Arabian Gulf Journal of Humanities and Social Studies

ISSN: 3080-4086

الإصدار الخامس - العدد االثالث عشر || تاريخ الإصدار 2026-04-20

الجرائم الإلكترونية (التحديات وسبل مواجهتها)

Cybercrimes (Challenges and ways to Confront them)

الدكتور ليث إبراهيم الزواهـرة[1]– حسـام أحمـد أبو حمـــــور[2]

Hussam Ahmad Abu Hammour - Dr. Laith Ibrahim Alzawahreh

المملكة الأردنية الهاشمية

DOI: https://doi.org/10.64355/agjhss5136

الملخص:
تناول البحث مفهوم الجرائم الإلكترونية وخصائصها التي تميزها عن غيرها من الجرائم، كالعالمية، والسرعة، وصعوبة التتبع، وما يترتب على ذلك من تعقيدات في الإثبات والتحقيق.

وجرى التطرق إلى الأبعاد القانونية والتشريعية، حيث تبين وجود تفاوت في تعريف الجريمة الإلكترونية من دولة لأخرى، إضافة إلى قصور بعض التشريعات الوطنية في مواجهة هذا النوع المتجدد من الجرائم. كما أُشير إلى الجهود الدولية والإقليمية المبذولة عبر الاتفاقيات والمعاهدات، مثل اتفاقية بودابست، في محاولة لتوحيد الإطار القانوني لمكافحة هذه الجرائم.

أما من الناحية الإجرائية، فقد استعرض البحث دور الأجهزة الأمنية والقضائية في ملاحقة الجرائم الإلكترونية، والتحديات المرتبطة بجمع الأدلة الرقمية وحفظها وتحليلها. وتم التركيز على أن الدليل الرقمي يمثل محورًا أساسيًا في الإثبات، لما يتمتع به من خصائص مميزة، لكنه يواجه عدة صعوبات، منها هشاشته وقابليته للتغيير أو الإتلاف، بالإضافة إلى تعقيدات تقنية مثل التشفير والأنظمة المجهولة

كما تناول البحث الإطار المؤسسي لمكافحة الجرائم الإلكترونية، مبرزًا دور الوحدات المتخصصة لدى الأجهزة الأمنية، وأهمية الشراكة مع القطاع الخاص والمجتمع المدني في التوعية وبناء القدرات.

وفي الختام، خلصت الفصول السابقة إلى أن الجرائم الإلكترونية لم تعد مجرد سلوك إجرامي فردي، بل هي ظاهرة عالمية مركبة تحتاج إلى مقاربة شمولية تجمع بين التشريع الفعّال، والإجراءات الأمنية المتقدمة، والتعاون الدولي، إضافة إلى بناء كفاءات بشرية قادرة على التعامل مع الدليل الرقمي ومواجهة التحديات التقنية والقانونية.

الكلمات المفتاحية: الجرائم الإلكترونية.

Abstract:

The research addressed the concept of cybercrime and its distinctive characteristics that set it apart from other types of crimes, such as its global nature, speed, difficulty in tracing, and the resulting complexities in evidence and investigation.

It also touched on the legal and legislative dimensions, highlighting the differences in the definition of cybercrime from one country to another, in addition to the shortcomings of some national legislations in dealing with this evolving type of crime. Reference was made to international and regional efforts through agreements and treaties, such as the Budapest Convention, in an attempt to unify the legal framework for combating these crimes.

From a procedural perspective, the research reviewed the role of security and judicial authorities in pursuing cybercrimes, along with the challenges related to collecting, preserving, and analysing digital evidence. Emphasis was placed on digital evidence as a central element in proof due to its distinctive characteristics, yet it faces several difficulties, including its fragility and susceptibility to alteration or destruction, as well as technical complexities such as encryption and anonymous systems.

The research also examined the institutional framework for combating cybercrime, highlighting the role of specialized units within security agencies, and the importance of partnerships with the private sector and civil society in awareness-raising and capacity building.

In conclusion, the previous chapters found that cybercrime is no longer merely an individual criminal act but a complex global phenomenon requiring a comprehensive approach that combines effective legislation, advanced

security procedures, international cooperation, and the development of human capacities capable of handling digital evidence and addressing technical and legal challenges.

