Al-Adab Journal Vol. 68, No. 2, Supplement (June 2026)
E-ISSN: 2706-9931 P-ISSN: 1994-473X

Challenges of Achieving Justice in Combating Cybercrimes in the Digital Age and Proposed Solutions from the Perspective of Security Personnel

Eman Abdulla Saeed ALNaour ALNaqbi
Ph.D. in Applied Sociology, specialization (Applied Sociology)
University of Sharjah - College of Arts, Humanities and Social Sciences
al.emaaan22@gmail.com

DOI: https://doi.org/10.31973/r7gp2813

Abstract:

The study aimed to identify the challenges of achieving justice in addressing cybercrimes in the digital age and the proposed solutions from the perspective of security personnel. The descriptive-analytical approach was followed, with a questionnaire applied to a random sample of (25) security personnel in Emirate of Sharjah in United Arab Emirates. After collecting and analyzing the data, the study concluded that the level of challenges hindering justice in confronting cybercrimes in the digital age was significant, with an average of (3.836) This indicates the presence of many and varied obstacles. The results also showed that the importance of the proposed solutions to achieve justice in the digital age was high, with an average of (3.861) indicating the importance of following up on the implementation of the proposed solutions. The study recommended the necessity of raising community awareness about criminal risks, training human resources to face challenges, and creating laws and regulations to prevent cybercrime and achieve justice worldwide.

Keywords: Justice challenges – confronting cybercrimes – digital age – security personnel

***The authors has signed the consent form and ethical approval**

Al-Adab Journal Vol. 68, No. 2, Supplement (June 2026)
E-ISSN: 2706-9931 P-ISSN: 1994-473X

تحديات عدالة مواجهة الجرائم الالكترونية في العصر الرقمي والحلول المقترحة من وجهة نظر رجال الأمن

د. إيمان عبدالله سعيد الناعور النقبي
دكتوراه الفلسفة علم الاجتماع التطبيقي
تخصص (علم الاجتماع التطبيقي)
جامعة الشارقة– كلية الآداب والعلوم الإنسانية والاجتماعية

(مُلَخَّصُ البَحث)

هدفت الدراسة إلى الكشف عن تحديات عدالة مواجهة الجرائم الإلكترونية في العصر الرقمي والحلول المقترحة من وجهة نظر رجال الأمن، وقد تم اتباع المنهج الوصفي التحليلي، بتطبيق استبيان على عينة عشوائية في إمارة الشارقة بدولة الإمارات العربية المتحدة بعدد(٢٥) فرد من رجال الأمن، وبعد جمع البيانات وتحليلها توصلت الدراسة إلى النتائج: بلغ مستوى وجود تحديات تعيق عدالة مواجهة الجرائم الإلكترونية في العصر الرقمي بدرجة (كبيرة) وبمتوسط(٣.٨٣٦)، وهذا يدل على وجود معيقات كثيرة ومتنوعة، كما بينت النتائج مستوى أهمية الحلول المقترحة لتحقيق العدالة في العصر الرقمي بدرجة(كبيرة) وبمتوسط(٣.٨٦١) وهذا يدل على أهمية متابعة تنفيذ الحلول المقترحة، وأوصت بضرورة التوعية المجتمعية بالمخاطر الإجرامية وتدريب الكادر البشري لمواجه التحديات وايجاد قوانين وتشريعات لمنع الجريمة الإلكترونية وتحقيق العدالة في كل أنحاء العالم.

الكلمات المفتاحية: تحديات عدالة – مواجهة الجرائم الإلكترونية – العصر الرقمي – رجال الأمن

*** وقع المؤلفون على نموذج الموافقة والموافقة الأخلاقية الخاصة بالمساهمة البشرية في البحث**

مقدمـــــة:

شهد العالم خلال العقود الأخيرة تطوراً علمياً كبيراً خاصة في تقنية التكنولوجيا التي غزت كافة نواحي الحياة وأصبح لدى كافة المؤسسات والأفراد وسائل الكترونية متنوعة مع توفر كافة المعلومات التي يحتاجها الأفراد للتعامل معها، مما جعل البعض يستغل هذه الوسائل في أعمال سلبية غير مقبولة تتنافى مع القيم والأخلاق وتصل بعضها إلى جرائم الكترونية تصنف حسب أهدافها ومستواها كجرائم القرصنة والنصب والاحتيال والابتزاز والتشويه وقد تمس الأمن العام والسلم الاجتماعي وغيرها.

ومع انتشار هذه الوسائل الحديثة للتكنولوجيا بين افراد المجتمعات وشيوع استخدامها، أضحى لدى كل فرد القدرة على التفاعل والتواصل دون مانع من حدود أو جغرافيا، وذلك مع توافر القدرة على نقل وتلقي المعلومات والتقنيات والاضطلاع على البيانات والبرامج بكل سهولة و يُسر ، ومع وجود الحسنات والفوائد الجمة التي رافقت ظهور هذه المكونات الجديدة والمتطورة من العلوم والمعرفة والتقنية، إلا أن ذلك قد ترافق مع مشكلات وسلبيات ظهرت على شكل جرائم يقترفها بعض مستخدمي التكنولوجيا والتي تتصف بخطورتها وسهولة ارتكابها ومعضلة عبورها للحدود الوطنية، ويطلق عليها الجرائم الإلكترونية (كاظم،٢٠١٨ ، ص.٤٠).

فضلا عن امتداد شبكة الإنترنت لتشمل البحث العلمي والمعاملات التجارية والتواصلات الاجتماعية، مما زاد من ظهور الجرائم الإلكترونية على الشبكة بصورها وأشكالها المتنوعة، حيث تسمح شبكة الإنترنت بظهورها بعيداً عن أعين الجهات الأمنية، يقترفها مجرمون أذكياء يمتلكون قدرة المعرفة الفنية والتقنية، وقد تمس الحياة الخاصة للأفراد وتهدد الأعمال التجارية بخسائر فادحة كما تنال من الأمن القومي والسيادة مما جعل الإنترنت نموذجاً صارخاً للإجرام فيه ثغرات قانونية تتحدى الأجهزة الأمنية والقضائية. (الكعبي، ٢٠٢٠)

ولتحديد مفهوم الجريمة الالكترونية ذكر خالد، أن للجريمة الالكترونية تعريفات مختلفة ومتنوعة، لتنوع الأبحاث والدراسات التي تتعلق بها ، فهناك من يطلق عليها اسم جرائم الحاسبات، أو إساءة استخدام الحاسب، أو الجرائم المرتبطة أو المتعلقة بالحاسبات، أو جرائم المعالجة الآلية للبيانات أو جرائم التكنولوجيا الحديثة والسيبرانية أو جرائم المعلوماتية. (لطفي، ٢٠١٩، ص. ٢٥)

وقد أثبتت نتائج دراسة كل من : (معتوق٢٠٢١، وكاظم٢٠١٨، حسين وبهاء الدين(د.ت) أن الأغلبية يتعرضون لجرائم الكترونية ممن يستخدمون المواقع التعليمية ويليها المواقع الخاصة بتحميل الأفلام والألبومات الغنائية، والرياضية والتجارية وأثناء قيامهم بهذا يتعرضون للجرائم الالكترونية من نصب وتزوير وتشويه وتحرشات وتخريب بيانات وغيرها.

كما أكد إبراهيم، على أن الجرائم الالكترونية قد تمس الحياة الخاصة للأفراد وتهدد الأعمال التجارية بخسائر فادحة، كما تنال من الأمن القومي والسيادة. (إبراهيم، ٢٠٠٨، ص.٧)

ومما لفت نظر الباحثة بعد اطلاعها على الواقع المعاش ومما يتم نشره تبين لها أن مجتمع إمارة الشارقة أحد المجتمعات المتضررة من شيوع الجرائم الالكترونية بصورة سريعة تتسع يومياً، وعليه فلا بد من قيام الجهات ذات العلاقة بالتصدي لهذه الجرائم من خلال وسائل الدفاع الاجتماعي المتعددة والتي من ضمنها وضع تشريعات الحماية القانونية والتي تعتبر أهم وسائل المجتمع في الحفاظ على قيمه وحماية مصالحه، وعلى الرغم من التحرك في هذا الجانب إلا أنه لا زال هنالك تحديات كثيرة توجب التصدي لها كالقصور في نشر ثقافة التحذير من الجرائم ونشر أساليب التصدي لها بالإضافة إلى أطر الحماية من الناحية القانونية والتشريعات، وعليه فقد حاولت الباحثة الوقوف على هذا الموضوع لتوضيح أهمية الإسراع في توفير الأطر القانونية السليمة والمرجعيات الإجرائية الواضحة لمكافحة هذا النوع الخطير من الجرائم وحماية المجتمع من جميع النواحي الاقتصادية والثقافية والأمنية، وفتح مجال التوسع في الدراسات لكشف عناصر الجريمة وأنواعها وايجاد حلول للحد منها ومنع حدوثها في مجتمعنا، وما هذه الدراسة إلا محاولة لتحديد التحديات التي تعيق عدالة التصدي للجريمة الإلكترونية وتقديم حلول ومقترحات لتحقيق هذه العدالة من أجل منع ظهور وتكرار الجريمة الإلكترونية.

مصطلحات الدراسة: تتحدد مصطلحات الدراسة في المفاهيم الآتية:

(١)تحديات عدالة مواجهة الجرائم الإلكترونية:

التعريف الإجرائي: هي الصعوبات التشريعية والقانونية التي تشكل عائق أمام تحقيق العدالة على كل من يرتكب جريمة إلكترونية من الجرائم العابرة للحدود والغير مراقبة أمنيا وتشكل خطرا على الأفراد والدول والسلم والأمن القومي والاجتماعي.

(٢)مفهوم الجرائم الإلكترونية:

تعريف الجرائم الإلكترونية بأنها "مجمل الجرائم المرتكبة باستعمال المعلوماتية أو الشبكات المعلوماتية، وتكون هذه الجرائم ذات طبيعة متعددة، ويمكن أن تأخذ شكل الإجرام التقليدي باستعمال الوسائل التقنية للشبكات". (مي العبد الله، ٢٠١٤، ص. ١٣٩)

وتُعرف الجريمة الإلكترونية على أنها "كل فعل يتسبب بضرر جسيم للأفراد أو الجماعات والمؤسسات، بهدف ابتزاز الضحية وتشويه سمعتها من أجل تحقيق مكاسب مادية أو خدمة أهداف سياسية باستخدام الحاسوب ووسائل الاتصال الحديثة مثل الإنترنت". الاسترجاع من الموقع(https://draya-eg.org/٢٠٢٢/٠٤/١٣).

