العدد ثلاث وأربعون
تاريخ الإصدار: 2 – أيار – 2022م
www.ajsp.net
ISSN: 2663-5798

"مُعوقات مُكافحة الجرائم الإلكترونية في المُجتمع الأردني من وجهة نظر ذوي الإختصاص"

(أُطروحة مُقدّمة إلى كُليّة الدّراسات العُليا استكمالًا لمتطلبات الحصول على درجة الدكتوراه في علم الاجتماع – تخصص علم الجريمة)

إعداد الباحث:

غُدي محمد علي الشوابكة

طالب دكتوراه في قسم علم الاجتماع– تخصص علم الجريمة/ جامعة مؤتة

إشراف:

الأستاذ الدكتور قُبلان المجالي

أستاذ علم الاجتماع الأستاذ الدكتور قُبلان المجالي– كلية العلوم الاجتماعية/ جامعة مؤتة

جامعة مؤتة، 2022م

العدد ثلاث وأربعون
تاريخ الإصدار: 2 – أيار – 2022م
www.ajsp.net
ISSN: 2663-5798

المُلخص:

هدفت الدراسة إلى التعرف على المُعوقات الفنية والقانونية لمُكافحة الجرائم الإلكترونية في المُجتمع الأردني من وجهة نظر ذوي الاختصاص، وقد تكون مجتمع الدراسة من جميع المختصين في مجال الجرائم الإلكترونية في كل من: وحدة الجرائم الإلكترونية في مديرية الأمن العام، المركز الوطني للأمن السيبراني، القضاة المُتخصصين في الجرائم الإلكترونية، الخبراء الفنيين المُعتمدين لدى القضاء النظامي الأردني، والبالغ عددهم جميعاً (106) مختص. فيما تكونت عينة الدراسة الاستطلاعية من (20) مختصاً، والعينة الأساسية من (80) مختصاً.

وقد اسفرت نتائج الدراسة عما يلي: جاءت المُعوقات القانونية بدرجة (مرتفعة وبالمرتبة الاولى)، المُعوقات الفنية بدرجة (متوسطة وبالمرتبة الثانية). وبناء على نتائج الدراسة أوصى الباحث بضرورة تنمية الوعي المجتمعي حول الجرائم الالكترونية وبكافة الوسائل الإعلامية. العمل على تنظيم مؤتمرات دولية يجتمع فيها ذوي الاختصاص بهدف الاتفاق وتطوير اللوائح والتشريعات القانونية المُتعلقة بمُكافحة الجرائم الالكترونية على المستوى الدولي والوطني. بالإضافة الى ضرورة عقد دورات تدريبية محلية ودولية لذوي الاختصاص العاملين في مجال مُكافحة الجرائم الالكترونية، بحيث أن تعمل هذه الدورات على صقل مهاراتهم وقدراتهم في التعامل مع الجرائم الالكترونية بكفاءة عالية.

الكلمات المفتاحية: مُعوقات، مُكافحة، الجريمة الإلكترونية، ذوي الاختصاص.

مقدمة:

أدى التطور الكبير في الأنظمة الإلكترونية والانتشار الواسع لشبكة الويب العالمية إلى ظهور نمط جديداً من الجرائم أطلق عليها الجرائم الإلكترونية، حيث أن هذه الشبكة أوجدت عالماً افتراضياً جعل الجريمة لا تُرتكب بشكلها التقليدي وانتقلت من صورتها المادية التقليدية إلى صورة معنوية عابرة للحدود الجغرافية، الأمر الذي أدى إلى صعوبة تحديد هوية مُرتكب الجريمة لاستخدامه وسائل تقنية تُتيح له إخفاء نشاطه الإجرامي عن أجهزة العدالة، مما أثار جملة من التحديات أمام السلطات القضائية (مناعسة، 2001).

إن الجرائم الإلكترونية تُعد من أخطر الجرائم التي ظهرت حديثاً، حيث أن لها أثراً سلبياً على الفرد والمجتمع، وأيضاً على الصعيد الدولي لنموها المُستمر والمتطور، وهناك اهتماماً كبيراً من قبل الرأي العام الدولي حول أهميّة مُكافحتها لما تُسببه من خسائر كبيرة، حيث أصبحت خطورتها تُهدد أمن المُجتمعات وأخلاقياتها ومُكتسباتها، مما دفع المُجتمع الدولي إلى البحث عن آليات جديدة لمُكافحتها (الشحات، 2002).

حيث تم إبرام عدة اتفاقيات ومُعاهدات دولية لمُكافحة الجرائم المُرتبطة بتكنولوجيا المعلومات بعد إدراك الدول والحكومات مدى خطورة هذه الجرائم خاصة مع ازدياد استخدام التكنولوجيا الحديثة، ومن أهم المعاهدات التي أبرمت في إطار التعاون الدولي لمُكافحة هذه الجرائم المعاهدة الأوروبية ومُعاهدة بودابيست (2001)، حيث أكدت مُعاهدة بودابيست ضرورة اتخاذ تدابير تشريعية لمُكافحة الجرائم الإلكترونية، وعلى أهمية أخذ التدابير التشريعية والتنظيمية بحق مرتكبي هذه الجرائم لملاحتهم وكشف جرائمهم، والتأكيد على الحاجة إلى توحيد الجهود الدولية، فيما الزمت المعاهدة الأوروبية الدول الموقعة عليها بسن وتشريع القوانين للتعامل مع الجرائم الإلكترونية (عبابنة، 2004).

ذلك نتيجة لتنوع أساليب الجريمة الإلكترونية وتعدد أشكالها واتساع مجالاتها، حيث وفرت قدراً كبير من السلامة والأمان وخلق جو مريح لمُرتكبيها، ومع ارتباط المجتمعات الدولية بشبكات الاتصال الدولية زادت خطورة هذه الجرائم، فيما استغلت الجماعات والمنظمات الإرهابية تقنية المعلومات واستفادت منها، إذ أصبح من الممكن اتمام العمليات الإجرامية واختراق الأنظمة وتدمير بنيتها، وزادت خطورة هذه الجرائم في الدول المتقدمة كون بنيتها التحتية تُدار بالشبكات الإلكترونية (بوادي، 2006).

تبعا لذلك بذلت الأردن جهداً في مُكافحة الجرائم الإلكترونية، حيث أنها لم توفر جهداً على المستوى الدولي في مد أواصر التعاون في العالم، حيث تم عقد مجموعة من المؤتمرات في الأردن لمناقشة آثار هذه الجرائم وطرح التوصيات حولها، كما تمثل دور الأردن في التشريعات الوطنية والمؤسسات المعنية في مُكافحة هذه الجرائم، ويسعى محامو الأردن إلى مواكبة التطور في مجال التكنولوجيا (السالمي، 2002).

وفي ضوء تزايد مُعدلات الجرائم الإلكترونية في المجتمع الأردني، وتزايد الجهود في مُكافحة هذه الجرائم على المستوى المحلي والدولي، كان لابد من الدراسة والبحث لمعرفة المُعوقات والتحديات التي تقف أمام هذه الجهود في وقتنا الحاضر، فقد جاءت هذه الدّراسة محاولة للتعرّف على مُعوقات مُكافحة الجرائم الإلكترونية في المُجتمع الأردني، من وجهة نظر ذوي الاختصاص.

مشكلة الدراسة

رافق ظهور منصات التواصل الاجتماعي والشبكات الإلكترونية ظاهرة تعتبر من الظواهر المستجدة وهي ظاهرة الجرائم الإلكترونية، حيث أنها تطورت في الآونة الأخيرة لسهولة ارتكابها وصعوبة التعرف على مرتكبيها، ومع غياب التوعية بمخاطر الجرائم الإلكترونية وقلة المعرفة بقانون الجرائم الإلكترونية تزداد العرضة للجريمة الإلكترونية، لا سيما في ظل استخدام المواقع الإلكترونية ومنصات التواصل الاجتماعي لفترات طويلة (الضبان، 2019)، وأشارت الإحصائيات إلى أن نسبة مُستخدمي الإنترنت في الأردن لعام 2017 تبلغ 64% من عدد السكان للأعمار خمس سنوات فأكثر، فيما تحيط الجريمة الإلكترونية جملة من المُعوقات التي تقف أمام اكتشافها وإثباتها والوصول إلى الجاني، حيث أنه يصعب إثبات هذا النوع من الجرائم كون المجرم يتميز بالخبرات الفنية والعقلية ودرايته بتدابير الحماية الاحترازية التي تمكنه من إخفاء الدليل في ظل فقدان الآثار التقليدية للجريمة (موسى، 2009).

هذا وأشارت الأردن للجمعية العامة للأمم المتحدة 2019 ضمن تقرير عن مُكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية"، والذي شاركت فيه 60 دولة، بأن أبرز التحديات المُتعلقة بمُكافحة الجرائم الإلكترونية في الأردن، تتمثل بوجود برمجيات وبرامج مجانية تخفي هويات المستخدمين، الأمر الذي يحول دون تعقبهم وكشفهم، بالإضافة إلى إمكانية اكتساب المعرفة باستخدام الأدوات الإجرامية واكتساب الخبرة في استخدام تلك الأدوات، لتوافر المعلومات وسهولة الحصول عليها من مواقع مجانية على الشبكة العنكبوتية، بينما تشكل الشبكة الخفية مرتعاً خصباً للأعمال غير المشروعة، الأمر الذي يحد من إمكانية رصد هذه المواقع ومراقبتها، وذلك بسبب التشفير لغايات إخفاء هوية مستخدميها، وكذلك يشكل بطء الإجراءات وتبادل المعلومات في قضايا الجرائم الإلكترونية التي تقع في بعض الدول إحدى مُعوقات مُكافحة الجرائم الإلكترونية، ويضاف إلى ذلك عدم تجاوب بعض منصات التواصل الاجتماعي حول تبادل المعلومات مع أجهزة إنفاذ القانون وعدم تعاونها، ومن هنا برزت الحاجة لبناء القدرات من خلال برامج تدريبية دولية والتأكيد على أهمية تبادل الخبرات مع الدول المتقدمة في مسائل الجريمة الإلكتروني (الجمعية العامة للأمم المتحدة، 2019).

وبناءً على ما سبق، ونظراً لندرة الدراسات السسيولوجية التي تبحث في مُعوقات مُكافحة الجرائم الإلكترونية من الناحية الفنية والقانونية والاجتماعية في المجتمع الأردني تسعى الدراسة الحالية الى رصد وتحليل مُعوقات مُكافحة الجرائم الإلكترونية في المجتمع الأردني من وجهة نظر ذوي الاختصاص وهم العاملين في وحدة الجرائم الالكترونية، العاملين في المركز الوطني للأمن السيبراني، القضاة المُتخصصين في الجرائم الإلكترونية والخبراء الفنيين المُعتمدين لدى القضاء النظامي الأردني.