Keywords: Cyber Crimes.

قائمة الاختصارات	
ITU	International Telecommunication Union (الاتحاد الدولي للاتصالات).
OECD	Organisation for Economic Co-operation and Development (منظمة التعاون الاقتصادي والتنمية).
DOJ	U.S. Department of Justice (وزارة العدل الأمريكية).
COE	Council of Europe (مجلس أوروبا).
DDOS	Distributed Denial of Service (هجوم حجب الخدمة الموزّع)
VPN	Virtual Private Network (الشبكة الخاصة الافتراضية)

المقدمة

في عصر تكنولوجيا المعلومات والاتصالات، أصبحت الجرائم الإلكترونية واحدة من أكبر التحديات التي تواجه الأفراد، المؤسسات، والدول على حد سواء؛ وتتمثل الجرائم الإلكترونية بالأنشطة غير القانونية التي تتم عبر الشبكات الرقمية، بما في ذلك الإنترنت، باستخدام تقنيات متقدمة للتسلل إلى الأنظمة الرقمية، سرقة البيانات، اختراق الخصوصية، والابتزاز، وفي حين كانت الجرائم التقليدية تقتصر في الماضي على الأنشطة المادية مثل السرقة أو الاعتداءات الجسدية، فقد تطورت الأنماط الإجرامية في ظل الثورة الرقمية لتشمل الأفعال التي تتم عن بُعد عبر الفضاء السيبراني، مما يوسع نطاق الأضرار ويزيد من صعوبة ملاحقة مرتكبي هذه الجرائم (سلامة، نسرين، 2023).

وفي السنوات الأخيرة، شهدت الجرائم الإلكترونية ارتفاعًا كبيرًا في تأثيراتها السلبية على الأفراد. أحد أخطر الأنواع التي يعاني منها الأفراد هو الاحتيال الإلكتروني، الذي يتم من خلاله خداع الضحايا للحصول على معلوماتهم الشخصية أو المالية. يشمل الاحتيال الإلكتروني العديد من الأساليب مثل التصيد الاحتيالي، وهو عندما يتلقى الفرد رسالة بريد إلكتروني مزيفة تبدو وكأنها من مؤسسة موثوقة، تطلب منه تقديم معلومات شخصية أو مالية. يمكن أن تؤدي هذه الأنواع من الجرائم إلى خسائر مالية ضخمة للأفراد المتأثرين، ولا سيما في حالات سرقة الهوية أو فقدان الأموال نتيجة الاحتيال، إضافة إلى ذلك، تواجه الأفراد خطر الابتزاز الإلكتروني، حيث يستخدم المجرمون صورًا أو معلومات خاصة بالضحايا في محاولة للضغط عليهم مقابل المال أو غيره من المكاسب؛ وتعد هذه الجرائم من أكثر الجرائم الإلكترونية تأثيرًا نفسيًا على الأفراد. يشعر الكثير من الضحايا بالإهانة والخوف من فقدان سمعتهم أو تعرضهم للمزيد من الأذى. قد تتسبب هذه الأنواع من الجرائم في انهيار العلاقات الشخصية، بالإضافة إلى تأثيرات نفسية خطيرة مثل القلق والاكتئاب؛ حيث أن واحد من التأثيرات الأخرى للجرائم الإلكترونية على الأفراد هو التأثير على الخصوصية. في عالم يتزايد فيه الاعتماد على الإنترنت لتخزين البيانات الشخصية، تصبح هذه المعلومات عرضة للسرقة من قبل المهاجمين، قد يتسبب ذلك في انتهاك حاد لحقوق الأفراد، خاصة في حالات تسريب المعلومات الحساسة مثل السجلات الطبية أو التفاصيل المالية. مع تزايد عدد الأفراد الذين يتعاملون مع الشركات والمؤسسات عبر الإنترنت، يتزايد خطر وقوعهم ضحية لهذا النوع من الجرائم (Goni O, 2022).