ويمكن تعريف الجرائم الالكترونية إجرائياً بأنها: كل الأعمال غير القانونية التي يمارسها أشخاص محترفين باستخدام الأنظمة المحوسبة بحيث تلحق الضرر بالفرد والمجتمع وتتم عبر شبكة الانترنت وتكون غير أخلاقية منافية للسلوك الحسن كتدمير البرامج والبيانات وسرقة المعلومات والقرصنة ونشر الفيروسات والتشويه والتحريض واختراق الأنظمة الاقتصادية والأمنية وغيرها من الأعمال المنافية للعقل والأخلاق.

(٣)الحلول المقترحة من وجهة نظر رجال الأمن:

التعريف الإجرائي: هي الأطر التشريعية والنصوص القانونية التي تضمن للأفراد والمؤسسات والمجتمعات الأمن والسلامة من خلال من ارتكاب الجرائم الالكترونية وتأمين البرامج والمعلومات ومراقبة القرصنة وغيرها من الانتهاكات التقنية وانزال العقوبة بحق من يرتكب أي نوع من هذه الجرائم.

أولاً: مشكلة الدراسة :

تبرز ظاهرة الجريمة الالكترونية في العصر الحديث بتطورها الملحوظ خاصة مع توسع انتشار الحاسبات وشبكات الأنترنت ونظم المعلومات حتى باتت تؤرق الأفراد والمجتمعات، حيث اصبحت تمس الحياة الخاصة للأفراد والجماعات وتهدد الاقتصاد، كما تحاول النيل من الأمن القومي والسيادة الوطنية، وتمويل الارهاب بالعملات الافتراضية عبر الفضاء السيبراني. (صالح ، ٢٠٢١) ، كما أن لها مخاطر حددها (معروف، ٢٠١٩) بقضايا الملكية الفكرية وحقوق التأليف والنشر حيث تهدد أمن البيانات والمعلومات من قبل مستخدمي الشبكة متمثلة في: سرقة المعلومات وانتهاك خصوصية الأفراد وتعرض البحوث العلمية للسرقة وتزوير الشهادات العلمية وانتحال صفة أشخاص آخرون واخيراً تعرض اجهزة الكمبيوتر والبرامج المحملة عليها من قبل القراصنة، وخاصةً المعاملات التجارية والبطاقات الائتمانية التي أصبحت أكثر اختراق من قبل القراصنة، وهذا ما أكدته دراسة (البيوك ، ٢٠٢١) ومن المخاطر ظهور شبكات دولية تقوم بجرائم منافية للقيم الأخلاقية، واصبحت المواقع الالكترونية ومواقع التواصل الاجتماعي على شبكة الانترنت ملوثة بارتكاب جرائم الكترونية، منها (الكذب والغش ، اعطاء معلومات غير صحيحة ، التجسس والسرقة والنصب ، والاعتداء على الخصوصية ، والتهديد الابتزاز، التعامل مع الصور الخليعة ، ادمان التعامل مع الانترنت) وقد يتم ذلك من خلال إعداد المجرم لبريد الكتروني مغلوط

(الحبسي ، ٢٠٢١) ، وأكد معروف(٢٠١٩) على أن المخاطر الناجمة عن الجرائم المعلوماتية تجاوزت الأفراد والجماعات ليصل تأثيرها على الدول والحكومات وأكبر المؤسسات العالمية، وذلك يمنح مرتكبي الجرائم عبر الإنترنت من استغلال الثغرات الأمنية للوصول إلى أنظمة الحوسبة ونشر البرامج الضارة عليه، وهذا ما اشارت إليه دراسةJackson, Jennifer T ، ٢٠١٧)) ، وتبرز الفجوة بين استخدام التكنولوجيا في الحصول علي المعرفة والاستخدام الامثل والفعال والأخلاقي وبين مخاطرها، خاصة مع وجود تحديات كثيرة تواجه العدالة في التقاضي من مرتكبي تلك الجرائم، ولا يمكن حماية المصالح الجوهرية في حياة أفراد المجتمع؛ إلا من خلال إسدال ستار الحماية الجنائية وتطبيق العدالة على كل الحقول الإلكترونية والحاسوب والإنترنت والاختراقات، وعليه يمكن طرح مشكلة البحث في التساؤلات الآتية:

١- ما التحديات التي تعيق عدالة مواجهة الجرائم الإلكترونية في العصر الرقمي من وجهة نظر رجال الأمن؟

٢- ما الحلول المقترحة لتحقيق عدالة مواجهة الجرائم الإلكترونية في العصر الرقمي من وجهة نظر رجال الأمن؟

ثانياً: أهمية الدراسة :

١- التوجه العالمي للاهتمام بالجرائم الالكترونية التي تمس حياة وقيم ومصالح كاف الأفراد والجماعات مما يستوجب دراسته وتنمية الوعي بمخاطرة.

٢- هناك حاجة ماسة للدراسات والبحوث التي تهتم بتنمية الوعي بالجرائم الالكترونية كأحد القضايا الحديثة لدى كافة أفراد مجتمع الشارقة.

٣- تزويد الأفراد بمفهوم الجريمة الالكترونية ومخاطرها يعد أمراً مهماً لفهمه في كل المراحل التعليمية.

٤- وضع مقترحات وحلول للحد من هذه الجرائم في مجتمعنا من خلال مواجهة زيادة الجرائم الالكترونية بتحقيق العدل.

ثالثاً: أهداف الدراسة: تتمثل أهدف للدراسة في الآتي :

١- تحديد التحديات التي تعيق عدالة مواجهة الجرائم الالكترونية في العصر الرقمي.

٢- اقتراح حلول لتحقيق عدالة مواجهة الجرائم الالكترونية في العصر الرقمي.

رابعاً: حدود الدراسة:

الحدود الزمنية: تم تنفيذ البحث في مطلع العام ١٤٤٦هـ/ ٢٠٢٥م

الحدود المكانية: إمارة الشارقة.

الحدود الموضوعية: تمثلت في التحديات والحلول المقترحة لعدالة الجرائم الالكترونية في العصر الرقمي.

الحد البشري : تمثلت بعينة من رجال الأمن في مدينة الشارقة.

الاطار النظري والدراسات السابقة

أولاً : الاطار النظري :

تكون الاطار النظري من مبحثين على النحو التالي:

المبحث الأول : الجريمة الالكترونية وتطوراتها.

المبحث الثاني : تحديات عدالة مواجهة الجرائم الالكترونية والحلول المقترحة.

وقد تم استعراضهما على النحو الآتي:

المبحث الأول : الجريمة الالكترونية وتطوراتها:

المطلب الأول: مفهوم الجريمة الالكترونية:

لقد تعددت التعريفات التي تناولت الجريمة الالكترونية، ويرجع ذلك إلى اختلاف وجهات النظر بين الأفراد والمجتمعات حول نوع وطبيعة وأهداف وأساليب هذه الجرائم ، فمع انفجار ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى إلكترونية، قد يصعب التعامل معها، لأن الجريمة الالكترونية هي من الظواهر الحديثة وذلك لارتباطها بتكنولوجيا المعلومات والاتصالات الحديثة وشبكة الأنترنت.

وتُعرف الجريمة من منظور الفكرة الاجتماعية بأنها: كل فعل يتعارض مع ما هو نافع للجماعة وما هو عدل في نظرها (رمضان ، ٢٠٠٠، ص. ٢٢).

وتعرف بأنها: "فعل غير مشروع يعتمد الدراية والمعرفة الفنية بتقنية المعلومات، يتم بأي أداة من أدوات الاتصال الذكي والبرمجي، ويكون فيه الفضاء الإلكتروني محلا ومسرحا لها" (الزنداني، ٢٠١٨، ص.٢٧)

وعرفها عياد(٢٠٠٧) على أنها: "افعال غير مشروعة، تهدف للوصول لمعلومات معينة أو حذفها أو نسخها أو تغييرها" (ص.٤٠).

وعرف القحطاني(٢٠١٦،ص.١٨) الجريمة الإلكترونية بأنها: نشاط غر مشروع، يتخذ نظم المعلومات ووسائل الاتصال الحديث أداة له، يصدر عن إرادة آثمة، ويقرر له القانون عقوبة أو تدبر احرازي.

المطلب الثاني: خصائص وأركان الجريمة الالكترونية:

تتشابه الجريمة الإلكترونية مع الجريمة التقليدية من جانب أركان الجريمة (المجرم والضحية والدافع والزمان والمكان)، ونظراً لارتباط الجريمة الالكترونية بجهاز الحاسوب ، وشبكة الانترنت بصورة عامة ووسائل التواصل الاجتماعي بصورة خاصة فقد وجدت مجموعة من الخصائص المميزة لها التي تجعلها غير الجرائم التقليدية ومن هذه الخصائص:

ومن خصائص الجريمة الإلكترونية ما ذكره العجمي، ومنها:

أولاً: جريمة عابرة للقارات:

ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم، أدى إلى انعكاس على طبيعة الأعمال الإجرامية، التي يعمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، وهو ما يعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا ويتم من دولة إلى أخرى.

ثانياً: صعوبة اكتشافها واثباتها:

السبب في ذلك لأنها لا تترك اي اثر مادي ظاهر يمكن ضبطه فعلاً عن التباعد الجغرافي الذي يثير الإشكال بداية حيث تشير الدراسات الى ان ما تم اكتشافه من جرائم المعلومات يصل الى نسبة ١% والذي يتم الابلاغ عن هذه النسبة لا يكاد يصل الى ٥%فقط ، والوسيلة المستخدمة لارتكاب الجريمة هي سبقة الكترونية ينتهي دورها في أقل من ثانية واحدة وكأن الجاني يقوم بتدمير كل دليل لمجرد الاستعمال وبكل هدوء دون أي ضجة. (العجمي، ٢٠١٤، ص.٢٠)

ثالثاً: جرائم ناعمة ومغرية للمجرمين:

إذا كانت الجريمة بصورتها التقليدية تحتاج في الأغلب إلى مجهود عضلي كجرائم القتل والاغتصاب، فإن الجريمة الإلكترونية على العكس لا تحتاج إلى أدنى مجهود عضلي، بل تعتمد على الدراية الذهنية والتفكير المدروس، القائم على المعرفة بتقنيات الحاسب الآلي، فهي لا تحتاج إلى أي درجة من القرب أو التلامس المادي بين الجاني والضحية، لذا تتسم بأنها أقل عنفا وخشونة من التقليدية. (بغدادي، ٢٠١٨، ص.١١)

رابعاً: الاعتداء فيها يطال معطيات الحاسب الآلي: من خلال ارتكاب الجريمة بواسطة الحاسب الالي، أو الاعتداء على الحاسب الالي او ملحقاته.(عبابنة، ٢٠٠٤، ص.٣١).

وصنفت شفيقة المجرمين عن (فكري،٢٠١٤؛ و لطفي،٢٠١٩) كالآتي:

أولا: القراصنة: يمكن تصنيفهم إلى صنفين:

الهاكرز: هي طائفة من المتطفلين يتحدون إجراءات أمن النظام والشبكات، لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية، وإنما ينطلقون من دوافع التحدي وإثبات المقدرة، فاصطلاح الهاكرز مرادف في الغالب لهجمات التحدي.(فكري ،٢٠١٤، ص. ١٢٣).

