوط الاجتماعية والنفسية التي يتعرض لها الفرد والمجتمع من فقر وبطالة وأمية وظروف اقتصادية صعبة عوامل ضاغطة على الشباب والمجتمع ككل، مما يولد مشاعر سلبية لديهم تدفعهم إلى أساليب تكيف وتوافق سلبية. ويمثل الإتجار الإلكتروني بالبشر والجنس والجريمة الإلكترونية أحد هذه الوسائل سعياً للحصول على المتعة وتجنب الألم بالوسائل غير المقبولة اجتماعياً لتحقيق أهداف مقبولة اجتماعياً. وهذا ما أوضحته نظرية "اللامعيارية" (دوركاييم) بأن الرغبة في الثراء تعترضها صعوبات بالغة في تحقيقها بالطرق المقبولة اجتماعياً وقانونياً؛ ولذلك يلجأ بعض الشباب إلى الجرائم الإلكترونية، حيث المستهدف مجتمع أكبر وسهولة التنفيذ وسرعة المردود وقلة الخطورة على مرتكبيها. وتتجسد التأثيرات المباشرة لهذه الأبعاد الاجتماعية في تدمير سمعة الأفراد والمؤسسات، وتفكك العلاقات الأسرية والاجتماعية الناتجة عن الابتزاز والتشهير الإلكتروني، مما يهدد بنية الثقة والتضامن الاجتماعي. ويزيد من سرعة انتشارها وفعالية أخطارها على الضحايا ضعف إنفاذ القانون وتطبيقه على الجريمة

الإلكترونية في الكثير من المجتمعات، وكذلك ضعف الشرطة الإلكترونية والتحقيق والقضاء وكيفية التعامل مع الأدلة الرقمية في مجتمعاتنا العربية، وغياب التشريعات الجزائية والجنائية، وضعف الممارسات العدلية والشرطية والقضائية في محاكمة والتحقيق في الجرائم الإلكترونية، وغالباً ما تجد في دول كثيرة تواضع التقنيات المتوافرة وكذلك الخبراء القادرون على متابعة ورصد وملاحقة الجريمة الإلكترونية داخل المجتمع والعابرة منها للحدود الوطنية.

إجابة السؤال الثاني: ما هي المسببات الاجتماعية للجريمة الإلكترونية وأثارها على كل من الضحية ومرتكب الجريمة؟