تساؤلات الدراسة

تسعى هذه الدراسة للإجابة عن التساؤلات الآتية:

1. ما المُعوقات الفنية في مُكافحة الجرائم الالكترونية في المجتمع الأردني، من وجهة نظر ذوي الاختصاص؟
2. ما المُعوقات القانونية في مُكافحة الجرائم الالكترونية في المجتمع الأردني، من وجهة نظر ذوي الاختصاص؟

أهداف الدراسة

تسعى الدراسة الى التعرف على الأهداف الآتية:

1. التعرّف إلى المُعوقات الفنية في مُكافحة الجرائم الالكترونية في المجتمع الأردني، من وجهة نظر ذوي الاختصاص.
2. التعرّف إلى المُعوقات القانونية في مُكافحة الجرائم الالكترونية في المجتمع الأردني، من وجهة نظر ذوي الاختصاص.

أهمية الدراسة

تكمن الأهمية العلمية للدراسة من جانبين:

أ- الأهمية النظرية:

وتكمن الأهمية النظرية في:

1- تُعدّ هذه الدّراسة من الدّراسات النادرة في هذا الحقل الذي يشكل تحدي كبير للقائمين على مُكافحة الجرائم الالكترونية في المجتمع الأردني، وهذا ما تبين للطالب وبحدود اطّلاعه بعد أن تم إجراء مسح مكتبي بخصوص موضوع الدّراسة.

2- تبرز أهمية الدراسة في رصد وتحليل مُعوقات مُكافحة الجرائم الالكترونية في المجتمع الأردني، من وجهة نظر ذوي الاختصاص وفقًا لمتغيّرات الدّراسة.

ب–الأهمية التطبيقية:

وتكمن الأهمية التطبيقية في:

1– يتوقع أن تزوّد نتائج هذه الدّراسة الميدانية الباحثين وصنّاع القرار التشريعي والتنفيذي في الجوانب الفنية والقانونية، طلبة العلم وإدارة المؤسسات الحكومية، بمعلومات ميدانية دقيقة تساعدهم في تفّهم المُعوقات الفنية، القانونية والاجتماعية في مُكافحة الجرائم الالكترونية في المجتمع الأردني.

2– مساعدة أصحاب القرار والمتخصصين في السلطات التشريعية لصياغة القوانين والسياسات والبرامج الوقائية التي تحد منّ الجرائم الالكترونية في الأردن.

التعريفات الإجرائية

مُعوقات: صعوبات مواجهة الجريمة المعلوماتية، مثل اكتشاف وإثبات الجريمة المعلوماتية.

مُكافحة: أي مواجهة أي عمل غير قانوني ومقاومته باستخدام التشريعات والقوانين والأنظمة التي تساعد على ذلك.

الجريمة الإلكترونية: فعل غير مشروع يتم باستخدام الأجهزة الإلكترونية يقرر القانون له عقوبة، ينتج عنه الحصول على فوائد مادية أو معنوية وترتكب ضد أفراد أو جماعات بدافع جرمي.

ذوي الاختصاص: وتشمل كل من العاملين في وحدة الجرائم الالكترونية في مديرية الأمن العام والمركز الوطني للأمن السيبراني والقضاة المتخصصين في الجرائم الالكترونية والخبراء الفنيين المعتمدين لدى القضاء النظامي الأردني، وتقتصر هنا على حدود عينة ومجتمع الدراسة الحالية.

الإطار النظري والدراسات السابقة

الإطار النظري

رغم التطور التشريعي الهام الذي عرفته السياسات الجنائية سواء على المستوى الوطني او الدولي وما صاحب ذلك من تغيير للمفاهيم القانونية في سبيل محاربة الجريمة المعلوماتية التي لا تعترف بالإقليم فلا زالت هناك مجموعة من الإشكالات والصعوبات التي تعرقل وتقلص المجهودات الرامية إلى وضع حد لهذه الجرائم، وقبل التعمق بالمُعوقات يمكن سرد بعض الأمور التي تصعب على الجهات المختصة تذليل هذه المُعوقات، ويمكن تلخيصها في العناصر التالية:

1. عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي ذلك أن الأنظمة القانونية في بلدان العالم قاطبة لم تتفق على صور محددة يندرج في إطارها ما يسمى بإساءة استخدام نظم المعلومات الواجب اتباعها وربما يتجلى سبب غياب هذا النموذج في كثرة التعاريف والمفاهيم القانونية التي تؤطر هذا الجانب فكل دولة تضع تعريفات ومصطلحات حسب أنظمتها القانونية الجنائية

بالخصوص هذه الكثرة الناتجة أساساً عن التطور الذي يعرفه المجال المعلوماتي وبالتالي تطور تقنيات وسائل ارتكاب الجرائم المعلوماتية او جرائم الانترنيت (حجازي، 2006).

2. مسألة الطبيعية القانونية للمال المعلوماتي ومدى اعتباره مالاً مادياً أو معنوياً ومنقولاً باعتبارها هذا الأخير محلاً لمعظم جرائم الأموال (لحسن، 2008).

3. عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة بخصوص الجريمة المعلوماتية بين الدول المختلفة خاصة ما تعلق منها بأعمال الاستدلال أو التحقيق، فجرائم الحاسب الآلي آثار خارجية ظاهرة، وإنما تنصب على البيانات والمعلومات والمستندات المخزنة في نظم المعلومات والبرامج وبالتالي عدم الحصول على آثار مادية تشكل دليلاً لإثبات الجريمة المعلوماتية الواقعة وفي غياب أعمال العنف والاقتحام والتكسير على خلاف الجرائم العادية يصعب إثبات الجريمة بالإضافة إلى ارتكاب الجريمة المعلوماتية في الخفاء وتعمد الجاني عدم ترك أي دليل إدانة بعد ارتكابه للجريمة (لحسن، 2008).

4. عدم وجود معاهدات ثنائية أو جماعية بين الدول نحو يسمح بالتعاون المثمر في هذا المجال وحتى في حال وجودها فإنها لا تستطيع مواكبة التطور السريع لنظم وبرامج الحاسب وشبكة الانترنت، وتبرز أهمية وضرورة وجود مثل هذه المعاهدات عندما نستحضر الطابع العابر للحدود والقارات الذي تتميز به الجريمة المعلوماتية بحيث تتباعد المسافة بين الجاني ونتيجة فعله مما يؤثر سلبياً على أعمال البحث والتحري والتحقيق ونتيجة الطابع العابر للحدود لهذه الجريمة تظهر مشكلة الاختصاص على المستوى الوطني والدولي والقانون الواجب تطبيقه(لحسن، 2008).

5. ضخامة كم البيانات المعلوماتية التي تقف عائقاً أمام إجراءات التحقيق الجنائي والبحث عن دليل الإدانة والأكثر من ذلك تتجلى الصعوبة عندما يقوم الجاني بتشتيت المعلومات والمستندات رغبة منه في عدم الابقاء على أي دليل إثبات إضافة إلى أن طباعة كل ما هو موجود على الدعامة الممغنطة لحاسب متوسط العمر، يتطلب مئات ألاف الصفحات في الوقت الذي قد لا تقدم فيه هذه الصفحات شيئا مفيداً للتحقيق (حجازي، 2006).

المُعوقات الفنية في مُكافحة الجرائم الإلكترونية:

في تقرير تقييم تهديدات الجريمة المنظمة عبر الإنترنت لعام 2019، ناقش المركز الأوروبي للجرائم الإلكترونية (EC3) التابع لليوروبول التهديدات الرئيسية وأظهر أنه بينما يطور المجرمون أساليب مبتكرة لارتكاب الجرائم الإلكترونية، لا تزال غالبية الجرائم تعتمد على استخدام الأساليب الراسخة التي قدمت نتائجها عبر التاريخ، ويعني بالاستخدام المستمر لهذه الأساليب أن التحديات المشتركة لإنفاذ القانون لم تتغير في السنوات الأخيرة. يقدم التقرير نظرة ثاقبة للتحديات الخمسة الرئيسية (رمضان، 2015).

أولاً: فقدان البيانات:

بسبب التغييرات التشريعية مثل اللائحة العامة لحماية البيانات (GDPR)، قد يُحرم تطبيق القانون من الوصول إلى البيانات أو قد يتمكن فقط من الوصول إلى بيانات محدودة للغاية كجزء من تحقيق جنائي، وتمثل زيادة التطور التكنولوجي واستخدام الإنترنت أيضاً تحدياً لإنفاذ القانون، مما يؤدي إلى كميات كبيرة للغاية من البيانات حيث يصعب التمييز بين مستخدم معين (رمضان، 2015).

التشفير هو أداة أخرى يستخدمها المجرمون لمنع وصول البيانات إلى أيدي سلطات إنفاذ القانون، بينما يسمح استخدام العملات المشفرة مثل البيتكوين للمجرمين بالتعامل في عائدات الجريمة بمستوى نسبي من إخفاء الهوية، ويعتبر نقص البيانات التي تتطلبها جهات إنفاذ القانون له تأثير ضار كبير على عملهم، وغالباً ما يؤدي إلى تأخير التحقيقات أو حتى إيقافها (لحسن، 2008).

ثانياً: فقدان الموقع:

في حين أن استخدام التشفير والعملات المشفرة وغيرها من التقنيات مثل الويب المظلم أو التخزين السحابي قد يؤدي إلى فقدان البيانات، إلا أنها تمثل أيضاً تحديات كبيرة لتطبيق القانون في تحديد الموقع المادي للجناة أو البنية التحتية الجنائية أو الأدلة الإلكترونية، وهذا يثير اعتبارات قضائية معقدة ويجعل من الصعب تحديد المسؤول عن إجراء التحقيقات (حجازي، 2006).

ثالثاً: التحديات المرتبطة بالأطر القانونية الوطنية:

تختلف الأطر القانونية بين البلدان في أوروبا، مما يجعل التحقيق الفعال عبر الحدود وملاحقة الجرائم الإلكترونية أمراً صعباً للغاية، تتعلق الاختلافات الرئيسية بالسلوك الذي يتم تجريمه وكيف يمكن إجراء التحقيقات، وهذا الأخير له تأثير كبير على جمع الأدلة الإلكترونية ومراقبة الأنشطة الإجرامية عبر الإنترنت، والتي تعتبر بالغة الأهمية لأي تحقيق في جرائم الإنترنت (خليفة، 2016).

رابعاً: مُعوقات التعاون الدولي:

في حين أن الاختلافات في الأطر الوطنية تمثل تحديات أمام التعاون بين الدول الأعضاء في أوروبا، فإن الافتقار إلى إطار قانوني مشترك في جميع أنحاء العالم يمثل تحديات كبيرة للتعاون الدولي بشكل عام، هذا يمثل مشكلة خاصة في حالة الهجمات الإلكترونية واسعة النطاق التي تمتد عبر قارات متعددة، ويُنظر إلى المساعدة القانونية المتبادلة على أنها بطيئة وغير فعالة، مع عدم تأمين الأدلة في كثير من الأحيان في الوقت المناسب لضمان نجاح قضية جنائية (البداينة، 2009).