الكراكز :اصطلاح الكراكرز مرادف للهجمات الحاقدة والمؤذية، وهم الأشخاص الذين يقومون بالتسلل إلى أنظمة المعالجة الآلية للإطلاع على المعلومات المخزنة بها، لإلحاق الضرر أو العبث بها أو سرقتها. (لطفي، ٢٠١٩، ص.٣٨).

ثانيا: الحاقدون: يحرك أنشطة هذه الفئة الرغبة بالانتقام والثأر كأثر لتصرف صاحب العمل معهم أو لتصرف المنشأة المعنية معهم، عندما لا يكونون موظفين فيها، وتغلب على أنشطتهم من الناحية التقنية استخدام تقنيات زراعة الفيروسات و البرامج الضارة وتخريب النظام.(فكري ،٢٠١٤، ص. ١٢٣).

ثالثا: الهواة: من يرتكبون هذه الجرائم بغرض التسلية، دون أن تكون لديهم نية إحداث أي أضرار بالمجني عليهم، وتتميز هذه الفئة بصغر سنهم ونبوغهم في علوم الحاسب، إلا أن خطورتهم تكمن في أنهم قد يكونون نواة جيدة للتحول إلى قرصان محترف.(لطفي،٢٠١٩، ص.٣٨)

رابعاً: خصوصية المجرم الالكتروني : يتميز المجرم الالكتروني عن غيره من مرتكبي جرائم المعلوماتية بطائفة من الخصائص التي تميزه عن غيره من المجرمين منها: صغير السن وذكي متخصص ومحترف و يعود لارتكاب الجرائم باستمرار لتغطية أثار جرائمه.(الشكري، ٢٠٠٨، ص.٩)

المطلب الثالث: صور وأنواع الجرائم الالكترونية:

الجرائم الالكترونية تختلف حسب معيار الفقهاء في تقسيمهم لهذه الجرائم، لهذا تتعدد صور ارتكاب الجرائم الالكترونية جرائم المعلوماتية فيها ما يمس استقلال البلاد ويتعلق بالمحافظة على الامن والاستقرار وفيها ما يتعلق باستخدام الانترنت في ارتكاب جرائم الاتجار بالبشر والمخدرات والممارسات الجنسية والاحتيال والتزوير وغيرها ونتناول أهم هذه الجرائم كالآتي: اتفق (الشوايكة، ٢٠١٤، ص.١٠٥؛ خنيفر،د.ت ، ص.٩) على عدد من اصناف الجرائم الالكترونية والتي قسمت الجرائم الالكترونية إلى الآتي:

١- **الجرائم الجنسية والإباحية وغير الأخلاقية واستغلال الأطفال**. عالمية الانترنت ساحة مفتوحة لممارسة جميع انواع الجرائم ومن ضمنها الاعمال المخلة بالآداب العامة والاخلاق والتي تختلف من بلد لأخر كعرض المواد الخليعة عبر شبكة الانترنت باستخدام التقنية الرقمية.

٢- **قرصنة البرامج عبر شبكة الانترنت.** يقصد بها النسخ وتشغيل الحاسوب والدخول غير المشروع بقصد تدمير المواقع الالكترونية وكل من فك أو نزع أو أتلف تشفيراً لموقع الكتروني أو أجهزة الحاسوب أو شبكة المعلومات.

٣- **إتلاف المعلومات المخزنة:** بمسح البرنامج أو إفساد المعلومات مغناطيسيا أو عن طريق ضرب وحدات تشغيل المعلومات أو احراقها، أو تفجيرها بشحنات ناسفة وغيرها.

٤- **إساءة استخدام البطاقات البنكية:** كاستخدام البطاقات المسروقة أو منتهية الصلاحية، أو تزوير البطاقات، قيام صاحب البطاقة نفسه بسحب مبالغ نقدية أكبر من المبالغ المسموح له .

٥- **سرقة البيانات الشخصية:** وهي الاستيلاء على المعلومات سواء أكانت هذه البيانات في أسطوانات أو على شريط ممغنط أو على ورق.

٦- **التلاعب في برامج الأشخاص:** ومن هذه البرامج: تغيير برنامج نظام التشغيل، خلق برنامج جديد (وهمي) من أجل ارتكاب الجريمة.

٧- **جرائم القذف والسب والتشهير:** من خلال التسلل لمواقع الشخص وأخذ ما فيها من صور خاصة وأخبار، والعمل على نشر ها وقد تمس الشرف، كما تستخدم بغرض الابتزازي.

٨- **جرائم المقامرة:** وتشمل تملك وإدارة مشروع مقامرة على الانترنت، وتسهيل ذلك وتشجيعه، واستخدام الانترنت لترويج الكحول ومواد الإدمان للقصر.

٩- **الاحتيال الإلكتروني:** ويقصد به أي سلوك أو تصرف يحدث من فرد أو العديد من الأفراد يرهق أو يتسبب في أعباء إضافية على أية أطراف أخرى، تتفق جريمة النصب(الاحتيال) مع جريمتي السرقة وخيانة الأمانة لأنها تطال مال الغير إلا أنها تختلف عنها في أن محلها يمكن ان يكون عقاراً . واضاف كاظم (٢٠١٨، ص.١٣) عدد من أنواع الجرائم الإلكترونية منها:

جرائم الارهاب الالكتروني: استخدام اجهزة الحاسوب وشبكة المعلومات بقصد ارتكاب الجرائم التي تمس استقلال البلاد ووحدتها وسلامتها ومصالحها الاقتصادية او السياسية او العسكرية او الامنية العليا من خلال اتلاف اجهزة وانظمة المعلومات العائدة للجهات الأمنية.

تجارة المخدرات عبر الانترنت: تسهم بعض المواقع في انحراف الشباب وخصوصاً من المراهقين وذلك من خلال انشاء مواقع الكترونية تقصد التجارة بالمخدرات او المؤثرات العقلية او الترويج لها.

سرقة المال المعلوماتي: يثور الخلاف عندما يتم الاستيلاء على المعلومات المخزنة داخل الجهاز دون وجه حق او نسخ هذه المعلومات وبذلك فأنه يجزم بإمكانية سرقة المعلومة والأموال.

وفي نطاق هذا القانون النموذجي الوارد ضمن مشروع القانون النموذجي الأمريكي فإنه تم تقسم الجرائم الإلكترونية على :

١- الجرائم الواقعة على الأشخاص.

٢- الجرائم الواقعة على الأموال عدا السرقة.

٣- الجرائم الماسة بالمصالح الحكومية.

٤- جرائم التزوير والمقامرة والجرائم المنافية للآداب.

٥- جرائم السرقة والاحتيال.(تم الاسترجاع من الموقع، https://draya-eg.org/2022/04/13

ومن أنواع الجرائم الإلكترونية:

يتفق الباحث مع ما ورد في الموقع(https://draya-eg.org) بأن هناك الكثير من أنواع الجرائم الإلكترونية والتي تستهدف الأفراد والجماعات والمؤسسات والدول ، وجاء التقسيم الأكثر شمولية لأنواع هذه الجرائم كالتالي :

(أ) جرائم تستهدف الأفراد: وهي جرائم يتم من خلالها استهداف فئة من الأفراد أو فرد بعينه من أجل الحصول على معلومات هامة تخص حساباته سواء البنكية أو على الإنترنت، من أجل استغلالها لتحقيق مكاسب مادية أو التشهير بسمعة أو إفساد العلاقات سواء الاجتماعية أو علاقات العمل، واستغلالها في ابتزاز الضحايا بالقيام بأعمال غير مشروعة تتعلق بالدعارة وتجارة المخدرات وغسيل الأموال والعديد من الجرائم الإلكترونية الأخرى.

(ب) جرائم تستهدف المؤسسات: تتسبب الجرائم الإلكترونية بخسائر كبيرة للمؤسسات والشركات متمثلة في خسائر مادية وأخرى تتعلق بالنظم ومنها:

اختراق الأنظمة: اختراق أنظمة الشبكات الخاصة بالمؤسسات والشركات والحصول على معلومات قيمة وخاصة بأنظمة الشركات، ومن ثم يقوم باستخدام المعلومات من أجل خدمة مصالحه الشخصية والتي تتمثل في سرقة الأموال وتدمير أنظمة الشركة الداعمة في عملية الإدارة مما يسبب خسائر جسيمة للشركة أو المؤسسة.

اختراق المواقع الإلكترونية والسيطرة عليها: ومن ثم توظيفها لتخدم مصالح كيانات خطيرة تهدف إلى زعزعة الأمن بالبلاد والسيطرة على عقول الشباب وتحريضهم للقيام بأعمال غير مشروعة.

تدمير النظم: يكون هذا النوع من التدمير باستخدام الطرق الشائعة وهي الفيروسات الإلكترونية والتي تنتشر في النظام وتسبب الفوضى والتدمير، ويتسبب ذلك في العديد من الخسائر المرتبطة بالملفات المدمرة ومدى أهميتها في إدارة وتنظيم الشركات والمؤسسات.

هجمات تعطيل الخدمة (DOS): يمكن تعريف هجوم DoS او Denial-of-Service أو الحرمان من الخدمة بأنه طريقة تُستخدم لتعطيل وصول المستخدمين الشرعيين إلى شبكة مستهدفة أو مورد ويب. عادة يتم تحقيق ذلك عن طريق التحميل الزائد على الهدف (غالبًا خادم ويب) بكمية هائلة من التصفح أو عن طريق إرسال طلبات ضارة تتسبب في خلل المورد المستهدف أو تعطيله بالكامل ويمكن أن تستمر هذه الهجمات من دقائق إلى ساعات وفي بعض الحالات النادرة تستمر لأيام وكثيراً ما تتسبب هذه الأنواع من الانقطاعات في خسائر مالية كبيرة للشركات التي تصبح أهدافًا والتي ليس لديها استراتيجيات للحد منها أو خفض تأثيرها .

(ج) جرائم تستهدف الأموال: الاستيلاء على حسابات البنوك: وهي جرائم تهدف للاستيلاء على الأموال والممتلكات عن طريق اختراق الحسابات البنكية والحسابات المتعلقة بمؤسسات الدولة وغيرها من المؤسسات الخاصة.

انتهاك حقوق الملكية الفكرية والأدبية: وهي صناعة نسخ غير أصلية من البرامج وملفات المالتيميديا ونشرها من خلال الإنترنت، ويتسبب ذلك في خسائر فادحة في مؤسسات صناعة البرامج والصوتيات.