أوضحت هذه الدراسة اختلاف المسببات الاجتماعية للجريمة الإلكترونية وفق هدفها، سواء كان سرقة المعلومات أو تجارة المعلومات، أو كانت شخصية إجرامية ارتكبت جرائمها من باب التحدي وحب الظهور في الإعلام، أو بسبب الضغوطات الاجتماعية. حيث تؤدي البيئة الاجتماعية إلى الخروج على القواعد الاجتماعية والانحراف عن قواعد الامتثال وعدم وجود رقابة. وهذه العوامل تزيد من فرصة ارتكاب الجريمة الإلكترونية، وبالتالي يمكن سرقة المعلومات ومحتوياتها، فهي فرصة مربحة وقليلة المخاطر. وتنطلق هذه الدراسة من النظريات السلوكية القائلة بأن البيئة الاجتماعية تخلق شباباً ذوي ضبط منخفض للذات. وتؤكد هذه النظريات أن احتمالية انخراط الشباب في الأفعال الإجرامية تحدث بسبب وجود الفرصة مع توفر سمة شخصية من سمات الضبط الذاتي المنخفض، وأنه سلوك يقوم على القوة والخداع لتحقيق الرغبات الذاتية. وبناءً على ذلك، يُستدل على طبيعة هذا السلوك من خصائص الأشخاص ويُعد مظهراً من مظاهر الضبط الذاتي المنخفض. وتؤكد نظرية الضبط الاجتماعي بأن الدوافع لارتكاب هذا السلوك ليست متغيرة، لأن كل فرد قد يندفع لتحقيق مصالحه الشخصية بما في هذا السلوك، فهو عمل سهل قد يُحقق المصالح الخاصة بسرعة دون انتظار أو بذل جهد. ولكن الاختلاف بين الأفراد يعود إلى مستوى ضبط الذات، ووجود الفرصة لارتكاب السلوك المنحرف. وهذا ما تؤكدته دراسة كل من (محمد، 2021) و (موسى وأبو عكير، 2023) بأن توفر الضبط الذاتي المنخفض مع وجود الفرصة لارتكاب السلوك المنحرف يُعدان عاملين مؤثرين في ارتكاب هذا السلوك، فالاختلاف بين مرتكبي هذه الجرائم يرجع إلى الاختلاف في مستوى ضبط الذات؛ لأن نقص ضبط الذات قوة طبيعية تظهر في غياب الخطوات من أجل تطويره، أي أنه نتاج للتنشئة الاجتماعية الناقصة، حيث يفشل الآباء في مراقبة سلوك أبنائهم ولا يلاحظون السلوك المنحرف بسبب إهمال معاقبة الأبناء عند اقترافهم لسلوك منحرف. وعندما يتكون الضبط الذاتي في المراحل الأولى عند الأفراد، فإن الاختلافات في ضبط الذات تبقى ثابتة بشكل معقول من الوقت الذي تم تحديده عبر أطوار الحياة غير متأثر بالمؤسسات الاجتماعية، بل على العكس، فإن ضبط الذات قد يؤثر على أداء الأفراد في هذه المؤسسات مثل المدرسة والعمل والزواج. والأشخاص ذوو الضبط المنخفض لا يميلون إلى السلوكيات المنحرفة فقط، بل إنهم في الأغلب غير ناجحين في المدرسة أو العمل أو الزواج، وأن لديهم استعداداً لتحمل المخاطر من أجل تحقيق مكاسب قصيرة الأجل. وهذا قد ينطبق على الأفعال التي يمكن أن تُسهل أو تتعزز بواسطة وسائط الاتصالات الإلكترونية والإنترنت. بالإضافة إلى ذلك، يتعرض الأفراد على الإنترنت لنماذج التعلم الإجرامي والأقران، وقد يكونون أكثر ميلاً للانخراط في الجريمة الإلكترونية. وتتفق نتائج هذه الدراسة مع ما جاء في نظرية التقليد؛ ففي الجرائم الإلكترونية يحتاج مرتكبو هذه الجرائم إلى تعلم تقنيات تمكنهم من التصرف في البيئة الافتراضية كما يتصرفون في العالم الحقيقي. ويزداد ضحايا الجريمة الإلكترونية من خلال التغييرات في أنشطة الأفراد الروتينية في الحياة اليومية، فمع ظهور شبكة الإنترنت تغيرت طرق التواصل والتفاعل مع الآخرين في العلاقات الشخصية والترفيه والتجارة، كما أن استخدام شبكة الإنترنت وشبكات التفاعل الاجتماعي والفيديو والإيميل والمواقع خلقت فرصاً لمرتكبي الجرائم الإلكترونية المتحفرين مع وجود أهداف سهلة في هذه الشبكات وغياب الحراسة، فالجريمة الإلكترونية تحدث بالتقاء الجاني المتحفر والهدف المناسب وغياب الحراسة والرقابة الاجتماعية. أما عن أثارها على الضحية، فبالإضافة إلى الخسائر المادية والمعنوية، تشير الدراسات (مثل موسى وأبو عكير، 2023) إلى أن الضحايا قد يعانون من القلق الاجتماعي والخوف من الجريمة الإلكترونية، وقد يتملكهم الشعور بالوصم والخزي، مما يدفعهم إلى عدم الإبلاغ عن تعرضهم للجرائم، وهذا يفاقم من انتشار الظاهرة في المجتمع. كما سبب ازدياد الوفود البشرية من الريف إلى المدينة



وإلى المناطق الحضرية والمدن الكبيرة، وخاصة هجرة الشباب غير المتمكنين من مواجهة متطلبات الحياة الحضرية باهظة التكاليف والتي تتطلب مهارات عالية، مما يجعل الكثير من المهاجرين غير قادرين على تلبية متطلبات الحياة الحضرية فيضطرون للسكن في أحياء طرفية غير ملائمة، فيجد الشاب نفسه في تنافس غير قادر على مجاراته مما يجعله يلتفت إلى الاستثمار في الجريمة الإلكترونية المربح حيث لا تتطلب رأس مال كبير.