خامساً: تحديات الشراكة بين القطاعين العام والخاص:

غالبًا ما يمتلك القطاع الخاص مفاتيح تزويد أجهزة تنفيذ القانون بالبيانات الهامة لتسهيل التحقيقات، ويمكن أن يلعب دوراً رئيسياً في المساعدة على تفكيك البنى التحتية الجنائية، على الرغم من أهمية التعاون بين القطاعين العام والخاص، لا يوجد إطار قانوني واضح يحدد كيفية تعاون القطاع الخاص مع أجهزة تنفيذ القانون مع ضمان عدم انتهاك خصوصية عملائهم أو حقوقهم (المقصودي، 2015).

ترتبط تحديات أخرى بالتقنيات الجديدة والناشئة مثل الحوسبة الكمومية والذكاء الاصطناعي، أثناء تقديم الفرص لإنفاذ القانون والقطاع الخاص في الكشف والتخفيف، هناك أيضاً احتمال لسوء الاستخدام الإجرامي لتغذية الجرائم الإلكترونية (باطلي، 2013).

المُعوقات القانونية في مُكافحة الجرائم الإلكترونية:

على الرغم مما انطوت عليه ثورة الإعلام من تأثيرات إيجابية إلا أنها قد شهدت كذلك بعض التداعيات السلبية لاسيَّما تلك التي شهدتها وسائل التواصل الاجتماعي، التي تحفل بالعديد من الأنشطة التي يمكن إدراجها تحت مسمى الأفعال الإجرامية. فاستخدام الهواتف الذكية والأجهزة اللوحية على نطاق واسع، بالإضافة إلى سهولة الوصول إلى الانترنت ورغبة الشباب في المعرفة وشعورهم بالفضول في العديد من المناسبات أدى إلى استغلال شبكات الجريمة المنظمة لهم. علاوةً على ذلك، فقد استخدمت العديد من الجماعات الإرهابية الإنترنت كوسيلة لتجنيد أعضاء جدد، وطرح أيديولوجياتهم المتطرفة العنيفة (حامد، 2019).

وفي الأردن، أقرت الحكومة قانون مُكافحة الجرائم الإلكترونية في عام 2015. ولهذا الغرض، أنشأت مديرية الأمن العام في عام 2015، وحدة متخصصة باسم وحدة مُكافحة الجرائم الإلكترونية تختص بمعالجة جميع أشكال الجرائم الإلكترونية. وفي عام 2018، تم إدخال تعديلات على القانون شددت العقوبات على مرتكبي مثل هذه الجرائم (حامد، 2019).

وقد واصل مكتب الأمم المتحدة الإقليمي المعني بالمخدرات والجريمة للشرق الأوسط وشمال أفريقيا في إطار مشروعه "تعزيز القدرات التحقيقية وتعزيز التعاون الدولي في مُكافحة الجريمة المنظمة في الأردن" الذي تقوم حكومة اليابان بتمويله، واصل تقديم دعمه لمؤسسات إنفاذ القانون لمنع التطرف العنيف، وتعزيز التعاون الدولي في المسائل الجنائية من خلال مجموعة من الأنشطة مثل عقد دورات تدريبية لبناء القدرات، ووضع مرجع تدريبي مختص بمُكافحة الجرائم الإلكترونية، وعرض الممارسات الدولية في مجال منع التطرف العنيف والتعاون الدولي (حامد، 2019).

على الرغم من وجود التشريعات الدولية الضابطة لمُكافحة الجرائم الإلكترونية، إلا أن الاختلافات في الصياغات القانونية المحلية غالباً ما تثبت الأطر القانونية في الدول الأعضاء والتشريعات الدولية، وهو ما يعيق التحقيق الجنائي الدولي وملاحقة الجرائم الإلكترونية، ويرجع ذلك جزئياً إلى نقل غير كامل للقوانين الدولية في التشريعات المحلية (سعدات، 2015).

أما التكيف والمحاذاة من الأطر القانونية غالباً ما يستغرق وقتاً طويلاً وصعب، نظراً للتطور السريع في مشهد تهديدات الجرائم الإلكترونية، يمكن أن تكون السوابق القضائية (الاجتهاد القضائي) أداة قيمة لتعويض عدم وجود تشريعات محددة، ولكن لسوء الحظ، لا يوجد الكثير من السوابق القضائية للتعامل مع الجديد من التطورات (مثل الانتهاك الجنائي للعملات المشفرة وأدوات إخفاء الهوية ومختلف أساليب العمل الإجرامية القائمة على التكنولوجيا)، علاوة على ذلك، العمليات التشغيلية الحالية (مثل أن تستفيد عملية المساعدة القانونية المتبادلة (MLA) من تنسيق وعملية أفضل، وبالمثل، فإن معايير الطب الشرعي الفنية لجمع ونقل الأدلة الإلكترونية يمكن تطويرها وتعزيزها واعتمادها، وينطبق نفس الوضع على التشريعات المخصصة التي تنظم القانون بشكل أكثر تحديداً حضور وإنفاذ في بيئة عبر الإنترنت، ينبغي أن يكون مثل هذا التشريع منسقاً على مستوى الاتحاد الأوروبي، والتي من شأنها أن تسمح بإجراءات تشغيلية مشتركة أكثر فعالية مثل شبكات الروبوتات واسعة النطاق و / أو عمليات الإزالة للمنتدى الجنائي السري، على وجه التحديد، احتمالات مراقبة الأنشطة الإجرامية عبر الإنترنت وجمع الأدلة الهامة بشكل قانوني على Deep Web ويمكن تنسيق الويب المظلم عبر الاتحاد الأوروبي للسماح بالأنشطة التشغيلية الفعالة والتقديم اللاحق للأدلة في الإجراءات القضائية (المهدي، 2018).

وتعتبر هذه المسألة ذات أهمية متزايدة بسبب زيادة تدابير الأمن العملياتي اعتمدها المجرمون على شبكة الويب المظلمة (مثل المصادقة الثنائية، والرسائل المشفرة، الضمان متعدد التوقيع، وما إلى ذلك) بعد العمليات الناجحة، على الرغم من أن المنتديات

السرية لا تزال جزءاً حيوياً من نموذج أعمال المجرمين الإلكترونيين، وهو تقارب متزايد بين مجرمي الإنترنت للدردشة الحديثة الخدمات التي تقدم التشفير من طرف إلى طرف كما تمت ملاحظتها حيث يخلق هذا الموقف المزيد من العقبات (المهدي، 2018).

النظريات المفسرة

نظرية التعلم الإجتماعي

وضع هذه النظرية العالم الأمريكي "سذرلاند" والتي تتمحور حول محتويات الأنماط المقدمة من خلال الارتباط، وهي نظرية عامة للجريمة تم استخدامها لشرح مجموعة متنوعة من السلوكيات الإجرامية، يجسد هذا العمل في داخله أربعة مقدمات أساسية تشمل الارتباط التفاضلي والتعريفات والتعزيز التفاضلي والتقليد، وتستند نظرية التعلم الاجتماعي على فكرة أن الأفراد يطورون الدوافع والمهارات لارتكاب الجريمة من خلال الارتباط أو التعرض للآخرين المتورطين في الجريمة (الوريكات، 2013).

يشير التعزيز التفاضلي إلى المكافآت المرتبطة بسلوك إجرامي معين، يتم تعلم هذا السلوك الإجرامي في الأصل من خلال عملية التقليد، والتي تحدث عندما يتعلم الأفراد الأفعال والسلوك من خلال المشاهدة والاستماع إلى الآخرين، لذلك عندما يرتكب الفرد جريمة، فإنه يقلد الأفعال التي شاهد الآخرين ينخرطون فيها (Akers، 1966).

فيما يتعلق بجرائم الإنترنت إن نظرية التعلم الاجتماعي يمكن أن تشرح التطور والمشكلة المستمرة لقرصنة البرامج، في دراستهم لقرصنة البرامج، حيث أن الأفراد الذين يرتبطون بقرصنة البرامج يتعلمون السلوك المنحرف ويقبلونه لاحقًا. تتطلب قرصنة البرامج درجة معينة من المهارات والمعرفة للوصول إليها والأقران المنحرفون لتعلم هذه المهارات في الأصل منهم. علاوة على ذلك، فإن الأفراد المنحرفين يبررون سلوكهم الإجرامي ويساعدون في تعزيز شبكة تربط الأفراد الآخرين وتعلمهم هذه التبريرات والسلوك وبالتالي، يمكن استخدام هذا التفسير لشرح الجرائم الإلكترونية.

ضبط الذات المنخفض

تم تطوير هذه النظرية من قبل علماء الجريمة مايكل جوتفريدسون وترافيس هيرشي، والتي تؤكد أن احتمالية انخراط الأفراد في فعل إجرامي تحدث بسبب وجود الفرصة مع توفر سمة شخصية من سمات الضبط الذاتي المنخفض. وقد عرف العالمان السلوك الطائش بأنه: كل فعل يقوم على الخداع لتحقيق الرغبات الذاتية. فإن السلوك الطائش من مظاهر الضبط الذاتي المنخفض، فالدوافع لارتكاب السلوك الطائش في نظرية الضبط الاجتماعي ليست متغيرة. وذلك لأن كل فرد قد يندفع لتحقيق مصالحه الشخصية بما في ذلك السلوك الطائش الذ يحقق المصالح بسرعة وسهولة دون انتظار أو بذل جهد، فالاختلاف بين الأفراد يعود إلى مستوى ضبط الذات، ووجود الفرصة لارتكاب السلوك المُنحرف (Hirschi & Gottfredson، 1990).

وفي مجال التطبيق النظري على موضوع الدراسة يمكن تطبيق خصائص ضبط النفس المنخفض على بعض الأشكال البسيطة للجرائم الإلكترونية، بما في ذلك قرصنة البرامج، فضعف ضبط النفس ترتبط ارتباطاً مباشراً بقرصنة البرامج، على سبيل المثال، من المرجح أن يقوم الفرد بقرصنة البرامج لأنه مندفع وغير قادر على الانتظار لشراء نسخة من البرنامج، ومن غير المحتمل أن يتعاطف هؤلاء الأفراد مع صاحب حقوق الطبع والنشر ويتجاهلوا أي مسؤولية علاوة على ذلك، فيما ينجذب هؤلاء الأفراد إلى الإثارة وسهولة المشاركة في

قرصنة البرامج، فهم يشاركون أولئك الذين لديهم مستويات منخفضة من ضبط النفس في سلوكهم المنحرف سواء داخل أو خارج الإنترنت بسبب رغبتهم في الإشباع الفوري.

نظرية الحتمية التكنولوجية

يعتبر مارشال ماكلوهان (Marshal Mcluhan) من أهم منظري نظرية الحتمية التكنولوجية، حيث يشير مصطلح الحتمية إلى الجبرية والإلزام الذي يسيطر على سلوك الإنسان الذي يضعف إرادة الإنسان، فالتكنولوجيا تعتبر من العوامل الخارجية للتغير الاجتماعي، فهي تحدد توجهات وتطورات وشكل المجتمع في المستقبل، فوسائل التواصل بشكل عام ووسائل التواصل الاجتماعي كأحد أهم وسائل التواصل في العصر الحالي جعلت العالم قرية واحدة فألغت المسافات وقللت الزمن، وبالتالي فعملت على انكماش الكرة الأرضية، إلا أنها زادت من وعي الإنسان بمسؤولياته والتزامه بمشاركة الآخرين أفكارهم غير المحدودة وأنشطتهم اللامتناهية، وهذا أصابه بالقلق (جمعة، 2017).