(د) الجرائم التي تستهدف أمن الدولة: وهي جرائم معلوماتية تكون الدولة فيها هي المجني عليه، ويكون الجاني قد دخل أو اخترق موقعًا أو بريدًا إلكترونيًا أو حسابًا خاصًا أو نظامًا معلوماتيًا يُدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة أو مملوكًا لها، أو يخصها على سبيل المثال جرائم التجسس أو التحريض على الإرهاب ضد مصلحة الوطن باستخدام معلومات قد تم سحبها من ملفات أجهزة الدولة.

المبحث الثاني : تحديات عدالة مواجهة الجرائم الالكترونية والحلول المقترحة.

المطلب الأول: تحديات عدالة مواجهة الجرائم الالكترونية:

يواجه العالم أفراد وجماعات تحديدات ومعيقات لعدالة منع الجرائم الالكترونية وبعد مراجعة الباحث للعديد من المراجع والدراسات التي تناولت الصعوبات والتحديات التي تواجه تحقيق العدالة الالكترونية ومنها: (طالة، سلام، ٢٠٢٠، ص.٨٦)؛ (خنيفر، د.ت، ص.١٢)؛ (ربايعة،٢٠١٦، ص.٢٨)؛ (هانية، ٢٠٢٤، ص.٣٠٨)؛ (حسين وبهاء الدين، دت، ص.٥) تم التوصل إلى التحديات التي تعيق تحقيق العدالة تمثلت في التحديات الآتية:

أولا : طبيعة الجريمة الإلكترونية العابرة للحدود:

الجريمة الإلكترونية تتسم بالطابع الدولي ، لأن نظام الإنترنت جعل من معظم دول العالم في حالة اتصال دائم على الخط ، فهي لا تعترف بالحدود بين الدول، ويمكن ارتكاب هذه الجريمة عن بعد ، وقد يتعد ارتكابها بين أكثر من دولة ، كما أن المواقيت تختلف بين الدول مما يثير إشكالية حول القانون الواجب التطبيق على هذه الجريمة.

ثانياً: تحديات إثبات الجريمة الإلكترونية :

وترجع صعوبة إثبات الجريمة إلى أن الجريمة الإلكترونية لا تترك آثار مادية كمستندات ورقية، ولا تترك شهودا يمكن استجوابهم ولا أدلة يمكن فحصها ، ومن الصعب الاحتفاظ بدليل الجريمة الإلكترونية، إذ يستطيع المجرم في أقل من ثانية أن يمحو أو يحرف أو يغير المعلومات الموجودة في الكمبيوتر، وتحتاج لاكتشافها إلى خبرة فنية ، تعتمد الجريمة الإلكترونية على الخداع والذكاء في التعرف على مرتكبيها بالاحجام عن البلاغ. (الملط،٢٠٠٥، ص.١١٣)

ثالثاً: تحديات تنفيذ العقوبات في جرائم الإلكترونية:

صعوبة تتبع الجناة في الجرائم الإلكترونية لقدرتهم العالية بالإحاطة ببعض الأساليب الأمنية وتدابير الحماية الفنية حيث يمكن للجناة استخدام وسائل تقنية معقدة مثل الشبكات الافتراضية الخاصة (VPN) وأدوات إخفاء الهوية (Tor) لتنفيذ جرائمهم دون ترك أثر واضح؛ مما يحول دون الوصول إلى هويته الحقيقية وإكتشاف أفعاله غير المشروعة في فترة وجيزة، وهذا الأمر يجعل من الصعب على الجهات الأمنية القبض على الجناة وتقديمهم للعدالة.

رابعاً: التحديات القانونية في مواجهة الجرائم الإلكترونية المتمثلة بالآتي:

الطبيعة المعقدة للجريمة الإلكترونية: حيث تتميز بطبيعتها المعقدة، حيث يمكن للمجرمين تنفيذ عملياتهم من أي مكان في العالم دون الحاجة إلى تواجد فعلي في موقع الجريمة. هذا يجعل من الصعب تتبع الجناة وإحضارهم أمام العدالة.

الافتقار إلى الوعي التقني: رغم الجهود المبذولة لتدريب القضاة والعاملين في مجال القانون على التعامل مع الجرائم الإلكترونية، إلا أن هناك نقصًا في الوعي التقني لدى البعض، مما يعيق أحيانًا الفهم الكامل لكيفية حدوث الجريمة وكيفية التعامل معها خاصة مع ضعف النصوص التقليدية لمعالجة سائر الجرائم الإلكترونية المرتكبة.

وضعف التعاون الدولي لمكافحة الجرائم العابرة للحدود: وذلك لأن العديد من جرائم النصب والاحتيال الإلكتروني تتم على مستوى دولي، حيث قد يكون الجاني في دولة أخرى غير الدولة التي يقيم فيها الضحية. يتطلب هذا النوع من الجرائم تعاونًا دوليًا بين السلطات

القضائية في مختلف البلدان، وهو أمر قد يكون معقدًا بسبب اختلاف القوانين والإجراءات بين الدول.

والتكنولوجيا سريعة التطور: تتطور التقنيات الإلكترونية بسرعة، وهو ما يجعل من الصعب على القوانين أن تواكب هذه التطورات بشكل دائم. قد تستغرق عملية تعديل القوانين لتغطية الجرائم الجديدة وقتًا طويلاً، ما يمنح المجرمين فرصة لاستغلال الثغرات القانونية. (يوسف آخر تحديث: سبتمبر ٢٠٢٤ /٩/٢٦ متاح بالموقع (https://easylaweg.com.

مما سبق تبين للباحثة أن هناك العديد من التحديات التي تعيق تحقيق العدالة في حق مرتكبي الجرائم الالكترونية كضعف التعاون بين الدول والمجتمعات والمؤسسات وكذلك الذكاء والحرفية التقنية التي يمتلكها معظم ممارسي الجرائم الالكترونية وضعف التشريعات التي تحقق عدالة المسائلة كما أن البعد المكاني من أهم المعوقات حيث قد ترتكب جرائم في بلدان من أماكن مختلفة وهذه التحديات وغيرها بحاجة للدراسة واقتراح حلول من أجل سلامة الأفراد والمجتمعات ومن أجل تسهيل ضبط مرتكبي هذه الجرائم واللحد منها في مجتمعاتنا مع تأهيل الكوادر الأمنية والمتخصصين في مقاضاة ومتابعة من يقوم بها ومحاسبته .

إحصائية لنوع الجرائم الالكترونية في بعض البلدان:

ورد وفقاً لنتائج بعض الاحصائيات الدولية يتضح أن حجم أكثر جرائم الاختراقات شيوعاً والتي يرتكبها مستخدمي الإنترنت في بعض الأماكن والبلدان في العالم على سبيل المثال: فيما نسبته (٥٠٠٪) اخترقوا مواقع خليجية، وما نسبته (٢٠٩٪) اخترقوا مواقع عربية غير خليجية، وما نسبته (٣٠١٪) اخترقوا مواقع آسيوية غير عربية، وما نسبته (٠٠٣٪) اخترقوا مواقع أفريقية غير عربية، وما نسبته (١٠٨٪) اخترقوا مواقع أوروبية، وما نسبته (٠٠٥٪) اخترقوا مواقع أمريكية جنوبية، وما نسبته (٧٠٨٪) اخترقوا مواقع في الولايات المتحدة الأمريكية وكندا، وما نسبته (٦٥٠٤٪) لا يذكرون المواقع التي اخترقوها. (الحمدان، متاح في(https://www.qaafe.net)

المطلب الثاني: الحلول المقترحة لتحقيق عدالة الحد من الجرائم الالكترونية:

للتغلب على هذه المشاكل فإنه يجب على الجهات المسؤولة تطبيق العقوبات على مرتكبي أي من الجرائم الالكترونية، والبحث عن حلول للمعوقات والصعوبات وادراج ذلك في البرامج التعليمية والتربوية العامة والخاصة لمنع هذه الجرائم قدر الامكان ولابد من اتخاذ خطوات جادة حول ما تم طرحه من توصيات وتشريعات ومنها:

ذكر يوسف، أن هناك حلولاً لتحقيق العدالة في الجرائم الالكترونية تتمثل في الآتي:

تدريب القضاة والمحامين: يتم تقديم برامج تدريبية للقضاة والمحامين لتطوير مهاراتهم في التعامل مع الجرائم الإلكترونية وفهم كيفية تنفيذ الجرائم وتحديد الأدلة. هذه البرامج تهدف إلى تعزيز قدرة النظام القضائي على مواجهة التحديات التقنية وتقديم الجناة للعدالة.

تعزيز التعاون مع الجهات الأمنية: يعمل القضاء في بعض البلدان منها بلادنا بشكل وثيق مع الجهات الأمنية المتخصصة في مكافحة الجرائم الإلكترونية، مثل وحدة مكافحة الجرائم الإلكترونية التابعة لوزارة الداخلية. هذا التعاون يساعد في تتبع الجناة وجمع الأدلة اللازمة للمحاكمة.

زيادة الوعي المجتمعي: تُعد التوعية المجتمعية من الأدوات المهمة في مكافحة جرائم النصب والاحتيال الإلكتروني. تعمل الحكومة بالتعاون مع منظمات المجتمع المدني على إطلاق حملات توعية تهدف إلى تعليم الأفراد كيفية حماية بياناتهم وعدم الوقوع ضحايا لعمليات النصب الإلكتروني.

التعاون مع الجهات الأمنية: التعاون بين الجهات القضائية والجهات الأمنية المتخصصة في الجرائم الإلكترونية هو ركن أساسي في مواجهة هذه الجرائم و تتعاون النيابة العامة مع وحدات مكافحة الجرائم الإلكترونية في وزارة الداخلية لجمع الأدلة وتحليلها وتقديم الجناة للمحاكمة.

استخدام الأدلة الرقمية: أصبح القضاء في عدة بلدان يقبل الأدلة الرقمية والاعتماد عليها في المحاكمات و يتم تقديم السجلات الإلكترونية وتحليل البيانات من قبل خبراء متخصصين، وهذا يسهم في تحسين قدرة المحاكم على إصدار الأحكام بناءً على أدلة موثوقة.

التعاون الدولي: تلعب مصر دورًا نشطًا في التعاون الدولي لمكافحة الجرائم الإلكترونية، من خلال توقيع اتفاقيات دولية تهدف إلى تعزيز التعاون القضائي وتبادل المعلومات بين الدول. هذا يساعد في تعقب الجناة الذين يعملون عبر الحدود وتقديمهم للعدالة. (يوسف، ٢٠٢٤ ، متاح بالموقع https://easylaweg.com.).

وبعد مراجعة العديد من المراجع والمواقع تم تلخيص عدد من التوصيات لوضعها تحت نظر متخذي القرار للاستفادة منها في مواجهة التهديدات الناتجة عن الجرائم الإلكترونية، ووضع سياسات وحلول للحد منها ومن أبرز هذه التوصيات والحلول:

أولا: على مستوى السياسات العامة:

١) وضع استراتيجية وطنية لمواجهة الجرائم الإلكترونية تشارك فيها كل مؤسسات الدولة المعنية.