إلى جانب الأفراد، تواجه المؤسسات تحديات كبيرة بسبب الجرائم الإلكترونية. يتم استهداف الشركات الكبرى بطرق متنوعة من قبل المهاجمين، سواء بهدف السرقة التجارية أو الابتزاز. الهجمات الإلكترونية يمكن أن تؤدي إلى فقدان بيانات حساسة مثل أسرار الأعمال أو المعلومات المالية. في بعض الأحيان، يمكن أن تتسبب هذه الهجمات في تعطيل الخدمات، مثل هجمات الرفض الموزع للخدمة (DDoS)التي تهدف إلى تعطيل المواقع الإلكترونية أو الشبكات الداخلية للمؤسسات (Shafik, W, 2024).

وتشير التقارير الدولية إلى أن الجرائم الإلكترونية تشهد نموًا متسارعًا، مما يعكس حجم التهديد الذي تشكله على مستوى العالم. وفقًا لتقرير صادر عن الاتحاد الدولي للاتصالات (ITU)، يتعرض أكثر من (70%) من الشركات في العالم لهجمات إلكترونية سنويًا، كما أن الأنشطة الإجرامية التي ترتكب عبر الإنترنت تضر باقتصاديات الدول بشكل كبير. على سبيل المثال، تُقدّر الخسائر المالية الناتجة عن الجرائم الإلكترونية في الولايات المتحدة وحدها بمليارات الدولارات سنويًا، بينما تشير التوقعات إلى أن هذا الرقم سيزداد بشكل كبير مع استمرار تطور التكنولوجيا وانتشارها على مستوى العالم؛ ومن الناحية الأمنية، تُعتبر الجرائم الإلكترونية تهديدًا حقيقيًا للأمن الوطني والعالمي. في الواقع، يواجه العالم تحديات متزايدة في مكافحة الجرائم التي تتراوح من الهجمات الإلكترونية السياسية إلى الأنشطة الإرهابية الرقمية. من بين هذه الأنشطة، تتزايد المخاوف من هجمات الفدية التي تؤثر على المؤسسات الحكومية أو الشركات الكبرى(Wall, D. S. 2024) .

مشكلة البحث

تعد الجرائم الإلكترونية من المشكلات الكبيرة والمعقدة التي تواجهها المجتمعات الحديثة في ظل الانتشار الواسع للتكنولوجيا حيث أن ما يزيد من تعقيدها وصعوبة مواجهتها أنها غالباً ما تتم عبر الإنترنت، مما يمكن المجرم تنفيذها من أي مكان في العالم، مما يعقد عملية التحقيق والملاحقة القانونية، بالإضافة إلى ذلك، فإن العديد من هذه الجرائم تتسم بالسرية العالية، مما يجعل اكتشافها والتحقيق فيها أمرًا صعبًا للغاية على سبيل المثال، لا يتطلب الأمر من المجرم أن يكون موجودًا فعليًا في المكان الذي تحدث فيه الجريمة. فالمهاجمون قد يكونون في أي بقعة من الأرض، ويمكنهم استهداف أفراد أو مؤسسات في دول مختلفة دون أن يتركوا آثارًا ملموسة.

المشكلة الأخرى التي تبرز في الجرائم الإلكترونية هي الطبيعة المتطورة والمتغيرة لهذه الجرائم. مع تقدم التكنولوجيا، تظهر أنماط جديدة من الجرائم الإلكترونية التي قد تكون مجهولة أو غير مفهومة للأجهزة الأمنية أو للمشرعين. تتراوح هذه الجرائم من الاحتيال الإلكتروني، إلى الهجمات السيبرانية المعقدة، إلى الهجمات التي تستهدف البنية التحتية الحيوية مثل المستشفيات أو شبكات الطاقة، هذه الأنماط الجديدة تتطلب استراتيجيات استباقية لمكافحتها، بالإضافة إلى قوانين حديثة تسهم في محاكمة مرتكبيها وتقديمهم إلى العدالة.