فهذه النظرية تعتبر وسائل الاتصال بشكل عام ووسائل التواصل الاجتماعي كأهم وسائل الاتصال في العصر الحديث امتدادا لحواس الإنسان، وقد طبعت الفترة الحالية بطابعها وأخلاقياتها وأنماط التفكير، وأجبرت الإنسان على تقمص تلك الأخلاقيات وأنماط التفكير، فكما مثلت الراديو سابقا حاسة السمع والتلفزيون حاسة البصر، فإن وسائل التواصل الاجتماعي قد مثلت وشكلت جميع الحواس، فيمكن مشاهدة الحدث وسماعه، والإحساس به بالكلمة والصورة، والإحساس اثناء حدوثه، فكل وسيلة تسود في فترة زمنية تشكل أنماط التفكير الاجتماعية، فوسائل التواصل الاجتماعي ومن وجهة نظر هذه النظرية، شكلت قوة أثرت بشكل كبير على تفكير الفرد والأسرة والمجتمع رغما عن إرادتهم، فالجميع يتعرض لرسائل ومحتوى وقيماً اجتماعية أصبحت واحدة، نتيجة التأثر بما ينشر على تلك الوسائل فأصبحت الثقافة عالمية لا يستطيع أي فرد أن يتجنبها (أمين، 2016).

وفي مجال التطبيق النظري على موضوع الدراسة نجد أن وسائل التواصل الاجتماعي فرضت واقعا جديداً على الأسرة الأردنية، وتمثل في تغير قيم المجتمع نتيجة الانفتاح الثقافي، فاستخدام وسائل التواصل الاجتماعي جعلت أفراد المجتمع يشاركون الآخرين أفكارهم وقيمهم، مما يعرضهم إلى محتويات غير مناسبة، فاستخدام وسائل التواصل الاجتماعي بشكل غير مدروس زاد مُعدل الجرائم الإلكترونية، بسبب الآثار السلبية التي فرضتها استخدام وسائل التواصل الاجتماعي.

الدراسات العربية

أجرى (الشبلي، 2019) بحثا بعنوان الجريمة الإلكترونية في سلطنة عمان: التحديات والحلول القانونية، وهدف البحث إلى تحديد مفهوم الجريمة الإلكترونية وخصائصها، ودور التشريع العماني في إيجاد الحلول المناسبة لها، وتوصل البحث إلى أن المشرع العماني استطاع مواكبة التقدم الحضاري من خلال تطوير القوانين التي تكافح الجرائم بصورة عامة، والجرائم الإلكترونية وتقنية المعلومات على وجه الخصوص من خلال منظومة قانونية متكاملة؛ إذ تتراوح تلك العقوبات بين الغرامة المالية والعقوبات السالبة للحرية، وتوصل البحث إلى جملة من التوصيات منها:أهمية القيام بدراسات معتمدة على المسوح الميدانية تتناول أنواع الجرائم الإلكترونية المرتكبة، وأعداد مرتكبيها، ودوافعهم الإجرامية، وجنسياتهم، وفئاتهم العمرية؛ من أجل تطوير القوانين المعمول بها حالياً في سلطنة عمان لتتواكب مع القوانين العالمية الحديثة في ذات المجال، وتوعية المجتمع بخطورة الجرائم الإلكترونية، وأساليب ارتكابها، وتأثيرها الأخلاقي على الفرد والمجتمع، وطرق الوقاية منها.

أجرى (الأطرش وعساف، 2018) دراسة بعنوان: "مُعوقات مُكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية"،وهدفت إلى التعرّف على مُعوقات مُكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية والمتعلقة بكل من (الجريمة المعلوماتية ذاتها والمجني عليه والتحقيق الجنائي)، وتكونت عينة الدراسة من (125) شخص تم اختيارهم بطريقة العينة المتيسرة من مجتمع الدراسة، وأظهرت نتائج الدراسة أن الوسط الحسابي لمُعوقات مُكافحة الجرائم المعلوماتية المتعلقة بالجريمة المعلوماتية بلغ (3.51)، وهي درجة كبيرة، وبلغ الوسط الحسابي لدرجة المُعوقات المتعلقة بالمجني عليه (3.39)، وهي درجة متوسطة، في حين بلغ درجة المُعوقات المتعلقة بالتحقيق الجنائي (3.55)، وهي درجة كبيرة، وأوصت الدراسة بضرورة تدريب وتأهيل العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية، ووضع نظام للحوافز المادية والمعنوية للضباط المتميزين المتخصصين في التحري والكشف عن تلك الجرائم، وضرورة التنسيق بين الأجهزة الأمنية، وإلى أهمية انضمام فلسطين إلى الاتفاقات الدولية الخاصة بمُكافحة الجرائم المعلوماتية، وضرورة إيجاد تحديد تعريف دقيق لتلك الجرائم في القرار بقانون رقم (16) لسنة 2017 بشأن الجرائم المعلوماتية، وتشجيعا لمواطنين على الإبلاغ عن الجرائم المعلوماتية، وضرورة زيادة وعيهم بمخاطر تلك الجرائم.

أجرت (حبيتاني، 2018) دراسة بعنوان: "مُعوقات مُكافحة الجرائم المعلوماتية"، وهدفت الدّراسة إلى الإجابة عن التساؤل التالي: "فيما تتمثل الصعوبات التي تعترض سبل مُكافحة الجريمة المعلوماتية؟"، حيث ركزت على المشكلات القانونية والفنية التي تواجه مُكافحة الجريمة المعلوماتية بشكل عام، ومناقشة المُعوقات القانونية للمشرع الجزائري في مُكافحة تلك الجرائم، وأظهرت الدراسة العديد من المُعوقات التي تعترض سبل مُكافحة الجرائم المعلوماتية، منها ما هو متعلق بالكشف عن الجريمة ونقص خبرة سلطات الاستدلال والتحقيق، بالإضافة إلى تشويه الدليل من قبل الجاني، فيما أوصت الدراسة بضرورة تأهيل رجال الضبطية القضائية على الأساليب التقنية المستخدمة في هذه الجرائم، وضرورة توجيه الجهود الدولية في صياغة قانون موحد لمواجهتها، والحاجة إلى زيادة التعاون الدولي في تسليم المجرمين والتحقيق، وضرورة تأهيل القضاة والمحامين، بالإضافة إلى ضرورة زيادة درجة الوعي لدى مستخدمي الحاسب الآلي والإنترنت.

أجرى (نصيرات، 2015) دراسة بعنوان: "الجهود الدولية في مُكافحة الجرائم المعلوماتية والصعوبات التي تواجهها"، والتي هدفت إلى التعرف عل الجهود المبذولة في مُكافحة الجرائم المعلوماتية، وبيان الصعوبات التي تواجهها وكيفية القضاء على تلك الصعوبات، وقد أظهرت نتائج الدّراسة أنّ تنامي ظاهرة الجرائم المعلوماتية أفرز جملة من التحديات التي تكتنف إثبات هذه الجرائم وقبول الدليل، وتحديد العقبات التي تواجه الأجهزة الأمنية والقضائية في اتخاذ بعض الإجراءات عبر الحدود كالمعاينة والضبط والتفتيش في نطاق البيئة الافتراضية وأوصت بضرورة سعي الدول العربية إلى إنشاء منظمة عربية تعنى في مُكافحة الجرائم المعلوماتية، وضرورة التنسيق بين دول مجلس التعاون الخليجي لمُكافحة تلك الجرائم، والتأكيد على أهمية إجراء دراسات بحثية متخصصة بجرائم تقنية المعلومات.

دراسة (المقصودي، 2015) بعنوان: الجرائم المعلوماتية وكيفية مواجهتها قانونيا: التكامل الدولي المطلوب لمكافحتها، هذه الدراسة ما تتصف به الجريمة المعلوماتية من صفات ميزتها من غيرها من الجرائم التقليدية، فهي تشتمل على جوانب فنية إلكترونية، وتحتوي على مصطلحات ومفردات حديثة مثل: البيانات والبرامج محل الاعتداء الجرمي، كما نلمس أن غالبية موضوعات الجريمة الإلكترونية تكون عبارة عن تسجيلات إلكترونية تتم عرب شبكات الاتصال السيبراني، وقد توصلت الدراسة إلى أن عدم وجود قانون عالمي حديث يجرم التقنيات الفنية الجديدة الناشئة عن استخدام الإنترنت في ارتكاب الجرائم التقليدية أدى إلى اللجوء إلى التفسير القانوني، وهو ما

أثار بعض الإشكاليات في الوصول للتكييف القانوني للفعل المرتكب بشكل دقيق، وأثار كذلك مشكلة التمييز بين العمل التحضيري والبدء في تنفيذ الجريمة وغيرها، وبينت الدراسة أن التعامل مع الدليل في هذا النوع من الجرائم أوجد جمالاً حديثاً في الإثبات، فبعد أن كان جمال الإثبات ينحصر فقط في المستند الورقي أصبح الدليل الرقمي ينازعه في هذه المرتبة، إضافة إلى وجود العديد من الصعوبات العملية في تطبيق الأفكار التقليدية والمستقرة بالقانون الجنائي كمبدأ الشرعية القانونية ومبدأ سريان القانون من حيث الزمان والمكان واختصاص القضاء الوطني دون الأحكام الأجنبية، ووفقاً لكل ما تقدم يتضح لنا خطورة تحديات الجريمة الإلكترونية وضرورة التعاون الدولي لمكافحتها للوصول إلى أفضل السبل القانونية للحد من انتشارها، وبعد ذلك فقدان السيطرة على مرتكبيها في ظل غياب عامل افتراضي واسع المجال.

دراسة (عبد الباقي، 2014) بعنوان: التحقيق في الجريمة الإلكترونية واثباتها في فلسطين: دراسة مقارنة، لتحقيق في الجرائم الإلكترونية وكيفية ضبط الأدلة الرقمية وجمعها من الموضوعات المستجدة في فلسطين وغيرها من دول العالم. كما أن طبيعة الأدلة الرقمية وكيفية التعامل معها من قبل جهات التحقيق تعتبر من الموضوعات ذات الأهمية القانونية والعملية. ويقوم بالتحقيق في الجرائم الالكترونية نيابة متخصصة وفق إجراءات وقواعد إثبات خاصة، يساعدها في ذلك ضابطة قضائية متخصصة بالجرائم الالكترونية، على عكس الجرائم التقليدية التي تختص بالتحقيق فيها النيابة العامة، وفقاً لقواعد التحقيق وخضوعها للضابطة القضائية ذات الاختصاص العام ويعترض عمل النيابة العامة والضابطة القضائية العديد من الصعوبات، من أهمها القصور التشريعي وضعف التخصص لدى القائمين على التحقيق وجمع أدلة هذا النوع من الجرائم، إن تعزيز وتقوية التحقيق في الجرائم الإلكترونية يقوم على وضع مبادئ توجيهية للجهات المختصة بعمليات التحقيق، وذلك لضمان السيطرة على قضايا الجرائم الإلكترونية، إن وضع إجراءات إدارية فعالة على تؤدي إلى تحقيق النجاح المستمر في مُكافحة الجرائم الإلكترونية.