٢) عقد دورات تدريبية لأعضاء النيابة العامة والقضاة والاداريين بهدف تثقيفهم فنيا وعرض آخر التطورات التقنية والفنية فيما يتعلق بالجرائم الإلكترونية بالشكل الذي يعينهم على كشف الجرائم المعلوماتية وملاحقة مرتكبيها.

٣) إنشاء قسم جديد بكليات الحقوق بالجامعات يكون معنيا بدراسة هذا النوع من الجرائم وطرق الحماية القانونية من الانتهاكات الناجمة عنها، ويكون معنيا بوضع قانون خاص بجرائم المعلومات والإنترنت.

٤) تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب.

٥) تدريس مقررات حول الجرائم الإلكترونية وسبل مواجهتها في مناهج التعليم قبل الجامعي والجامعي ومجالات التخصص الفني والقانوني والاجتماعي والنفسي والاقتصادي.

٦) استحداث مادة حول "أخلاقيات استخدام الانترنت" وإدراجها ضمن المناهج التعليمية للتوعية وإكساب الأطفال والشباب اتجاهات إيجابية تجاه استخدام الإنترنت والتطبيقات الإلكترونية.

٧) دعم الإنفاق البحثي في الجامعات والمؤسسات التعليمية في مجال الإلكترونيات ووسائل الاتصالات الحديثة.

٨) تأهيل وتنمية قدرات الكوادر البشرية العاملة في مجالات مكافحة الجرائم المعلوماتية بُغية مواكبة التطور التكنولوجي المتعاقب.

٩) وضع تعريف واضح وشامل لمفهوم الجرائم الإلكترونية وأنواعها وتحديد الجهة التي يجب أن تتعامل مع هذا النوع من الجرائم.

١٠) إنشاء موقع إلكتروني يكون مختص بالرد على كافة الشكاوى والاستفسارات المتعلقة بتطبيق قانون مكافحة تقنية المعلومات ولائحته التنفيذية، ونشر كل ما يستحدث في مجال تقنية المعلومات من الناحية الفنية والقانونية.

١١) إحكام الرقابة على المقاهي الإلكترونية ووضع الضوابط التي تحد من الانفلات الواقع داخلها.

١٢) تفعيل دور مؤسسات المجتمع المدني للتوعية والتحذير من مخاطر شبكة الإنترنت والجرائم الرقمية والوقاية من الوقوع في الممارسات الخاطئة للسلوكيات والممارسات الضارة أخلاقياً عبر الشبكة.

١٣) ضرورة التنسيق والتعاون الدولي قضائيا وإجرائيا في مجال مكافحة الجرائم المعلوماتية.

١٤) رفع درجة الأمان للأجهزة الرقمية والمعلوماتية وعدم الكشف عن كلمة السر نهائيا وتغييرها بشكل مستمر واختيار كلمات سر صعبة يصعب اختراقها.

١٥) توعية مستخدمي الإنترنت بمخاطره وتجنب تحميل أي برنامج مجهول المصدر وحجب المواقع الإباحية.

١٦) رفع مستوى الإدراك لدى الأطفال تجاه ما يمكن أن يصلهم من محتوى غير لائق، وتوعيتهم بأهمية عدم الإدلاء بأية بيانات شخصية.

ثانيا: على مستوى التشريعات الوطنية:

١) تأسيس منظمة خاصة لمكافحة الجرائم الإلكترونية والحد منها .

٢) تعديل بعض أحكام القانون في شأن مكافحة جرائم تقنية المعلومات وذلك بهدف التزام الدقة في تحديد الأفعال المعاقب عليها، وتجنب غموض الصياغة التشريعية ووضع تعاريف دقيقة لها، وتغليظ العقوبات فيما يرتبط بجرائم تقنية المعلومات.

٣) مواكبة التطورات المرتبطة بالجريمة الإلكترونية والحرص على تطوير وسائل مكافحتها.

٤) استحداث بعض نصوص القانون لسد الثغرات ومواكبة سرعة التطور التكنولوجي وأدواته.

٥) إنشاء محكمة خاصة بهذه النوعية من الجرائم كونها تختلف في طبيعتها عن الجرائم التقليدية وتتطلب مواجهتها أساليبا تقنية وتكنولوجية شديدة الحداثة والتطور.

(طالة، سلام، ٢٠٢٠، ص٨٦)؛ (شفيقه خنيفر، د.ت، ص١٢)؛ (ربايعة،٢٠١٦، ص.٢٨)؛ (هانية، ٢٠٢٤، ص.٣٠٩)؛ (و https://draya-eg.org/13/4/2024 https://easylaweg.com.)

الآليات القانونية لمكافحة الجرائم الإلكترونية:

١) تعتمد الدول العربية على تشريعات مختلفة لمعاقبة مرتكبي الابتزاز الإلكتروني، ومن أبرزها:

٢) القوانين الخاصة بالجريمة الإلكترونية: مثل القانون المغربي رقم ١٠٣.١٣ المتعلق بمحاربة العنف ضد النساء والذي يشمل الابتزاز الإلكتروني.

٣) وحدات مكافحة الجرائم الإلكترونية: موجودة في معظم الدول.

٤) العقوبات الصارمة: تتراوح بين الغرامات المالية والسجن لفترات قد تصل إلى ١٠ سنوات. (https://ar.thoumetsghair.com استرجع(٥-١-٢٠٢٥).)

٥) اصدار تشريعات جديدة او تعديل التشريعات الجزائية القائمة لمواجهة الجرائم الالكترونية وذلك بتقرير الجرائم وتحديد العقوبات المناسبة لها بغية حماية النظام المعلوماتي.

٦) ايجاد ادلة اثبات جديدة مع طبيعة هذه الجرائم وذلك لعدم ملائمة ادلة الاثبات التقليدية في القانون الجنائي لا ثباتها.

٧) اعتماد الدقة والوضوح والحبكة القانونية عند تحديد انماط السلوك الاجرامي والابتعاد عن التعبيرات الغامضة او المطاطية التي تحمل اكثر من معنى او دلالة.

٨) عدم الاقتصار عند التجريم والعقاب على انماط السلوك المحظور المرتكبة حالياً بل يجب مراعاة الابعاد المستقبلية لان تكنلوجيا المعلومات والحواسيب في تطور سريع بل يكاد يكون مذهل. (كاظم،٢٠١٨ ، ص.٢٥)

منهج الدراسة:

اعتمدت الباحثة في هذه الدراسة على المنهج الإحصائي المبني على وصف الظاهرة وتحليل نتائجها.

مجتمع الدراسة : تكون مجتمع البحث من رجال الأمن في إمارة الشارقة.

عينة الدراسة : تم اختيار عينة من رجال الأمن بإمارة الشارقة بطريقة عشوائية تكونت من (٢٥) فرداً.

أداة الدراسة:

تمثلت أداة جمع البيانات من استبيان تكون من (٥٠) فقرة، وذلك بعد بنائه وضبط صدقه وثباته بالأساليب المعروفة وفق منهجية البحث العلمي من خلال صدق المحكمين وحساب الثبات لفقراته من نتائج عينة استطلاعية باستخدام معامل الفا كرومباخ الذي وصل إلى (٨٧%) وهي قيمة ثبات عالية ومقبولة واصبح في الصورة النهائية قابل للتطبيق.

الأساليب الإحصائية المستخدمة: تم حساب قيم التكرارات، والمتوسط الحسابي والانحراف المعياري لكل فقرة ومجال ومعامل الفا كرومباخ لحساب ثبات الاستبيان.

النتائج التي توصلت إليها الدراسة:

أولاً: للإجابة عن السؤال الأول :ما التحديات التي تعيق عدالة مواجهة الجرائم الالكترونية في العصر الرقمي من وجهة نظر رجال الأمن؟

تمت الإجابة من خلال ماتم استخلاصه من الاطار النظري ووضعه في استبيان وطرحه على رجال الأمن، ومن خلال استجاباتهم تم جمع البيانات حول التحديات التي تعيق تحقيق العدالة وبعد تحليل هذه البيانات إحصائياً تم الحصول على النتائج الموضحة في الجدول التالي:

جدول رقم(١) التحديات التي تعيق تحقيق عدالة مواجهة الجرائم الالكترونية في العصر الرقمي من وجهة نظر رجال الأمن

م	الفقرات	مجموع قيم التكرارات	المتوسط	الانحراف المعياري	الترتيب
1	الجرائم الإلكترونية عابرة للحدود فقد يكون الجاني في دولة غير دولة الضحية	101	4.04	.455	
2	تتميز الجرائم الإلكترونية بطبيعة معقدة	92	3.68	.476	
3	يمكن للمجرمين تنفيذ عملياتهم من أي مكان في العالم دون الحاجة إلى تواجد فعلي في موقع الجريمة	94	3.76	.663	
4	من الصعب تتبع الجناة وإحضارهم أمام العدالة.	85	3.40	.645	
5	تغيير المجرم للشبكات والمواقع بشكل مستمر يفقد كشف هويته وتتبع مكانة.	90	3.60	.645	
6	صعوبة الاحتفاظ بدليل الجريمة الإلكترونية فقد يتم إتلاف الدليل الإلكتروني بثانية.	92	3.68	.476	
7	تواجه الدولة تحديات في تنفيذ عقوبات هذه الجرائم لغياب التشريع ودليل ملموس.	104	4.16	.800	
8	صعوبة تتبع الجناة في الجرائم الإلكترونية والقبض عليهم وتقديمهم للعدالة	101	4.04	.539	
9	استخدام الجناة وسائل تقنية معقدة مثل الشبكات الافتراضية الخاصة (VPN) وأدوات إخفاء الهوية (Tor) لتنفيذ جرائمهم دون ترك أثر واضح.	106	4.24	.723	
10	تتم جرائم النصب والاحتيال الإلكتروني على مستوى دولي معقد.	102	4.08	.572	
11	صعوبة التعاون الدولي بين السلطات القضائية في مختلف البلدان، بسبب اختلاف القوانين والإجراءات بين الدول.	92	3.68	.476	
12	سرعة تطور التقنيات الإلكترونية يصعب تطوير القوانين اللازمة لمواكبتها	106	4.24	.831	
13	تعديل القوانين لتغطية الجرائم الجديدة يستغرق وقتًا طويلاً، يمنح المجرمين فرصة لاستغلال الثغرات القانونية.	91	3.64	.700	