أسئلة البحث

1. ماهية الجرائم الإلكترونية المختلفة؟ وما هي أسباب انتشار الجرائم الإلكترونية في العصر الرقمي؟ وكيفية تأثيرها على الأفراد والمجتمعات؟
2. ما هي الإجراءات القانونية المتخذة لمكافحة الجرائم الإلكترونية؟
3. ما هو واقع حال الجرائم الإلكترونية في المملكة الأردنية الهاشمية؟ وما هو دور مديرية الأمن العام في مواجهة الجرائم الإلكترونية؟
4. كيف يمكن تعزيز الوعي العام حول مخاطر الجرائم الإلكترونية وسبل الوقاية منها؟

أهداف البحث

1. تهدف هذه الدراسة لتناول مفهوم الجرائم الإلكترونية وأثرها على الأفراد والمجتمعات وتحليل الأنواع المختلفة للجرائم الإلكترونية مثل القرصنة، الاحتيال الإلكتروني، والابتزاز عبر الإنترنت وتحديد الأسباب الرئيسية التي تؤدي إلى انتشار الجرائم الإلكترونية.
2. تهدف هذه الدراسة لتناول الإطار القانوني والتشريعي لمكافحة الجرائم الإلكترونية في الدول المختلفة.
3. تهدف هذه الدراسة للتعرف على دور مديرية الأمن العام في مواجهة الجرائم الإلكترونية.
4. تهدف هذه الدراسة لتقديم استراتيجيات وحلول للحد من انتشار الجرائم الإلكترونية وتحقيق الأمن السيبراني.

منهجية الدراسة:

تم استخدام المنهج الوصفي وهو أحد المناهج البحثية التي تهدف إلى وصف الظواهر أو الظواهر الاجتماعية أو العلمية دون التدخل في التسبب بها أو تعديلها. يستخدم هذا المنهج لتحليل الحالة الراهنة أو الوضع القائم لفهم خصائص الظاهرة المدروسة؛ والهدف الرئيسي من المنهج الوصفي هو تقديم صورة واضحة ومفصلة عن الموضوع محل الدراسة من خلال جمع البيانات والحقائق المتعلقة به وتحليلها.

حدود الدراسة:

الحدود الموضوعية: الجرائم الإلكترونية بين التحديات وطرق مواجهتها.

الحدود المكانية: المملكة الأردنية الهاشمية.

الحدود الزمانية: 2023-2024.

أهمية البحث

تكمن أهمية البحث في تسليط الضوء على ظاهرة الجرائم الإلكترونية التي تؤثر بشكل مباشر على الاقتصاد الرقمي والأمن الشخصي والعام. كما يهدف إلى رفع الوعي حول أهمية تبني تدابير وقائية من قبل الأفراد والمؤسسات، وكذلك الحاجة إلى تطوير التشريعات الوطنية والدولية للتعامل مع هذه الجرائم بشكل فعال.

الدراسات السابقة

أولاً: الدراسات العربية

1. سلامة، نسرين سيد. (2023). الجرائم الإلكترونية وأثرها على المجتمع .

هدفت الدراسة لتناول تطورت الظاهرة الإجرامية في العصر الحديث تطوراً ملحوظاً ومذهلاً سواء في أشخاص مرتكبيها أو في أسلوب ارتكابها والذي يتمثل في استخدام أخر م توصلت إليه العلوم التقنية والتكنولوجية وتطويعها في خدمة الجريمة. وقد تميز القرن العشرين باختراعات هائلة على المستوي التقني لعل من أهمها ظهور الحاسبات الإلكترونية تسعي الدراسة الحالية إلى تحديد دور الجرائم الإلكترونية وأثرها على المجتمع.، وهي من البحوث الوصفية التحليلية، وتحاول الإجابة على تساؤل رئيس مؤداه " التعرف على أثر الجرائم الإلكترونية على المجتمع المصري؟، واستهدف البحث تحديد الوسائل والأساليب التي تستخدمها الدولة والمؤسسات في موجهه الجرائم الإلكترونية على المجتمع , وتحديد الآليات التي تستخدمها منظمات الدولة في حمايه المجتمع من الجرائم الإلكترونية, وتحديد دور المجتمع في مواجهه الجرائم الإلكترونية, وتحديد المعوقات التي تواجه المنظمات والتي تحد من الاستفادة من برامج توعيه المجتمع التي تقدمها تلك المنظمات للمجتمع, والتوصل إلى اهم أساليب للحد من الجرائم الإلكترونية بالمجتمع وكيفيه الاستفادة منه.