إجابة السؤال الثالث: ما هي أهم الاستراتيجيات والآليات للحد من الجرائم الإلكترونية؟ أشارت دراسة كل من (النفيعي، 2002) و (المنشاوي، 2003) و (محمد، 2021) أن استراتيجيات مواجهة الجريمة الإلكترونية تتضمن مجموعة من الإجراءات العلاجية التنظيمية والتوعوية والوقائية، والتي من شأنها أن تحد من تفاقم أضرار هذه الجرائم ومواجهة مرتكبيها وردعهم وهي على النحو التالي:

#### الاستراتيجيات العلاجية والتنظيمية:

- الإبلاغ الفوري عن الجريمة الإلكترونية التي يمكن أن يتعرض لها الفرد إلى الجهات المختصة في أقرب وقت ممكن.
- طلب المساعدة القانونية واستشارة محامٍ أو خبير قانوني عند التعرض للاحتيال أو الابتزاز للحصول على حلول قانونية احترافية.
- الإبلاغ عن التهديدات الخطيرة والمباشرة، ويجب الاتصال برقم الطوارئ المحلي.
- وضع قوانين وتشريعات رادعة خاصة بجرائم المعلوماتية وتحديد عقوبات صارمة لمرتكبيها.
- تطوير طرق ووسائل التتبع والتحقيق في هوية مرتكبي الجرائم الإلكترونية والقبض عليهم بدقة.
- تعزيز التعاون الدولي بين الدول لمكافحة الجرائم الإلكترونية التي تتجاوز الحدود الجغرافية.
- تفعيل مهام وحدات الشرطة الإلكترونية والمحاكم المتخصصة في الجرائم الإلكترونية لتعزيز القدرة على الاستجابة.

#### الاستراتيجيات التوعوية والاجتماعية:

- زيادة الوعي المجتمعي بمخاطر الجرائم الإلكترونية وكيفية الوقاية منها من خلال وسائل الإعلام.
- تطوير المهارات التقنية وتشجيع الأفراد والمؤسسات على تعزيز مهاراتهم في هذا المجال لمواجهة التهديدات المتطورة.

#### الاستراتيجيات الوقائية:

- استخدام كلمات مرور معقدة وقوية وتغييرها بانتظام وتفعيل المصادقة الثنائية متعددة العوامل لزيادة الأمان.
- الحذر من الرسائل والروابط المشبوهة وتجنب فتح رسائل البريد الإلكتروني والروابط المجهولة والحذر من الإعلانات التي قد تكون احتيالية.
- تثبيت وتحديث برامج الحماية من مكافحة الفيروسات والاختراقات على الأجهزة والقيام بتحديثها بانتظام.
- الحفاظ على خصوصية المعلومات الشخصية: تجنب نشر المعلومات الشخصية والصور على وسائل التواصل الاجتماعي بشكل مفرط.
- تجنب استخدام وتثبيت البرامج المجهولة من مصادر غير موثوقة لتجنب القرصنة وسرقة الحسابات.
- تغيير كلمات المرور بانتظام خاصة للحسابات المصرفية أو حسابات مواقع التواصل الاجتماعي.

#### الاستنتاجات:

- تُعد الجريمة الإلكترونية جريمة تمس الآداب العامة والأخلاق بسبب اختراق مرتكبيها لحسابات ونظم معلوماتية للآخرين، مما يستهدف تدمير وإعادة نشر معلومات سرية وشخصية أو إتلافها لغرض السرقة والاحتيال والمطاردة والمضايقة والتحرش والاعتداء.
- يُعتبر أغلب مرتكبي الجريمة الإلكترونية من الفئة العمرية (18-45 سنة)، أي المرحلة التي يكتمل فيها الإدراك وتتحدد فيها ملامح الشخصية أيًا كانت تركيبتها (سوية أو منحرفة).

- لجوء مرتكبي الجريمة الإلكترونية إلى ارتكابها ببث تسجيلات صوتية أو مرئية من خلال شبكة الإنترنت مقابل كسب مال غير مشروع دون إذن صاحبها، وهو ما يُجرّم هذا الفعل قانوناً.
- انتقال المجتمعات العربية من مجتمعات تقليدية إلى مجتمعات رقمية افتراضية، وما ترتب عليه من انتقال أنشطة الأفراد من واقع مادي ملموس إلى واقع افتراضي تنهار فيه القيم المجتمعية ويسهل فيه إلحاق الأذى والجرائم بالآخرين والوصول إليهم.
- ضعف الوازع الديني والأخلاقي وانشغال أرباب الأسر بملاحظة عجلة الحياة السريعة عن تربية أبنائهم وملاحظة سلوكياتهم، بالإضافة إلى تلبية رغبات الأبناء مهما كانت وأينما وجدت، خلق بداخلهم الاستهانة بالآخرين وإلحاق الضرر بهم.