أجرى (الزهراني، 2013) دراسة بعنوان: "تحديات الأمن المعلوماتي في الشبكات الاجتماعية في المملكة العربية السعودية من منظور قانوني"، وهدفت الدراسة الى تحليل أمن المعلومات للمستخدم في الشبكات الاجتماعية وعلاقتها بالأمن الاجتماعي، وما هي مكامن الضعف في التشريع الوطني السعودي التي تؤدي إلى انتهاك الخصوصية الفردية من خِلال نظام مُكافحة الجرائم المعلوماتية، حيث استعرض نقاط الخلل في نظام مُكافحة الجرائم الإلكترونية السعودي الصادر عن وزارة الاتصالات وتقنية المعلومات، وتحديد النقاط التي أغفلتها بعض مواد النظام، وأوصت الدراسة على ضرورة العمل على زيادة الدقة والوضوح في نظام مُكافحة الجرائم الإلكترونية السعودي، وإضافة عدد من الفقرات على النظام، وتدريب العاملين في قطاعات الاتصالات والإنترنت على أخر التطورات الحاصلة في قوانين الإنترنت، وضرورة فتح مكاتب خاصة بشبكات التواصل الاجتماعي، وأن يكون ممثل رسمي يقوم بالتنسيق مع الجهات المعنية في إتباع الأنظمة في المملكة العربية السعودية.

العدد ثلاث وأربعون
تاريخ الإصدار: 2 – أيار – 2022م
www.ajsp.net
ISSN: 2663-5798

الدراسات الأجنبية

دراسة (Holt and Lavorghna, 2021) بعنوان:

Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches

يوفر الكتاب مجموعة حديثة حول إجراء أبحاث الجرائم الإلكترونية، ويسعى هذا الكتاب أيضًا إلى تطوير مصطلحات مشتركة ومنهجية ومعايير أخلاقية للبحث في الجرائم الإلكترونية في جميع أنحاء العالم. من ناحية أخرى، يقدم مجموعة متنوعة من الأمثلة البحثية للجرائم الإلكترونية، من مجموعة دولية من المساهمين. يتحدث الكتاب إلى العاملين في العلوم الاجتماعية والفلسفة التطبيقية وعلوم الكمبيوتر والأخلاق القانونية وما بعدها هدف هذا الكتاب إلى استكشاف مقترحات السياسة للتعامل مع واحدة من أكثر المشاكل تعقيدًا التي تطرحها الإنترنت، وهي مشكلة الاختصاص القضائي. في حين أن الجريمة السيبرانية هي ظاهرة بلا حدود، فإن الملاحقة القضائية الفعالة لهذه الجريمة تعوقها بشكل خطير النزاعات الإقليمية والولاية القضائية. تتفاقم هذه المشاكل بسبب تطور تكنولوجيا المعلومات، ولا سيما الحوسبة السحابية التي تخلق مشاكل "فقدان الموقع" لجمع الأدلة الإلكترونية التي لا غنى عنها لمحاكمة الجرائم.

دراسة (Kops, 2016) بعنوان:

Major trends and major challenges for cybercrime and cyber terrorism policy and research", this study raised the following question

ما هي التحديات الكبرى لسياسة وأبحاث الجرائم الإلكترونية والإرهاب الإلكتروني خلال العقد أو العقدين القادمين؟"، وبينت بأن للإجابة على هذا السؤال، نحتاج أولاً إلى فهم بعض الاتجاهات الرئيسية التي تؤثر على مستقبل الجرائم الإلكترونية والإرهاب الإلكتروني، قامت الدراسة بتجميع الاتجاهات الكبرى في مجموعة اتجاهات تحدثت فيها عن مختلف طبقات الإنترنت: بنيتها التحتية وتطبيقاتها ومحتواها، ومجموعة ثانية نتجت عن الاتجاهات في المجموعة الأولى مرتبطة بالتغيرات في المجتمع ككل، مع تغييرات في كيفية حدوث الجريمة والإرهاب في المجتمع، ومع التغيرات في الجرائم الإلكترونية والإرهاب الإلكتروني وكيفية مكافحتها، وأظهرت النتائج مخطط للتحديات الكبيرة للأبحاث وسياسات الجريمة الإلكترونية والإرهاب الإلكتروني، على خلفية الاتجاهات الكبرى التي لديها القدرة على تغيير المجتمع، بما في ذلك الجريمة والإرهاب، وأوضحت الدراسة في المخطط المرسوم المشهد الذي توجد فيه القضايا الأكثر إلحاحاً التي تحتاج إلى بحث ومعالجة.

دراسة (Hayes, 2015) بعنوان:

Law Enforcement Challenges Related to Cybercrime: Are We Really Playing Catch Up?

وهدفت هذه الدراسة إلى تحليل الادعاءات والخلافات عبر الإنترنت بشأن إنفاذ القانون، والتركيز على كيفية تعريف ورؤية الجهات المعنية بإنفاذ القانون لتحديات الجرائم الإلكترونية، وأظهرت نتائج الدراسة أن الجريمة الإلكترونية تشكل تحديات كبيرة لإنفاذ القانون، فإنها الشاغل الرئيسي للجرائم الإلكترونية لإنفاذ القانون، ووجدت الدراسة أن التحدي الرئيسي أمام إنفاذ القانون هو عدم وجود إطار قانوني فعال للأنشطة التشغيلية التي تضمن مبادئ الحقوق الأساسية المنصوص عليها في القانون الأساسي والثانوي للاتحاد الأوروبي، وتؤكد الدراسة أن الكثير من سياسة الاتحاد الأوروبي بشأن مُكافحة الجرائم الإلكترونية تستند إلى تدابير غير تشريعية بما في ذلك التعاون التشغيلي والشراكات المخصصة بين القطاعين العام والخاص، نظرا لتعقيد البنية التحتية للجرائم الإلكترونية في الاتحاد الأوروبي، وأن البرلمان الأوروبي يُستثنى إلى حد كبير من التطورات السياسية في هذا المجال، مما يعيق التدقيق العام والمساءلة، ويؤدي هذا إلى

تفاقم المشاكل الحالية التي يواجهها البرلمان الأوروبي في ضمان حماية الحقوق الأساسية والبيانات بجدية في مجال العدالة والشؤون الداخلية، وأوصت الدراسة ضرورة أن يطالب البرلمان الأوروبي بمراجعة البنية التحتية للجرائم الإلكترونية في الاتحاد الأوروبي وصلاحياتها، وأنه يجب عليه التأكد من أن التزامات اتفاقية جرائم الإنترنت الخاصة بمركز التميز بين الدول الأعضاء يجب أن تتماشى مع قانون الاتحاد الأوروبي وحماية الحقوق الأساسية.

ما يميز الدراسة الحالية عن الدراسات السابقة:

ومن خلال تتبع الدراسات السابقة يلاحظ أنها لم تتناول موضوع معوقات مُكافحة الجرائم الإلكترونية في المُجتمع الأردني من وجهة نظر ذوي الاختصاص حيث تتفرد الدراسة الحالية بأنها الأولى في الأردن –حسب علم الطالب– وتتميز الدراسة الحالية عن غيرها من الدراسات في سعيها للكشف عن المعوقات (الفنية، القانونية) في مكافحة الجرائم الالكترونية في المجتمع الأردني من وجهة نظر ذوي الاختصاص.

المنهجية والتصميم

يتضمن هذا الفصل وصفاً لمنهج الدراسة واجراءاتها، كما يتضمن توضيحاً لمجتمع وعينة الدراسة وطريقة اختيارها، والأداة المستخدمة، وخطوات بناءها، وطرق التحقق من صدقها وثباتها، ووصف الأساليب الإحصائية التي تم استخدامها في تحليل البيانات بهدف الإجابة عن أسئلة الدراسة.

منهجية الدراسة

انطلاقاً من طبيعة الدراسة والمعلومات المراد الحصول عليها استخدم الباحث المنهج الوصفي، بهدف التعرف على مُعوقات مُكافحة الجرائم الإلكترونية في المُجتمع الأردني من وجهة نظر ذوي الاختصاص، حيث يُعرف المنهج الوصفي بأنه: منهج بحث يستخدم في المجال التربوي من أجل وصف وتفسير ما هو كائن، ودراسة الواقع كما هو، ووصفه وصفاً دقيقاً من خلال التعبير الكمي والكيفي باستخدام الأدوات المناسبة، وتفسير الظواهر، ومحاولة إيجاد العلاقة بين المتغيرات (أبو سمرة والطيطي، 2019).

مجتمع الدراسة وعينتها

ويقصد بمجتمع الدراسة بأنه: مجموعة متكاملة من العناصر أو الأفراد، والتي تجمعها خواص مشتركة يمكن ملاحظتها وقياسها وتحليلها، ويجب أن يكون لكل عنصر من عناصر المجتمع فرصة الظهور في عينة الدراسة (العزاوي، 2008). وفي الدراسة الحالية تكون مجتمع الدراسة من جميع المختصين في مجال الجرائم الإلكترونية في كل من: وحدة الجرائم الإلكترونية في مديرية الأمن العام، المركز الوطني للأمن السيبراني، القضاة المُتخصصين في الجرائم الإلكترونية، الخبراء الفنيين المُعتمدين لدى القضاء النظامي الأردني.

والجدول (1) يوضح اعداد مجتمع الدراسة وفقاً لمجال العمل، والنسبة المئوية لكل مجال.

العدد ثلاث وأربعون
تاريخ الإصدار: 2 – أيار – 2022م
www.ajsp.net
ISSN: 2663-5798

جدول (1)

أعداد والنسب المئوية لمجتمع الدراسة وفقاً لمجال العمل

الرقم	مجال العمل	العدد	النسبة
1	وحدة الجرائم الإلكترونية في مديرية الأمن العام	50	47.2%
2	المركز الوطني للأمن السيبراني	30	28.3%
3	قضاة مُتخصصين في الجرائم الإلكترونية	19	17.9%
4	خبراء فنيين مُعتمدين لدى القضاء النظامي الأردني	7	6.6%
6	المجموع	106	100.0%

صدق وثبات أداة الدراسة

أداة الدراسة

استخدم الباحث الاستبانة كأداة لجمع المعلومات المطلوبة من عينة الدراسة، والاستبيان هو عبارة عن مجموعة من الأسئلة المتنوعة والتي ترتبط ببعضها البعض بشكل يحقق الهدف الذي يسعى إليه الباحث من خلال المشكلة التي يطرحها بحثه، ويتم توجيهه إلى مجموعة من الأفراد أو المؤسسات التي اختارها الباحث كعينة للبحث لكي تتم الإجابة عليها (عطار، 2012).