م	الفقرات	مجموع قيم التكرارات	المتوسط	الانحراف المعياري	الترتيب
14	عدم تطوير آليات جديدة وتعاونًا مع الجهات الدولية والمحلية لمكافحتها.	86	3.44	.583	
15	غياب الأدلة المادية التي يمكن تقديمها في المحكمة.	84	3.36	.490	
16	تعتمد الجرائم الإلكترونية على الأدلة الرقمية المشفرة. تتطلب خبراء متخصصين لتقديمها بشكل مناسب أمام المحكمة.	93	3.72	.678	
17	استخدام الجناة أدوات وتقنيات حديثة تفوق قدرات الجهات القضائية	95	3.80	.408	
18	استخدام الجناة برامج تشفير متطورة لإخفاء الهوية مما يصعب تتبع أنشطتهم.	101	4.21	.884	
19	غياب تدريب الأجهزة على استخدام التكنولوجيا الرقمية وكيفية جمع الأدلة وتحليلها.	100	4.00	1.04	
20	جمود النصوص التقليدية لمعالجة سائر الجرائم الإلكترونية المرتكبة.	100	4.00	.764	
21	ندرة قيام المجني عليه بالإبلاغ عن الجريمة يصعب اكتشافها.	94	3.76	.879	
22	قدرة المجرم العالية اختراق الأساليب الأمنية وتدابير الحماية الفنية مما يحول دون الوصول إلى هويته.	104	4.16	.800	
23	الجريمة الإلكترونية لا تترك شهودا يمكن استجوابهم ولا أدلة يمكن فحصها .	96	3.84	1.11	
24	ضعف استخدام رجال القانون للتقنية للتعامل مع الجرائم الإلكترونية، وكيفية حدوثها.	93	3.72	.678	
25	تحتاج الجريمة لاكتشافها إلى خبرة فنية وإلمام بمعلومات ارتكابها أو التحقيق فيها .	91	3.64	.490	
	المتوسط العام للمجموع الكلي	95.72	3.836	0.672	

يتبين من نتائج فقرات الجدول (١) أن استجابات العينة لهذه الفقرات قد توزع بين مستوى (متوسط ، وكبيرة، وكبيرة جداً) حيث بلغت المستوى الأعلى (كبيرة جداً) خمس فقرات توزعت متوسطات فقراته ما بين (٤.١٦ وحتى٤.٢٤) كان أكبر متوسط (٤.٢٤)

للفقرتين رقم (٩ و ١٢) ومتوسط (٤.٢١) للفقرة (١٨) بينما الفقرتين (٧ و ٢٢) كان متوسطهما (٤.١٦) وبذلك احتلت هذه الفقرات ترتيبها من الترتيب الأول وحتى الثالث، كان في الترتيب الأول الفقرتين التاسعة والثانية عشر(استخدام الجناة وسائل تقنية معقدة مثل الشبكات الافتراضية الخاصة (VPN) وأدوات إخفاء الهوية (Tor) لتنفيذ جرائمهم دون ترك أثر واضح. وسرعة تطور التقنيات الإلكترونية يصعب تطوير القوانين اللازمة لمواكبتها) بمتوسط (٤.٢٤)، ويليها في الترتيب الثاني الفقرة الثامنة عشر() بنفس المتوسط(٤.٢١)، وفي الترتيب الثالث الفقرتين السابعة والثانية والعشرين (تواجه الدولة تحديات في تنفيذ عقوبات هذه الجرائم لغياب التشريع ودليل ملموس. وقدرة المجرم العالية اختراق الأساليب الأمنية وتدابير الحماية الفنية مما يحول دون الوصول إلى هويته) بمتوسط (٤.١٦)، بينما حصلت على المستوى (كبيرة) تسعة عشر فقرة توزعت متوسطاتها ما بين (٣.٤ وحتى ٤.٠٨) كان أعلاها الفقرة العاشرة (تتم جرائم النصب والاحتيال الإلكتروني على مستوى دولي معقد) بمتوسط (٤.٠٨) والمرتبة الرابعة، وكان أدناها الفقرتين الرابعة والرابعة عشر(من الصعب تتبع الجناة وإحضارهم أمام العدالة. وعدم تطوير آليات جديدة وتعاونًا مع الجهات الدولية والمحلية لمكافحتها) بمتوسط (٣.٤)، وقد حصلت على أقل مستوى متوسط الفقرة الخامسة عشر(غياب الأدلة المادية التي يمكن تقديمها في المحكمة) بمتوسط (٣.٣٦) والترتيب الأخير، وبذلك تبين أن الفقرات (٧، ٩، ١٢، ١٨، ٢٢) قد برزت بشكل أفضل من الفقرات(٤، ١٤، ١٥) وعليه فإن اكبر عوائق تحقيق عدالة مكافحة الجريمة تمثلت بقدرة مرتكب الجرائم على البرمجة واختراق الأنظمة والتخفي، مع اختفاء ادوات الجريمة وطمسها وغياب ادلة ملموسة وقدرته على اختراج اجهزة الأمن وهذا ما يتفق مع دراسة (الملط، ٢٠٠٥) وغياب التشريعات والتعاون الدولي لمنع الجريمة وتحقيق العدالة في حق مرتكبيها، كما يجب زيادة التركيز والاهتمام بتتبع الجناة وإحضارهم أمام العدالة، وتطوير آليات جديدة وتعاونًا مع الجهات الدولية والمحلية لمكافحتها وعلى إثارة الوعي بالقضايا المهمة في تقديم الأدلة المادية التي يمكن تقديمها في المحكمة حتى يتم ردع الجرائم وتحقيق العدالة وهذا ما اتفق مع دراسة يوسف(٢٠٢٤) متاح بالموقع https://easylaweg.com.

وقد كانت النتيجة النهائية لهذا المحور (كبيرة) بمتوسط (٣.٨٣٦) وهذا يعني أن من الضروري التركيز والاهتمام بالتصدي لهذه العوائق من خلال ايجاد حلول مناسبة لتجاوز العوائق من أجل تحقيق عدالة مكافحة الجريمة في العصر الرقمي.

ثانياً: للإجابة عن السؤال الثاني :ما الحلول المقترحة لتحقيق العدالة بمواجهة الجرائم الالكترونية في العصر الرقمي من وجهة نظر رجال الأمن؟

تمت الإجابة من خلال ما تم استخلاصه من الاطار النظري ووضعه في استبيان (المحور الثاني) وطرحه على رجال الأمن ومن خلال استجاباتهم تم جمع البيانات حول المقترحات والحلول الممكنة وبعد تحليل هذه البيانات إحصائياً تم الحصول على النتائج الموضحة في الجدول التالي:

جدول رقم (٢) نتائج الحلول المقترحة لتحقيق العدالة بمواجهة الجرائم الالكترونية في العصر الرقمي من وجهة نظر رجال الأمن

م	الفقرات	مجموع التكرارات	المتوسط	الانحراف المعياري	الترتيب
1	تفعيل دور وحدات مكافحة الجرائم الإلكترونية في دول العالم، كوحدة الجرائم المعلوماتية في الإمارات.	100	4.00	.500	
2	وضع استراتيجية وطنية لتأسيس منظمة خاصة لمكافحة الجرائم الإلكترونية والحد منها.	99	3.96	.539	
3	إقرار تشريع خاص بالجرائم الالكترونية ينظمها من جميع جوانبها الموضوعية والإجرائية.	102	4.08	.572	
4	إنشاء محكمة خاصة بهذه النوعية من الجرائم مزودة بأساليب تقنية وتكنولوجية شديدة الحداثة والتطور.	97	3.88	.666	
5	تأهيل وتنمية قدرات الكوادر البشرية العاملة في مجالات مكافحة الجرائم المعلوماتية لمواكبة التطور التكنولوجي المتعاقب.	102	4.08	.862	
6	دعم الإنفاق البحثي في الجامعات والمؤسسات التعليمية في مجال الإلكترونيات ووسائل الاتصالات الحديثة.	100	4.00	.816	
7	ضرورة التنسيق والتعاون الدولي قضائيا وإجرائيا في مجال مكافحة الجرائم المعلوماتية.	98	3.92	.493	
8	التعاون بين النيابة العامة مع وزارة الداخلية لجمع الأدلة وتحليلها وضبط ومحاكمة الجناة.	94	3.76	.723	
9	استخدام أساليب وتقنيات متطورة لكشف هوية مرتكب الجرم والقبض عليهم بأقل وقت .	99	3.96	.539	
10	تدريس مقررات حول الجرائم الإلكترونية وسبل مواجهتها وأخلاقيات استخدام الانترنت.	99	3.96	.790	

م	الفقرات	مجموع التكرارات	المتوسط	الانحراف المعياري	الترتيب
11	توعية الأفراد بمخاطر الجرائم الإلكترونية وحجب مواقع الأفعال المعيبة والاجرامية.	103	4.12	.881	
12	تشديد الرقابة على الأبناء ومتابعة حساباتهم الشخصية وطبيعة المواقع التي يتصفحوها.	98	3.92	.812	
13	إنشاء مواقع وطنية تنويريه تحافظ على القيم وتفرض عقوبات صارمة على مرتكبي جرائم.	97	3.88	.726	
14	المسارعة بإبلاغ الجهات الأمنية فور التعرض لجريمة إلكترونية.	102	4.08	.862	
15	الحفاظ على سرية المعلومات الخاصة بالحسابات الالكترونية وتغيير كلمة السر المعقدة.	100	4.00	.707	
16	استخدام برمجيات آمنة ونظم تشغيل خالية من الثغرات وتجنب البرنامج مجهول المصدر.	92	3.68	.476	
17	فصل اتصال جهاز الحاسوب بشبكة الانترنت في حال عدم الاستخدام.	82	3.28	.980	
18	التزم القانون في احترام الحقوق والملكيات وأمن المعلومات ومنع التجسس.	85	3.40	.500	
19	تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب.	82	3.28	.843	
20	استحداث بعض نصوص القانون لسد الثغرات ومواكبة سرعة التطور التكنولوجي وأدواته.	89	3.56	.651	
21	رفع درجة الأمان للأجهزة الرقمية والمعلوماتية بشكل يصعب معه الاختراق وتحديث برامجها.	98	3.92	.702	
22	إنشاء موقع إلكتروني يكون مختص بالرد على كافة الشكاوى المتعلقة بالجريمة الالكترونية.	97	3.88	.833	
23	سن قانون العقوبات الصارمة تتراوح بين الغرامات المالية والسجن لفترات طويلة.	99	3.96	.676	
24	تعميم العقوبات عالمياً على مرتكبي الجريمة وأي مؤسسة ساعدته.	96	3.84	.746	
25	رصد مكافئات لتشجيع الأفراد والمواقع التي تتصدى لمرتكبي الجرائم الالكترونية.	103	4.12	.526	
المتوسط العام للمجموع الكلي		96.52	3.861	0.697	