2. بن عمروش، فريدة، جاب الله، حكيمة. (2023). الجريمة الإلكترونية: المفهوم، الأشكال والآليات.

هدفت الدراسة لإبراز معالم الجريمة الإلكترونية بمفاهيمها المختلفة باعتبارها ظاهرة جديدة أوجدها التطور التكنولوجي نتيجة الاستخدام الكبير لهذه التكنولوجيات وتوفر الإنترنت، وقد تعددت الآراء في ضبط مفهوم الجريمة الإلكترونية باختلاف الآراء والتشريعات. والجريمة الإلكترونية تختلف عن الجرائم التقليدية لأنها ترتكب في البيئة الرقمية كما تتم باستخدام التقنيات الحديثة وهي سلوك غير مشروع تعددت أشكاله بتعدد الأهداف وتعدد الآليات المعتمدة، نتيجة تعدد البرمجيات المستخدمة وتطورها المستمر نتيجة تسارع التطور التكنولوجي.

3. المطيري، سعد فهد سعد ادبيس. (2023). مفهوم الجرائم الإلكترونية وسماتها

هدفت الدراسة لتناول واحدة من أهم القضايا التي تقلق رجال الفكر القانوني في الوقت الحاضر تلك هي الجريمة الإلكترونية فاتساع استخدام الحاسوب وما تبعه من استخدام الشبكة الدولية (الإنترنت) وما نجم عنه من أنماط جديدة للسلوك الإجرامي لم يكن يتوقعه المشرع في معظم بلدان العالم. الأمر الذي دفع بالدول إلى الوقوف وقفة جادة لمعالجة هذه المشكلة. فقد خلف هذا التطور التكنولوجي العديد من المخاطر والأضرار لا سيما وضعف الرقابة عليها أدي إلى ظهور هذا النوع الجديد من الجرائم المتطورة والتي تختلف عن سابقتها من حيث طريقة وأسلوب ارتكابها، وشكل وصفات المجرم وطباعة سميت بالجرائم الإلكترونية، وأصبحت تمثل تهديدا مباشرا وواضحا للأمن والاستقرار المحلي والعالمي، وعائقا يحول دون إتمام عملية التطوير والتنمية الاقتصادية والأمنية. وإزاء ذلك سعت العديد من الدول إلى تطوير نظمها التشريعية بإدخال نصوص وتشريعات عقابية وإجرائية تتوافق مع ظاهرة الإجرام التقني الحديثة عبر الإنترنت التي هي من الجرائم التي تتخطى حدود الدولة الواحدة وتدخل كذلك في عداد الجريمة المنظمة التي تقوم على أساس تنظيم هيكلي وتدرجي له صفة الاستمرارية لتحقيق مكاسب طائلة. لذلك تناول البحث التعريف بالجرائم الإلكترونية ومحاولة الإحاطة بجوانبها الفنية والتقنية، وتحديد ماهية الجرائم التي تثيرها هذه التكنولوجيا وطبيعتها وموضوعها وصورها المختلفة، ومعرفة خصائصها وسمات مرتكبيها وأركانها والإشكال التي يطرحها ركنها الشرعي.

ثانياً: الدراسات الأجنبية

1. Goni, O., Ali, M. H., Showrov, (2022). The basic concept of cybercrime.

هدفت الدراسة لتناول الجريمة الإلكترونية واعتبارها ظاهرة شائعة في العالم. الجريمة الإلكترونية هي مجموعة من الأنشطة التي يقوم بها الأشخاص من خلال إحداث اضطراب في الشبكة، وسرقة البيانات والمعلومات الهامة والخاصة للآخرين، واختراق تفاصيل الحسابات البنكية وتحويل الأموال إلى حساباتهم الخاصة. الجريمة الإلكترونية، خاصة عبر الإنترنت، قد زادت أهميتها مع تحول الكمبيوتر إلى محور التجارة والترفيه والحكومة. الجريمة الإلكترونية، التي تُسمى أيضًا جريمة الكمبيوتر، هي استخدام الكمبيوتر كأداة لتحقيق أغراض غير قانونية، مثل ارتكاب الاحتيال، والاتجار في المواد الإباحية للأطفال والملكية الفكرية، وسرقة الهويات، أو انتهاك الخصوصية. الجريمة الإلكترونية وتأثيراتها على المجتمع في شكل اضطراب اقتصادي، اضطراب نفسي، تهديد للأمن الوطني، إلخ. تقييد الجرائم الإلكترونية يعتمد على التحليل الصحيح لسلوكها وفهم تأثيراتها على مختلف مستويات المجتمع. في الوقت الحاضر، تزداد الجرائم الإلكترونية يوماً بعد يوم. لقد عانى الناس كثيرًا بسبب ذلك. إنه لا يسبب المعاناة البشرية فحسب، بل يؤثر عليها أيضًا. لذا فإن الجرائم الإلكترونية هي واحدة من الجرائم الرئيسية التي يرتكبها خبراء الكمبيوتر. تقدم هذه الورقة المفهوم الأساسي للجريمة الإلكترونية.