وهو أيضاً مجموعة من الأسئلة المكتوبة والتي تُعد بقصد الحصول على معلومات أو التعرف على أراء المبحوثين حول ظاهرة أو موقف معين (الضامن، 2007).

وقد تم بناء أداة الدراسة الحالية وفق الخطوات الآتية:

أ. تحديد الهدف من الاستبيان وهو التعرف على مُعوقات مُكافحة الجرائم الإلكترونية في المُجتمع الأردني من وجهة نظر ذوي الاختصاص.

ب. تم ترجمة هدف الاستبانة إلى مجالين أساسيين بحيث أن تتضمنها الاستبانة وهما:

- **المجال الأول:** مُعوقات مُكافحة الجرائم الإلكترونية في المُجتمع الأردني من وجهة نظر ذوي الاختصاص. ويتضمن هذا المجال المُعوقات الفنية، المُعوقات القانونية.

ج. تم الرجوع أيضاً إلى الأدب النظري وبعض الدراسات السابقة التي كانت الجرائم الإلكترونية بشكل عام هدفاً بحثياً لها مثل (المقصودي، 2015) (الأطرش وعساف، 2018) (حبيتاني، 2018)، وذلك للاستفادة منها في بناء عبارات الاستبانة.

د. تم الوصول إلى الصورة الأولية من الاستبانة والتي كانت مكونة من مجالين هما:

- **المجال الأول:** مُعوقات مُكافحة الجرائم الإلكترونية في المُجتمع الأردني من وجهة نظر ذوي الاختصاص. ويتضمن هذا المجال المُعوقات الفنية وتمثله (13) عبارة، المُعوقات القانونية وتمثله (6) عبارات.

هـ. التأكد من صدق وثبات الاستبانة وفق الخطوات الآتية:

1. **الصدق الظاهري للاستبانة:** وهو الصدق المعتمد على آراء المحكمين، والذي يتم من خلاله التحقق من قدرة أداة الدراسة (العبارات والمجالات) على قياس ما صُممت لأجله (عودة، 2005). حيث قام الباحث بعرض الاستبانة بصورتها الأولية على (9) محكمين من الخبراء والمختصين في مجال الجرائم الالكترونية، وتم الطلب منهم دراسة الاستبانة وإبداء آرائهم فيها من حيث: مدى مناسبة العبارات وتحقيقها لأهداف الدراسة، وشموليتها، وتنوع محتواها، ومناسبة كل عبارة للمجال الذي تنتمي له، وتقييم مستوى الصياغة اللغوية، والإخراج، وأية ملاحظات يرونها مناسبة فيما يتعلق بالتعديل، أو التغيير، أو الحذف. وقد قدموا ملاحظات قيمة أفادت الدراسة، وأثرت الاستبانة، وساعدت على إخراجها بصورة جيدة. وبذلك تكون الاستبانة قد حققت ما يسمى بالصدق الظاهري أو المنطقي.
2. **صدق الاتساق الداخلي للاستبانة:** حيث يقصد بصدق الاتساق الداخلي قوة الارتباط بين كل عبارة من العبارات مع المجال الذي تنتمي له، ودرجة ارتباط كل مجال مع الدرجة الكلية للاستبانة (عبد اللطيف، 2006). حيث تم تطبيق الاستبانة على عدد (20) مختصاً من خارج عينة الدراسة، ومن خلال إجاباتهم تم حساب صدق الاتساق الداخلي للاستبانة، وذلك باستخدام:

- معامل ارتباط بيرسون بين درجة كل عبارة والدرجة الكلية للمجال الذي تنتمي له.
- ومن ثم تم حساب معامل الارتباط بيرسون بين درجة كل مجال والدرجة الكلية للاستبانة.

ثبات الاستبانة (Reliability)

ويقصد به أن تعطي الاستبانة نفس النتيجة لو تم إعادة توزيعها أكثر من مرة تحت نفس الظروف والشروط؛ أو بعبارة أخرى أن ثبات الاستبانة يعني الاستقرار في نتائج الاستبانة، وعدم تغيرها بشكل كبير فيما لو تم إعادة توزيعها على أفراد العينة عدة مرات خلال فترات زمنية معينة. (العساف، 2006). وقد تم حساب ثبات الاستبانة وفق الآتي:

- بمعادلة كرونباخ ألفا والجدول (2) يوضح نتائج ذلك.
- بطريقة التجزئة النصفية (سبيرمان براون) والجدول (3) يوضح نتائج ذلك.

جدول (2)

معامل ثبات الاستبانة بمعادلة كرونباخ ألفا

الرقم	المجال	عدد العبارات	كرونباخ ألفا
1	المُعوقات الفنية	13	.979
2	المُعوقات القانونية	6	.930

العدد ثلاث وأربعون
تاريخ الإصدار: 2 – أيار – 2022م
www.ajsp.net
ISSN: 2663-5798

يتضح من الجدول (2) أن نتيجة الثبات بمعادلة كرونباخ ألفا لجميع مجالات الاستبانة، مقبولة إحصائياً، حيث يرى (أبو هاشم، 2003) أن معامل الثبات يعتبر مقبول إحصائياً إذا كانت قيمته أعلى من (0.70)، مما يشير إلى صلاحية الاستبانة للتطبيق على عينة البحث.

جدول (3)

ثبات الاستبانة بطريقة التجزئة النصفية

الرقم	المجال	النصف الأول	النصف الثاني	الكلي	الارتباط بين الجزئيين	سبيرمان براون
1	المُعوقات الفنية	7	6	13	.891	.942
2	المُعوقات القانونية	3	3	6	.860	.925

يتضح من الجدول (3) أن نتائج الثبات بطريقة التجزئة النصفية لجميع مجالات الاستبانة، مقبولة إحصائياً، حيث يرى (أبو هاشم، 2003) أن معامل الثبات يعتبر مقبول إحصائياً إذا كانت قيمته أعلى من (0.70)، مما يشير إلى صلاحية الاستبانة للتطبيق على عينة البحث.

الأساليب الإحصائية المستخدمة

1) استخدم الباحث مقياس ليكرت الخماسي كما هو موضح أدناه:

سلم الإجابة	موافق بشدة	موافق	موافق الى حد ما	غير موافق	غير موافق بشدة
الدرجة	5	4	3	2	1

2) الإحصاء الوصفي المتمثل بالتكرارات والنسب المئوية لوصف عينة الدراسة وفقاً لمتغيرات: (مجال العمل، الجنس، المؤهل العلمي، عدد سنوات الخبرة).

وقد تم تقدير درجة وفق الآتي:

- المدى = أعلى قيمة – أقل قيمة = 5– 1= 4
- طول الفئة = المدى ÷ عدد الفئات = 4 ÷ 5= 0.80

الدرجة	المتوسط الحسابي
ضعيفة جداً	المتوسطات التي تتراوح من 1.00 إلى أقل من 1.80

ضعيفة	المتوسطات التي تتراوح من 1.80 إلى أقل من 2.60
متوسطة	المتوسطات التي تتراوح من 2.60 إلى أقل من 3.40
مرتفعة	المتوسطات التي تتراوح من 3.40 إلى أقل من 4.20
مرتفعة جداً	المتوسطات التي تتراوح من 4.20 إلى 5.00

3) معامل الارتباط بيرسون لحساب صدق الاتساق الداخلي للاستبانة.

4) معادلة كرونباخ ألفا لحساب ثبات الاستبانة.

5) معادلة (سبيرمان براون) لحساب ثبات الاستبانة بطريقة التجزئة النصفية.

6) الإحصاء الوصفي المتمثل بالمتوسط الحسابي والانحراف المعياري للتعرف على:

- المُعوقات الفنية والقانونية لمُكافحة الجرائم الإلكترونية في المُجتمع الأردني من وجهة نظر ذوي الاختصاص.

محددات الدراسة

التزم الباحث في إجراء الدراسة بالمحددات التالية:

- **المحدد الزماني:** أجريت هذه الدراسة الميدانية خلال الربع الأول من العام 2022.

- **المحدد المكاني:** المملكة الأردنية الهاشمية (عمان).

- **المحدد البشري:** اقتصرت هذه الدراسة على جميع المُختصين في مجال الجرائم الإلكترونية في كل من: وحدة الجرائم الإلكترونية في مديرية الأمن العام، المركز الوطني للأمن السيبراني، القضاة المُتخصصين في الجرائم الإلكترونية والخبراء الفنيين المُعتمدين لدى القضاء النظامي الأردني.

عرض النتائج ومناقشتها والتوصيات

يتناول هذا الفصل عرضاً للنتائج التي توصلت إليها الدراسة حول مُعوقات مُكافحة الجرائم الإلكترونية في المجتمع الأردني من وجهة نظر ذوي الاختصاص، وذلك من خلال الإجابة بالترتيب على أسئلتها.

❖ للإجابة عن سؤال الدراسة الفرعي الأول والذي ينص على: ما المُعوقات الفنية في مُكافحة الجرائم الإلكترونية في المُجتمع الأردني من وجهة نظر ذوي الاختصاص؟ تم استخدام المتوسط الحسابي والانحراف المعياري والترتيب وتقدير الدرجة، والجدول (4) يوضح نتائج ذلك.

العدد ثلاث وأربعون
تاريخ الإصدار: 2 – أيار – 2022م
www.ajsp.net
ISSN: 2663-5798

جدول (4)

المتوسط الحسابي والانحراف المعياري والترتيب وتقدير الدرجة للمُعوقات الفنية في مُكافحة الجرائم الالكترونية في المجتمع الأردني من وجهة نظر ذوي الاختصاص

م	العبارة	المتوسط	الانحراف	الترتيب	الدرجة
5	سهولة ابتكار اساليب جديدة لارتكاب الجرائم الالكترونية من قبل المجرمين	4.25	0.803	1	مرتفعة جداً
7	تنوع المجالات التقنية المستخدمة في ارتكاب الجرائم المعلوماتية	4.03	0.842	2	مرتفعة
9	عدم تعاون بعض منصات التواصل الاجتماعي حول تبادل المعلومات مع أجهزة إنفاذ القانون	4.01	0.974	3	مرتفعة
1	سهولة محو الدليل بزمن قصير	3.64	0.931	4	مرتفعة
11	قلة الخبرة الفنية في التعامل مع الكمبيوتر لدى القاضي	3.48	1.102	5	مرتفعة
4	البعد الجغرافي بين مرتكب الجريمة والضحية	3.39	1.217	6	متوسطة
8	قلة البرامج والأدوات التقنية المتخصصة في عملية التحقيق الجنائي	3.33	1.088	7	متوسطة
3	صعوبة توفير حماية أمنية للمعلومات الالكترونية نظراً لضخامتها	3.30	0.906	8	متوسطة
10	صعوبة التعرف على هوية الجاني	3.23	0.981	9	متوسطة
13	صعوبة إثبات ملكية المواقع الإلكترونية عند اتخاذ الإجراءات القانونية	2.94	0.959	10	متوسطة
6	نقص المهارات الفنية بالتحقيق الجنائي في الجرائم الالكترونية	2.84	1.185	11	متوسطة
2	افتقار الجرائم الالكترونية الى الدلائل	2.75	1.073	12	متوسطة
12	صعوبة تحديد نوع الجريمة الإلكترونية	2.65	0.943	13	متوسطة
	المُعوقات الفنية في مُكافحة الجرائم الالكترونية في المجتمع الأردني	3.37	0.491		متوسطة