يتبين من نتائج فقرات الجدول (٢) أن استجابات العينة لهذه الفقرات قد توزع بين مستويين (متوسطة ، وكبيرة) حيث بلغت المستوى الأعلى (كبيرة) ثلاث وعشرين فقرة توزعت متوسطاتها ما بين (٣.٥٦ وحتى٤.١٢) كان أكبر متوسط (٤.١٢) للفقرتين الحادية عشر والخامسة والعشرين رقم (توعية الأفراد بمخاطر الجرائم الإلكترونية وحجب مواقع الأفعال المعيبة والاجرامية، ورصد مكافئات لتشجيع الأفراد والمواقع التي تتصدى لمرتكبي الجرائم الالكترونية) وترتيبهما الأول، ويليه المتوسط (٤.٠٨) للفقرات الثالثة والخامسة والرابعة عشر (إقرار تشريع خاص بالجرائم الالكترونية ينظمها من جميع جوانبها الموضوعية والإجرائية، وتأهيل وتنمية قدرات الكوادر البشرية العاملة في مجالات مكافحة الجرائم المعلوماتية لمواكبة التطور التكنولوجي المتعاقب، والمسارعة بإبلاغ الجهات الأمنية فور التعرض لجريمة إلكترونية) وترتيبهن الثاني، بينما بقية فقرات المستوى (كبيرة) الثمانية عشر توزعت في الترتيب التالي وبمتوسطات توزعت ما بين (٣.٤ وحتى ٤)، بينما حصلت على المستوى (متوسطة) الفقرتين السابعة عشر والتاسعة عشر (فصل اتصال جهاز الحاسوب بشبكة الانترنت في حال عدم الاستخدام، وتجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب) حيث كان متوسطهما (٣.٢٨) والترتيب الأخير، وقد حصلتا على أقل مستوى من بين جمع الفقرات، وبذلك تبين أن الفقرات(٣ ،٥، ١١، ١٤، ٢٥) نالت اهتمام رجال الأمن، وهذا يعني اهمية التوعية من مخاطر الجرائم والمساهمة في كشف المجرمين، وهذا ما يتفق مع دراسة (كاظم،٢٠١٨) ولابد من تشريع يضمن تنفيذ العقوبات وتأهيل الكادر البشري للتعامل بدقة مع هذه الجرائم وأدواتها وسرعة الإبلاغ عن أي مشكلة تحدث، وهذه الفقرات قد برزت بشكل أفضل من الفقرات(١٧، ١٩) التي ترى فصل أجهزة الحاسوب عن الشبكات وعدم تخزين ملفات الصور فقد تتعرض لقرصنة وابتزاز، وهذا ما اتفق مع دراسة يوسف(٢٠٢٤) متاح بالموقع https://easylaweg.com. وقد كانت النتيجة النهائية لهذا المحور (كبيرة) بمتوسط (٣.٨٦١) وهذا يعني أن من الضروري التركيز على لإيجاد الحلول المناسبة لتحقيق عدالة مكافحة الجريمة في العصر الرقمي.

مناقشة النتائج التي توصلت إليها الدراسة:

أولاً: نتائج محور التحديات التي تعيق تحقيق عدالة مواجهة الجرائم الإلكترونية في العصر الرقمي:

تبين أن أكبر عوائق تحقيق عدالة مكافحة الجريمة تمثلت بقدرة مرتكب الجرائم على البرمجة واختراق الأنظمة والتخفي، مع اختفاء أدوات الجريمة وطمسها وغياب أدلة ملموسة وقدرته على اختراج أجهزة الأمن ، وغياب التشريعات والتعاون الدولي لمنع الجريمة وتحقيق العدالة في حق مرتكبيها، كما أن استخدام الجناة وسائل تقنية معقدة مثل الشبكات الافتراضية الخاصة (VPN) وأدوات إخفاء الهوية (Tor) لتنفيذ جرائمهم دون ترك أثر واضح. وسرعة تطور التقنيات الإلكترونية يصعب تطوير القوانين اللازمة لمواكبتها، وتحديات تواجه الدولة في تنفيذ عقوبات هذه الجرائم لغياب التشريع ودليل ملموس. وقدرة المجرم العالية اختراق الأساليب الأمنية وتدابير الحماية الفنية مما يحول دون الوصول إلى هويته، وتتم جرائم النصب والاحتيال الإلكتروني على مستوى دولي معقد، و تخزين ملفات الصور فقد تتعرض لقرصنة وابتزاز.

وعليه ترى الباحثة أنه يجب زيادة التركيز والاهتمام بتتبع الجناة وإحضارهم أمام العدالة، وتطوير آليات جديدة وتعاونًا مع الجهات الدولية والمحلية لمكافحة الجريمة، وإثارة الوعي بالقضايا المهمة في تقديم الأدلة المادية إلى المحكمة حتى يتم ردع الجرائم وتحقيق العدالة.

ثانياً: نتائج محور الحلول المقترحة لتحقيق العدالة بمواجهة الجرائم الالكترونية في العصر الرقمي:

تبين أن أهم الحلول المقترحة لتحقيق العدالة تمثلت في أهمية التوعية من مخاطر الجرائم والمساهمة في كشف المجرمين، ولابد من تشريع يضمن تنفيذ العقوبات وتأهيل الكادر البشري للتعامل بدقة مع هذه الجرائم وأدواتها وسرعة الإبلاغ عن أي مشكلة تحدث، ولا بد من فصل أجهزت الحاسوب عن الشبكات وعدم تخزين ملفات الصور في النت، وأن استخدام التقنيات الذكية في مجال الأمن يسهم في مكافحة الجريمة وتسهيل تحقيق العدالة.

وترى الباحثة أن من الحلول الهامة والسريعة تدريب الكوادر البشرية على البرمجة وكيفية التعامل مع هذه الجرائم، بالإضافة إلى التعاون الدولي وتوعية الأفراد والمجتمعات بهذه المخاطر مع ضرورة توفير تشريع قانوني وأخلاقي يضمن حقوق الناس ويعاقب المذنب والمقصر.

الخاتمة :

تبين من الاستعراض السابق أن الدراسة هدفت إلى توضيح التحديات التي تعيق تحقيق عدالة مواجهة الجرائم الإلكترونية في العصر الرقمي والحلول المقترحة من وجهة نظر رجال الأمن لمنع وقوع الجريمة والحد منها باستخدام كافة الوسائل وفي كل دول العالم ، وتم تحقيق هذا الهدف من خلال تحليل استجابات رجال الأمن على الاستبيان المعد لهذا الغرض.

توصيات الدراسة:

١) ضرورة التنسيق والتعاون الدولي لمكافحة الجريمة والابلاغ عن حدوثها ومعاقبة مرتكبيها.

٢) إعداد إطار تشريعي قضائي حديث تتناسب مع قوانين مكافحة جرائم العصر الرقمي.

٣) تأهيل وتنمية قدرات الكوادر البشرية وتدريبهم على كيفية مواجهة تحديات تحقيق العدالة.

٤) تطوير وسائل وتقنيات مكافحة الجرائم الالكترونية لمواكبة تطورات أنواع الجريمة.

٥) نشر الوعي المجتمعي للتعاون من الأجهزة الأمنية في مكافحة الجرائم ومن حدوثها.

مقترحات الدراسة:

١. أهمية استخدام تقنيات الذكاء الاصطناعي في مكافحة الجريمة الرقمية.

٢. أسباب انتشار جرائم العصر الرقمي وكيفية منع حدوثها.

٣. ما التحديات الأمنية المرتبطة بتحقيق عدالة مكافحة الجرائم.

المراجع

المراجع العربية:

إبراهيم، خالد ممدوح. (٢٠٠٨). *أمن الجريمة الإلكترونية*. الدار الجامعية، الإسكندرية، ص٧.

بغدادي، أدهم باسم نمر. (٢٠١٨). *وسائل البحث والتحري عن الجرائم الإلكترونية، ماجستير في القانون العام*. كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، ص١١-١٢.

بهاء الدين، حسين كامل (٢٠٠٣) : مفترق الطرق ، دار المعارف ، القاهرة ، ص٥٥ .

البيوك، حسين سليم. (٢٠٢١). *الحماية القانونية للبطاقات الائتمانية من خطر القرصنة الالكترونية*. [رسالة دكتوراه، غير منشورة]، كلية الحقوق ، قسم القانون التجاري والبحري ، جامعة عين شمس.

الحبسي، عيسي عبد الله عيسي. (٢٠٢١). *جرائم البريد الالكتروني "دراسة مقارنة"*. [رسالة دكتوراه غير منشورة]، كلية الحقوق، قسم القانون الجنائي، جامعة المنصورة.

خنيفر، شفيقة. (د.ت). الإجرام الإلكتروني، كفاءات ضائعة في عالم التقنية. ورقة علمية مقدمة للمؤتمر العلمي الافتراضي الأول: الجريمة الإلكترونية (الواقع والتداعيات)،جامعة محمد الشريف مساعدية ، سوق أهراس، الجزائر

ربايعة، عبد اللطيف محمود. (٢٠١٦). الجرائم الالكترونية (التجريم والملاحقة والإثبات). ورقة بحث مقدم إلى المؤتمر الأول للجرائم الالكترونية في فلسطين، المنعقد في جامعة النجاح الوطنية، نابلس ،١٧نيسان ٢٠١٦م.

رمضان، السيد. (٢٠٠٠). الجريمة والانحراف "رعاية الأحداث والمجرمين". دار المعرفة الجامعية، الأزاريطة، ص ٢٢.

الزنداني، ابراهيم محمد بن محمود. (٢٠١٨). الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني. [رسالة ماجستير]في قسم الدراسات الإسلامية، جامعة فطاني، تايلند ٢٠١٨، ص ٢٧.

الشكري، عادل يوسف الغني. (٢٠٠٨). الجريمة المعلوماتية وازمته الشرعية الجزائية. مجلة جامعة الكوفه ، العدد٧ ، مجلد٤،ص٩.

الشهري، البراء جمعان محمد. (٢٠٢٤). استخدامات تقنيات الذكاء الاصطناعي في مكافحة الجريمة. المجلة العربية للنشر العلمي، الإصدار السابع – العدد ثمانية وستون ، تاريخ الإصدار ٢ حزيران – ٢٠٢٤ م.صص٧٣- ٩٢.

الشوايكة، محمد أمين. (٢٠١٤). جرائم الحاسوب والانترنت. طبعه٤، دار الثقافة، عمان ،٢٠١٤،ص١٠٥.

صالح، ياسمين أحمد اسماعيل. (٢٠٢١). الارهاب الالكتروني في ظل أزمة كورونا، الأنماط – التداعيات. مجلة السياسة والاقتصاد، كلية السياسة والاقتصاد، جامعة بني سويف.

طالة، لامية وسلام، كهينة. (٢٠٢٠). الجريمة الإلكترونية: بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي. مجلة الرواق للدراسات الاجتماعية والإنسانية، المجلد٦، العدد٢ ، ص٨٦-٨٨.