#### التوصيات:

- التوعية والتنقيف لطلاب المدارس والموظفين ومستخدمي شبكات الإنترنت بكيفية حماية حساباتهم وخصوصيتهم المعلوماتية.
- العمل على تنمية وتطوير المتخصصين في مكافحة الجريمة الإلكترونية.
- حث الجامعات والمراكز البحثية العربية على البحث والدراسة في الجرائم عبر الإنترنت ومحاولة إنشاء دبلومات متخصصة في المجالات الفنية المتعلقة بمكافحة الجريمة الإلكترونية.
- إقامة الندوات والمحاضرات والمؤتمرات عن أبعاد الجريمة الإلكترونية وآثارها على المستوى الفردي والمجتمعي.

#### المراجع

1. توبة، عبد الحكيم رشيد. (2008). جرائم تكنولوجيا المعلومات. دار المستقبل للنشر والتوزيع. الأردن.
2. حامدي، محمد الصالح. (2012). علاقة تكنولوجيا المعلومات لظاهرة الاتجار بالبشر في عصر العولمة ومدى تأثيرها على دولة قطر. المجلة العربية الدولية للمعلوماتية، 1(2).
3. الديربي، عبد العالي. (2013). الجريمة المعلوماتية: أسبابها وخصائصها. (دراسة منشورة). المركز العربي لأبحاث الفضاء الإلكتروني.
4. الرومي، أحمد. (2003). جرائم الكمبيوتر والإنترنت. دار المطبوعات الجامعية. الإسكندرية.
5. سلامة، نسرين سيد. (2023). الجرائم الإلكترونية وأثرها على المجتمع. مجلة القاهرة للخدمة الاجتماعية، (39)، 389-422.
6. العريان، محمد. (2004). الجرائم المعلوماتية. دار الجامعة الجديدة للنشر. الإسكندرية.
7. عبده، هاني خميس أحمد. (2006). الأبعاد الاجتماعية للجرائم المعلوماتية (أطروحة دكتوراه غير منشورة). جامعة الإسكندرية. مصر.
8. عبد المطلب، ممدوح. (2001). جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية (ط. 1). دار الحقوق. الشارقة.
9. النفيعي، مزيد بن مزيد. (2002). مقاهي الإنترنت والانحراف إلى الجريمة بين مرتاديها: دراسة تطبيقية على مقاهي الإنترنت بالمنطقة الشرقية (رسالة ماجستير غير منشورة). جامعة نايف للعلوم الأمنية. الرياض، السعودية.
10. الملط، أحمد خليفة. (2006). الجرائم المعلوماتية (ط. 2). دار الفكر الجامعي. الإسكندرية.
11. محمد، وفاد محمد علي. (2021). الأبعاد الاجتماعية للجرائم الإلكترونية: دراسة تحليلية لمضمون عينة من القضايا في محكمة سوهاج. مجلة كلية التربية، جامعة عين شمس، 3(27)، 425-504.
12. المنشاوي، محمد بن عبد الله. (2003). جرائم الإنترنت في المجتمع السعودي (رسالة ماجستير غير منشورة). جامعة نايف للعلوم الأمنية. الرياض، السعودية.

13. موسى، محمود علي، وأبو بكر، محمد نايف. (2023). الخوف من الجريمة الإلكترونية المستهدفة للأفراد وعلاقته بالقلق الاجتماعي لدى عينة الشباب. مجلة جامعة نايف العربية للدراسات الأمنية، 39(2)، 135-163.
14. الهيتي، محمد. (2006). جرائم الحاسوب ماهيتها، موضوعها، أهم صورها: دراسة تحليلية لواقع الاعتداءات التي تعرض لها الحاسوب وموقف التشريعات الجنائية منها. دار المناهج للنشر والتوزيع. عمان.

**Disclaimer/Publisher's Note:** The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of **CJHES** and/or the editor(s). **CJHES** and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.