العدد ثلاث وأربعون
تاريخ الإصدار: 2 – أيار – 2022م
www.ajsp.net
ISSN: 2663-5798

يتضح من الجدول (4) والخاص بالمُعوقات الفنية في مُكافحة الجرائم الالكترونية في المجتمع الأردني من وجهة نظر ذوي الاختصاص ما يلي:

- إن (1) من المُعوقات الفنية جاءت في درجة (مرتفعة جداً) حيث جاء المتوسط الحسابي في فئة التقدير (4.20 إلى 5.00) وهي: سهولة ابتكار اساليب جديدة لارتكاب الجرائم الالكترونية من قبل المجرمين وبمتوسط حسابي (4.25) وانحراف معياري (0.803).
- إن (4) من المُعوقات الفنية جاءت في درجة (مرتفعة) حيث جاء المتوسط الحسابي في فئة التقدير (3.40 إلى أقل من 4.20)، حيث تراوحت المتوسطات الحسابية لها بين (4.03) و (3.48). وبانحرافات معيارية (0.842) و (1.102).
- إن (8) من المُعوقات الفنية جاءت في درجة (متوسطة) حيث جاء المتوسط الحسابي في فئة التقدير (2.60 إلى أقل من 3.40)، حيث تراوحت المتوسطات الحسابية لها بين (3.39) و (2.65). وبانحرافات معيارية (1.217) و (0.943).
- لقد جاءت المُعوقات الفنية في مُكافحة الجرائم الالكترونية في المجتمع الأردني من وجهة نظر ذوي الاختصاص في درجة (متوسطة) وبمتوسط حسابي (3.37)، وبانحراف معياري (0.491).

❖ للإجابة عن سؤال الدراسة الفرعي الثاني والذي ينص على: ما المُعوقات القانونية في مُكافحة الجرائم الإلكترونية في المُجتمع الأردني من وجهة نظر ذوي الاختصاص؟ تم استخدام المتوسط الحسابي والانحراف المعياري والترتيب وتقدير الدرجة، والجدول (5) يوضح نتائج ذلك.

جدول (5)

المتوسط الحسابي والانحراف المعياري والترتيب وتقدير الدرجة للمُعوقات القانونية في مُكافحة الجرائم الالكترونية في المجتمع الأردني من وجهة نظر ذوي الاختصاص

م	العبارة	المتوسط	الانحراف	الترتيب	الدرجة
1	ضعف التعاون الدولي بين البلدان بالإجراءات القانونية لمُكافحة الجرائم الالكترونية	3.70	0.877	1	مرتفعة
4	عدم تغليظ العقوبات القانونية لمرتكبي الجرائم الالكترونية	3.69	1.098	2	مرتفعة
2	عدم اتفاق التشريعات القانونية في بلدان العالم قاطبة على صورة محددة يندرج في إطارها ما يسمى بإساءة استخدام نظم المعلومات الواجب اتباعها	3.66	0.795	3	مرتفعة
5	صعوبة مواكبة القوانين لتطور أساليب ارتكاب الجرائم الالكترونية	3.61	0.864	4	مرتفعة
3	عدم اشتمال منظومة التشريعات الأردنية على مواد تعالج كافة أنواع الجرائم الالكترونية	3.58	0.839	5	مرتفعة
6	مسألة الطبيعية القانونية للمال المعلوماتي ومدى اعتباره مالاً مادياً أو معنوياً	3.49	0.746	6	مرتفعة

العدد ثلاث وأربعون
تاريخ الإصدار: 2 – أيار – 2022م
www.ajsp.net
ISSN: 2663-5798

م	العبارة	المتوسط	الانحراف	الترتيب	الدرجة
	المُعوقات القانونية في مُكافحة الجرائم الالكترونية في المجتمع الأردني	3.62	0.592		مرتفعة

يتضح من الجدول (5) والخاص بالمُعوقات القانونية في مُكافحة الجرائم الالكترونية في المجتمع الأردني من وجهة نظر ذوي الاختصاص ما يلي:

- إن (جميع) المُعوقات القانونية جاءت في درجة (مرتفعة) حيث جاء المتوسط الحسابي في فئة التقدير (3.40 إلى أقل من 4.20)، حيث تراوحت المتوسطات الحسابية لها بين (3.70) و (3.49). وبانحرافات معيارية (0.877) و (0.746).

لقد جاءت المُعوقات القانونية في مُكافحة الجرائم الالكترونية في المجتمع الأردني من وجهة نظر ذوي الاختصاص في درجة (مرتفعة) وبمتوسط حسابي (3.62) وبانحراف معياري (0.592).

مناقشة النتائج:

لقد أظهرت نتائج السؤال الفرعي الأول أن العبارات التي مثلت المُعوقات الفنية لمُكافحة الجرائم الإلكترونية في المُجتمع الأردني من وجهة نظر ذوي الاختصاص قد تراوحت بين المرتفعة جداً والمرتفعة والمتوسطة، حيث كانت أعلى عبارة تشكل تحدياً لذوي الاختصاص هي سهولة ابتكار اساليب جديدة لارتكاب الجرائم الالكترونية من قبل المجرمين، وهذا قد يعود وفق ما يرى الباحث إلى أنه ومن خلال المواقع الإلكترونية أصبح العالم كله ليس كما كنا نقول سابقاً (قرية صغيرة) وإنما أصبح العالم كله موجود في جهاز هاتف أو كمبيوتر محمول، مما اعطى المجرمين فرصة كبيرة جداً لتطوير وتغيير وسائلهم لارتكاب الجرائم الالكترونية بطرق وأساليب جديدة ومبتكرة.

في حين أن مُعوقات أخرى جاءت بدرجة مرتفعة مثل تنوع المجالات التقنية التي يمكن ان يستخدمها المجرمين؛ عدم تعاون بعض المواقع مع الجهات الأمنية للوصول الى الجاني تحت باب خصوصية المستخدم؛ سهولة محو الدليل بزمن قصير، وقلة خبرة القاضي في التعامل مع مثل هذا النوع من الجرائم. ويرى الباحث أن سبب هذه النتائج قد يكون إلى أن عالم الجرائم الالكترونية هو عالم متطور ومتسارع أكثر بكثير من التطوير والتحديث الحاصل على الجهود المبذولة في المجال الميداني والفعلي لمحاربته، وأن السرعة التي يسير بها مرتكبو الجرائم الالكترونية أكبر بكثير من السرعة التي يقوم بها ذوي الاختصاص بتطوير مهاراتهم وقدراتهم على التعامل مع مثل هذا النوع من الجرائم.

كما أن مُعوقات أخرى جاءت بدرجة متوسطة مثل البعد الجغرافي بين مرتكب الجريمة والضحية؛ قلة البرامج والأدوات التقنية المتخصصة في عملية التحقيق الجنائي؛ صعوبة توفير حماية أمنية للمعلومات الالكترونية نظراً لضخامتها؛ صعوبة التعرف على هوية الجاني؛ صعوبة إثبات ملكية المواقع الإلكترونية عند اتخاذ الإجراءات القانونية؛ نقص المهارات الفنية بالتحقيق الجنائي في الجرائم الالكترونية؛ افتقار الجرائم الالكترونية الى الدلائل؛ صعوبة تحديد نوع الجريمة الإلكترونية. ويرى الباحث أن هذه النتائج الخاصة بهذه العبارات تشير لوجود درجة لا بأس فيها من الكفاءة عند ذوي الاختصاص في التعامل مع الجرائم الالكترونية، سواء كان ذلك بسبب التدريب الفني الذي يخضعوا له حول كيفية التعامل مع مثل هذه الجرائم، أو بسبب الخبرات التراكمية الميدانية التي يتم اكتسابها من خلال التعامل مع

كل جريمة، أو بسبب حسن الاختيار من البداية للأفراد العاملين في مجال محاربة الجرائم الالكترونية، بحيث أن هذا الاختيار يكون وفق أسس ومعايير وكفاءات محددة تجعل من هذا المختص قادراً على التعامل مع مثل هذه المُعوقات بكفاءة.

لقد أظهرت نتائج السؤال الفرعي الثاني أن جميع العبارات التي مثلت المُعوقات القانونية لمُكافحة الجرائم الإلكترونية في المُجتمع الأردني من وجهة نظر ذوي الاختصاص قد جاءت بدرجة مرتفعة، وهي مرتبةً كما يلي: ضعف التعاون الدولي بين البلدان بالإجراءات القانونية لمُكافحة الجرائم الالكترونية. عدم تغليظ العقوبات القانونية لمرتكبي الجرائم الالكترونية. عدم اتفاق التشريعات القانونية في بلدان العالم قاطبة على صورة محددة يندرج في إطارها ما يسمى بإساءة استخدام نظم المعلومات الواجب اتباعها. صعوبة مواكبة القوانين لتطور أساليب ارتكاب الجرائم الالكترونية. عدم اشتمال منظومة التشريعات الأردنية على مواد تعالج كافة أنواع الجرائم الالكترونية. مسألة الطبيعية القانونية للمال المعلوماتي ومدى اعتباره مالاً مادياً أو معنوياً، ويرى الباحث أن هذه النتائج قد تعود إلى أن التشريعات القانونية التي تحكم الجرائم الإلكترونية سواء على المستوى الوطني أو على المستوى الدولي لا زالت بحاجة إلى المزيد من الدراسة والتحديث والتأطير بما يجعلها قادرة على التعامل مع كافة أنواع وصور الجرائم الالكترونية، حيث أن الحد من الجرائم الالكترونية لا يمكن أن يتحقق على الوجه المطلوب من دون وجود توافق وإجماع دولي على محاربة هذا النوع من الجرائم والتي تهدد الأمن المجتمعي سواء كان ذلك على مستوى الأفراد أو على مستوى المؤسسات والشركات وصولاً للحكومات.

التوصيات:

استناداً إلى أهم النتائج المتعلقة بمُعوقات مُكافحة الجرائم الإلكترونية في المجتمع الأردني من وجهة نظر ذوي الاختصاص، فإن الدراسة توصي بما يلي:

1- تنمية الوعي المجتمعي حول الجرائم الالكترونية وبكافة الوسائل الإعلامية، بحيث أن تشمل هذه التنمية للوعي جانبين الأول التوعية بكيفية حماية البيانات والمعلومات بحيث ألا يكون الفرد أو المؤسسة أحد المستهدفين لهذه الجرائم، والجانب الثاني التوعية بالعقوبات التي تنتظر كل من يفكر ليكون هو الجاني، بحيث أن يُدرك الجاني بأنه ليس ببعيد عن القبضة الأمنية، وأنه يمكن الوصول له بوقت قصير نسبياً

2- العمل على تنظيم مؤتمرات دولية يجتمع فيها ذوي الاختصاص من كل الدول، بحيث يتم من خلالها توحيد وتأطير اللوائح والتشريعات القانونية التي يمكن من خلالها وضع الأدوات القانونية والإجرائية والتنظيمية لمُكافحة الجرائم الالكترونية على المستوى الدولي أو الوطني .