عبابنة، محمود أحمد. (٢٠٠٤). جرائم الحاسوب وابعادها الدولية. دار الثقافة .عمان طبعة ١، لسنة ٢٠٠٤، ص٣١.

العجمي، عبد الله دغش. (٢٠١٤). المشكلات العملية والقانونية للجرائم الالكترونية ومايليها (دراسة مقارنة). [رسالة ماجستير]، جامعة الشرق الاوسط ٢٠١٤م،ص٢٠.

فريحة، حسين. (٢٠١١). *الجرائم الالكترونية والانترنت*. بحوث ومقالات، المعلوماتية السعودية ، متاح علي الرابط http://scord.m . andumah.com /Revord/122156

حسين، فريجه و بهاء الدين، فريجه رمزي. (د.ت). حماية المرفق العام من الجريمة الإلكترونية. (متاح بالموقع).

فكري، أيمن عبد الله. (٢٠١٤). *الجرائم المعلوماتية، دراسة مقارنة في التشريعات العربية والأجنبية*. مكتبة القانون والاقتصاد، الرياض.

القحطاني، مداوي سعيد مداوي. (٢٠١٦). *الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها* . وزارة الداخلية، قطر، الرياض، مجلس التعاون لدول الخليج العربية، الأمانة العامة، ص١٢٨.

كاظم، علي باسم. (٢٠١٨). *جريمة انتهاك مراسلات البريد الالكتروني (الجريمة الالكترونية)*. بحث كجزء من متطلبات نيل شهادة البكالوريوس في القانون كلية القانون جامعة القادسية.

الكعبي، منصور ناصر منصور حمد. (٢٠٢٠). أثر تكنولوجيا المعلومات علي ظهور الجرائم الالكترونية. دراسة ميدانية بإمارة أبو ظبي ، [رسالة دكتوراه غير منشورة] ، كلية الآداب ، قسم علم اجتماع ، جامعة المنصورة.

لطفي، خالد حسن أحمد. (٢٠١٩). *الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية*. دار الفكر الجامعي، الاسكندرية، ص٢٥.

معتوق، نورا بخيت عبد الرحيم.(٢٠٢١). *الجرائم الالكترونية ومخاطرها على الشباب الجامعي*. كلية الخدمة الاجتماعية، جامعة أسيوط.

معروف، كريم. (٢٠١٩). الأضرار الناجمة عن المخاطر الإجرامية في الجرائم المعلوماتية. *مجلة الدراسات الإستراتيجية للكوارث وإدارة الفرص*، المجلد الأول ، العدد الأول، مايو٢٠١٩، المركز الديمقراطي العربي، برلين.

الملط، أحمد خليفة. (٢٠٠٥). *الجرائم المعلوماتية وما بعدها* . دار الفكر الجامعي، الأسكندرية ، ٢٠٠٥ ص ١١٣.

مي العبد الله. (٢٠١٤). *المعجم في المفاهيم الحديثة للإعلام والاتصال، المشروع العربي لتوحيد المصطلحات*. ط١، دار النهضة العربية، بيروت، لبنان، ٢٠١٤، ص ١٣٩.

نظمي، كرستينا لطيف. (٢٠١٩). أنماط الجرائم الالكترونية المرتكبة ضد الإناث. [رسالة ماجستير غير منشورة] كلية الآداب والعلوم الانسانية ، قسم علم الاجتماع ، جامعة قناة السويس.

هانية، بوشارب. (٢٠٢٤). معوقات مكافحة الجريمة الإلكترونية على المستوى الوطني. كلية الحقوق والعلوم السياسية جامعة غرداية مخبر السياحة، الإقليم والمؤسسات.

يوسف. (٢٠٢٤). متاح في الموقع https://easylaweg.com. آخر تحديث: سبتمبر ٢٦/ ٩/ ٢٠٢٤ . جميع الحقوق محفوظة @ قوانين بلا تعقيد ٢٠٢٤.

المراجع الأجنبية ومواقع الكترونية:

البرنامج الوطني للذكاء الاصطناعي بدولة الإمارات العربية المتحدة https://ai.gov.ae/ar/about-us-ar.

جهود الدولة التشريعية والتنفيذية لمواجهة الجرائم الإلكترونية.(٢٠٢٢). واقع الجرائم الإلكترونية وتداعياتها على المجتمع المصري. (متاح بالموقع،https://draya-eg.org/2022/04/13/ ١٣/٠٤/٢٠٢٢).

https://www.qaafe.net/the-role-of-public-security-in-combating-cybercrime-through-social-networks. **الحمدان، سمية بنت عبدالرحمن بن سليمان**

Jackson, Jennifer T.(2017) A biodiversity approach to cyber security, Thesis (Ph.D.), University of Warwick , available at , https://ethos.bl.uk/OrderDetails.

https://draya-eg.org/2022/04/13 . .

https://easylaweg.com, 26/ 9/ 2024.

https://doi.org/.

References

Ibrahim, Khaled Mamdouh. (2008). Cybercrime Security. University Press, Alexandria, p. 7.

Baghdadi, Adham Basem Nimr. (2018). Methods of Investigating and Detecting Cybercrimes, Master of Public Law Thesis. Faculty of Graduate Studies, An-Najah National University, Nablus, Palestine, pp. 11-12.

Bahaa El-Din, Hussein Kamel (2003). Crossroads. Dar Al-Maaref, Cairo, p. 55.

Al-Bayouk, Hussein Salim. (2021). Legal Protection of Credit Cards from the Risk of Cyber Piracy. [Unpublished Doctoral Dissertation], Faculty of Law, Department of Commercial and Maritime Law, Ain Shams University.

Al-Habsi, Issa Abdullah Issa. (2021). Email Crimes: A Comparative Study. [Unpublished Doctoral Dissertation], Faculty of Law, Department of Criminal Law, Mansoura University.

Khneifer, Shafika. (n.d.). Cybercrime: Lost Talents in the World of Technology. A research paper presented at the First Virtual Scientific Conference: Cybercrime (Reality and Repercussions), Mohamed Cherif Messaadia University, Souk Ahras, Algeria.

Rabai'a, Abdel Latif Mahmoud. (2016). Cybercrimes (Criminalization, Prosecution, and Evidence). A research paper presented at the First Conference on Cybercrimes in Palestine, held at An-Najah National University, Nablus, April 17, 2016.

Ramadan, Al-Sayed. (2000). Crime and Deviance: "The Care of Juveniles and Offenders." University Knowledge House, Azarita, p. 22.

Al-Zindani, Ibrahim Muhammad bin Mahmoud. (2018). Cybercrimes from the Perspective of Islamic Law and its Rulings in Qatari and Yemeni Law. [Master's Thesis], Department of Islamic Studies, Fatoni University, Thailand, 2018, p. 27.

Al-Shukri, Adel Yousef Al-Ghani. (2008). Information Crime and its Legal and Criminal Crisis. Journal of the University of Kufa, Issue 7, Volume 4, p. 9.

Al-Shahri, Al-Baraa Jumaan Muhammad. (2024). The Uses of Artificial Intelligence Technologies in Combating Crime. Arab Journal of Scientific Publishing, Issue 7, No. 68, June 2, 2024, pp. 73-92.

Al-Shawaika, Muhammad Amin. (2014). Computer and Internet Crimes. 4th Edition, Dar Al-Thaqafa, Amman, 2014, p. 105.

Saleh, Yasmin Ahmed Ismail. (2021). Cyberterrorism in Light of the Coronavirus Crisis: Patterns and Repercussions. Journal of Politics and Economics, Faculty of Politics and Economics, Beni Suef University.

Tala, Lamia and Salam, Kahina. (2020). Cybercrime: A New Dimension of the Concept of Crime Across Social Media Platforms. Al-Riwaq Journal for Social and Human Studies, Volume 6, No. 2, pp. 86-88.

Ababneh, Mahmoud Ahmed. (2004). Computer Crimes and Their International Dimensions. Dar Al-Thaqafa, Amman, 1st Edition, 2004, p. 31.

Al-Ajami, Abdullah Daghash. (2014). The Practical and Legal Problems of Cybercrimes and Related Issues (A Comparative Study). [Master's Thesis], Middle East University, 2014, p. 20.

Fariha, Hussein. (2011). Cybercrimes and the Internet. Research and Articles, Saudi Informatics, available at http://scord.mandumah.com/Revord/122156

Hussein, Fariha and Bahaa El-Din, Fariha Ramzi. (n.d.). Protecting Public Facilities from Cybercrime. (Available online).

Fikri, Ayman Abdullah. (2014). Information Crimes: A Comparative Study of Arab and Foreign Legislations. Law and Economics Library, Riyadh.

Al-Qahtani, Madawi Saeed Madawi. (2016). Cybercrime in Gulf Society and How to Confront It. Ministry of Interior, Qatar, Riyadh, Cooperation Council for the Arab States of the Gulf, General Secretariat, p. 128.

Kazim, Ali Basem. (2018). The Crime of Violating Email Communications (Cybercrime). Research submitted as part of the requirements for a Bachelor of Laws degree, College of Law, Al-Qadisiyah University.

Al-Kaabi, Mansour Nasser Mansour Hamad. (2020). The Impact of Information Technology on the Emergence of Cybercrimes: A Field Study in the Emirate of Abu Dhabi. [Unpublished PhD Dissertation], Faculty of Arts, Department of Sociology, Mansoura University.

Lotfi, Khaled Hassan Ahmed. (2019). Digital Evidence and its Role in Proving Cybercrime. Dar Al-Fikr Al-Jami'i, Alexandria, p. 25.

Maatouq, Noura Bakheet Abdel Rahim. (2021). Cybercrimes and their Dangers to University Students. Faculty of Social Work, Assiut University.

Ma'rouf, Karim. (2019). Damages Resulting from Criminal Risks in Cybercrimes. Journal of Strategic Studies for Disasters and Opportunity Management, Volume 1, Issue 1, May 2019, Arab Democratic Center, Berlin.

Al-Malt, Ahmed Khalifa. (2005). Cybercrimes and Beyond. Dar Al-Fikr Al-Jami'i, Alexandria, 2005, p. 113.

Mai Al-Abdullah. (2014). Dictionary of Modern Media and Communication Concepts, Arab Project for Terminology Unification. 1st ed., Dar Al-Nahda Al-Arabiya, Beirut, Lebanon, 2014, p. 139.

Nazmi, Christina Latif. (2019). Patterns of Cybercrimes Committed Against Women. [Unpublished Master's Thesis] Faculty of Arts and Humanities, Department of Sociology, Suez Canal University.

Hania, Bouchareb. (2024). Obstacles to Combating Cybercrime at the National Level. Faculty of Law and Political Science, University of Ghardaia, Laboratory of Tourism, Region and Institutions.

Youssef. (2024). Available at https://easylaweg.com. Last updated: September 26, 2024. All rights reserved © Easy Laws 2024.