3- عقد دورات تدريبية محلية ودولية لذوي الاختصاص العاملين في مجال مُكافحة الجرائم الالكترونية، بحيث أن تعمل هذه الدورات على صقل مهاراتهم وقدراتهم في التعامل مع الجرائم الالكترونية بكفاءة عالية .

4- تقديم الدعم المادي للجهات المسؤولة عن مُكافحة الجرائم الالكترونية، والعمل على رفع المخصصات المالية المقدرة لهم، بما يمكنهم هذا الدعم المادي من تطوير وتحديث الأنظمة، وشراء الأجهزة والمعدات اللازمة في عملهم لمُكافحة الجرائم الالكترونية.

5- العمل على نشر ملابسات الجرائم الالكترونية التي يتم اكتشافها من قبل ذوي الاختصاص في مُكافحة الجرائم الالكترونية، مع نشر الأحكام القضائية التي تم النطق بها بحق الجناة في هذه الجرائم الالكترونية، بحيث أن يكون هذا النشر شكل من أشكال التوعية لأفراد المجتمع حول طبيعة وخطورة وعواقب الجرائم الالكترونية .

6- العمل على الاتفاق مع الشركات المزودة لخدمات الانترنت، وهيئة الاتصالات وتقنية المعلومات في الأردن على وضع ضوابط للاشتراك في خدمات الانترنت بشكل عام ومواقع التواصل الاجتماعي بما يُصعب ارتكاب للجرائم الالكترونية على الجناة ويجعل الوصول لهم أكثر سهولة .

7- نشر تحديث دوري حول الجرائم الالكترونية الأكثر انتشاراً في المجتمع الأردني على مختلف وسائل الإعلام، وكيف يمكن لكل فرد أو مؤسسة أن يتجنب أن يكون هدفاً لهذه الجرائم .

8- تحديث وتطوير منظومة التشريعات الأردنية التي تعالج كافة أنواع الجرائم الالكترونية، لا سيما وأن القضاة المتخصصين عينة الدراسة الحالية بالذات اتفقوا على عدم اشتمال منظومة التشريعات الأردنية على مواد تعالج كافة أنواع الجرائم الالكترونية بمتوسط حسابي (3.07) وبأهمية نسبية .(61.4%)

9- الاهتمام بصقل وتطوير الخبرة الفنية للقضاة بالتحديد في مجال تقنية المعلومات والتعامل مع الكمبيوتر والمواقع الالكترونية ومواقع التواصل الاجتماعي، بما سوف يساعدهم ذلك على فهم الكثير من التفاصيل المتعلقة بالجرائم الالكترونية اثناء دراستها لغاية النطق بالأحكام الخاصة بها.

قائمة المراجع

المراجع العربية

مناعسة، أسامة وجلال محمد (2001). صايل فاضل الهواوشة، جرائم الحاسب الآلي والانترنت، ط 0، دار وائل للنشر، الأردن.

الشحات، حاتم عبد الرحمن (2002). الإجرام المعلوماتي، دار النهضة العربية، القاهرة، ط1، بحث بعنوان التعاون الأمني في مُكافحة الجريمة المنظمة.

عبابنة، محمود أحمد (2004). جرائم الحاسوب وابعادها الدولية، دار الثقافة والنشر والتوزيع.

بوادي، حسين المحمدي (2006). إرهاب الإنترنت، الخطر القادم، الطبعة الأولى، دار الفكر الجامعي، القاهرة.

السالمي، علاء عبد الرزاق (2002). تكنولوجيا المعلومات، دار المناهج للنشر والتوزيع، عمان، الأردن.

موسى مسعود أرحومة (2009). الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس.

الجمعية العامة للأمم المتحدة (2019). مُكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، تقرير الأمين العام، الدورة الرابعة والسبعون البند ١٠٩ من جدول الأعمال المؤقت.

حجازي، مصطفى (2006). الجوانب النفسية لجرائم الانترنت، دار الفكر الجامعي، ط1.

لحسن، سامي (2008). الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي.

رمضان، إبراهيم (2015). الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية: دراسة تحليلية تطبيقية، كلية الشريعة والقانون بطنطا.

خليفة، محمد (2016). خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها، المجلة العربية للأبحاث في العلوم الإنسانية والاجتماعية، العدد 25.

البداينة، ذياب، الطراونة، أخليف، والعثمان، حسين، وأبو حسان ريم (2009). عوامل الخطورة في البيئة الجامعية لدى الشباب الجامعي في الأردن. المجلس الأعلى للشباب: مركز إعداد القيادات الشبابية.

المقصودي، محمد بن أحمد (2015). الجرائم المعلوماتية وكيفية مواجهتها قانونياً: التكامل الدولي المطلوب لمكافحتها، جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسب والمعلومات.

باطلي، غنية (2013). جامعة طاهري محمد بشار، مخبر الدراسات الصحراوية، العدد 4.

حامد، هدى (2019). جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة.

سعدات، محمود (2015). خصائص الجرائم المعلوماتية وصفات مرتكبيها في ظل مجتمع المعلوماتية، المؤتمر الدولي الأول لمُكافحة الجرائم المعلوماتية، جامعة الإمام محمد بن سعود الإسلامية – كلية علوم الحاسب والمعلومات.

المهدي، حاتم (2018). خصائص الجريمة المعلوماتية، عبد الفتاح الزيتوني، العدد 3.

الوريكات، عايد عواد (2013). نظريات علم الجريمة، الطبعة الأولى. دار وائل للنشر والتوزيع، عمان: الأردن.

جمعة، معاوية. (2017). أثر وسائل التواصل الاجتماعي على العلاقات الأسرية (الفيس بوك والواتساب نموذجا): دراسة حالة ولاية الخرطوم–محلية أمبدة–وحدة الأمير. رسالة ماجستير غير منشورة، جامعة النيلين، الخرطوم، السودان.

أمين، رضا. (2016). تأثير مواقع التواصل الاجتماعي على العلاقات الاجتماعية: دراسة ميدانية في ضوء نظريتي الحتمية التكنولوجية والقيمية. المجلة العلمية لبحوث العلاقات العامة والاعلان / جامعة القاهرة.

الشبلي، عبد الله (2019). الجريمة الإلكترونية في سلطنة عمان: التحديات والحلول القانونية، مجلة العلوم الاقتصادية والإدارية والقانونية، مجلد 3، عدد 2.

الأطرش عصام، وعساف محمد (2018). مُعوقات مُكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية، مجلة جامعة الشارقة، المجلد 16، العدد 1.

نصيرات، وائل (2015). الجهود الدولية في مُكافحة الجرائم المعلوماتية والصعوبات التي تواجهها، المؤتمر الدولي الأول لمُكافحة الجرائم المعلوماتية، جامعة الإمام محمد بن سعود الإسلامية – كلية علوم الحاسب والمعلومات.

حبياتني، بثينة (2018). مُعوقات مُكافحة الجريمة المعلوماتية، مجلة العلوم الإنسانية العدد 50.

عبد الباقي، مصطفى (2014). التحقيق في الجريمة الإلكترونية واثباتها في فلسطين، مجلة علوم الشريعة والقانون، المجلد 45، العدد 4، ملحق 2.

الزهراني، يحيى (2013). تحديات الأمن المعلوماتي في الشبكات الاجتماعية في المملكة العربية السعودية من منظور قانوني، المجلة العربية الدولية للمعلوماتية، مجلد 2، عدد 3.

أبو سمرة، محمود؛ الطيطي، محمد (2019). مناهج البحث العلمي من التبيين إلى التمكين. عمان: دار اليازوري العلمية للنشر والتوزيع.

العزاوي، رحيم (2008). منهج البحث العلمي، دار دجلة للنشر والتوزيع، عمان، الأردن.

عطار، طلال محمد نور (2012). المدخل إلى البحث العلمي. أسامة للنشر والتوزيع، عمان، الأردن.

الضامن، منذر (2007). أساسيات البحث العلمي. دار المسرة، عمان، الاردن.

عودة، أحمد (2005). القياس والتقويم في العملية التدريسية، دار الأمل للنشر والتوزيع، عمان، الأردن.

عبد اللطيف، فاتن (2006). أصول البحث العلمي الحديث، مركز الإسكندرية للكتاب، الإسكندرية، مصر.

العساف. صالح (2006). المدخل إلى البحث في العلوم السلوكية، مكتبة العبيكان، السعودية، الطبعة 4.

أبو هاشم. السيد محمد أبو هاشم (2003). الدليل الاحصائي في تحليل البيانات باستخدام SPSS، مكتبة الرشد. السعودية، الرياض.

المراجع الأجنبية:

Burgess, R.; Akers, R.; (1966). "Differential Association Strengthening Theory of Criminal Behavior". social problems. 14 (2): 128-147. doi: 10.2307/798612. JSTOR 798612.

Gottfredson, M. R. and Hirschi, T. (1990). A General Theory of Crime, California: Stanford University Press.

Lavorgna Anita, and J. Holt Thomas (2021). Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches, Springer link, ISBN: 978-3-030-74837-1.

Nir, Kops (2016). Major trends and major challenges for cybercrime and cyber terrorism policy and research, JSTOR Journal, Vol. 31, No. 7.

Hayes, Ben (2015). The Law Enforcement Challenges of Cybercrime: Are We Really Playing Catch-Up? A discussion Paper submitted at the Think Tank Conference , European Parliament.

العدد ثلاث وأربعون
تاريخ الإصدار: 2 – أيار – 2022م
www.ajsp.net
ISSN: 2663-5798

"Obstacles to Combating Cybercrime in Jordanian Society from the point of view of Specialists"

Researcher:
Oday Mohammad Alshawabkeh

Mutah University, 2022

Abstract:

The study aimed to identify the technical, legal and social obstacles to combating cybercrime in the Jordanian society from the point of view of the specialists. Specialists in cybercrime, technical experts accredited to the Jordanian regular judiciary, all of whom are (106) specialists. While the exploratory study sample consisted of (20) specialists, and the basic sample of (80) specialists.

The results of the study resulted in the following: Legal obstacles came to a degree (high and ranked first), and technical obstacles were at a degree (medium and ranked second). Based on the results of the study, the researcher recommended the need to develop societal awareness about cybercrime and in all media. Organizing international conferences in which specialists gather with the aim of agreeing and developing legal regulations and legislation related to combating cybercrime at the international and national level. In addition to the necessity of holding local and international training courses for specialists working in the field of combating cybercrime, so that these courses work to refine their skills and abilities in dealing with cybercrime with high efficiency.

Keywords: Obstacles, Eombating, Cybercrime, Specialists.