2. Goni, O. (2022). Cybercrime and its classification.

هدفت الدراسة لتناول الجريمة الإلكترونية وهي ظاهرة شائعة في العالم. الجريمة الإلكترونية هي تلك المجموعة من الأنشطة التي يقوم بها الأشخاص من خلال إحداث اضطراب في الشبكة، وسرقة البيانات والمعلومات الهامة والخاصة للآخرين، واختراق تفاصيل الحسابات البنكية وتحويل الأموال إلى حساباتهم الخاصة. الجريمة الإلكترونية، وخاصة عبر الإنترنت، قد زادت أهميتها مع تحول الكمبيوتر إلى محور التجارة والترفيه والحكومة. الجريمة الإلكترونية، التي تُسمى أيضًا جريمة الكمبيوتر، هي استخدام الكمبيوتر كأداة لتحقيق أغراض غير قانونية، مثل ارتكاب الاحتيال، والاتجار في المواد الإباحية للأطفال والملكية الفكرية، وسرقة الهويات، أو انتهاك الخصوصية. الجريمة الإلكترونية وتأثيراتها على المجتمع في شكل اضطراب اقتصادي، اضطراب نفسي، تهديد للأمن الوطني، إلخ. تقييد الجرائم الإلكترونية يعتمد على التحليل الصحيح لسلوكياتها وفهم تأثيراتها على مختلف مستويات المجتمع. في الوقت الحاضر، تزداد الجرائم الإلكترونية يومًا بعد يوم. لقد عانى الناس كثيرًا بسبب ذلك. إنه لا يسبب المعاناة البشرية فحسب، بل يؤثر أيضًا على الاقتصاد. من المستحيل حل المشاكل من قبل الحكومة وحدها. لذلك، يُعتبر الجرائم الإلكترونية واحدة من الجرائم الرئيسية التي يرتكبها خبراء الكمبيوتر.

المبحث الأول: ماهية الجرائم الإلكترونية

المطلب الأول: تعريف الجرائم الإلكترونية وأنواعها وأسباب انتشارها وآثارها

تُعتبر الجرائم الإلكترونية من أبرز التحديات التي تواجه العالم في عصر الثورة الرقمية، إذ تشهد هذه الجرائم تطورًا سريعًا بفضل تقدم التكنولوجيا والإنترنت. يشير مصطلح "الجرائم الإلكترونية" إلى الأنشطة الإجرامية التي يتم تنفيذها باستخدام أجهزة الكمبيوتر أو الإنترنت كأداة رئيسية في ارتكاب الجريمة. ومن خلال هذه الأدوات الرقمية، يتمكن الجناة من تنفيذ مجموعة واسعة من الأفعال غير القانونية التي قد تشمل، على سبيل المثال، اختراق البيانات، الاحتيال المالي، الهجمات السيبرانية، والابتزاز الإلكتروني. يتطلب التعامل مع هذه الجرائم إطارًا قانونيًا وتكنولوجيًا متقدمًا يتماشى مع التطور السريع في أساليب الجريمة الإلكترونية.

أولاً: تعريف الجرائم الإلكترونية

- الجرائم الإلكترونية، وفقًا لمنظمة (OECD) هي "الأنشطة التي تتم باستخدام تكنولوجيا المعلومات والاتصالات كوسيلة لارتكاب جريمة أو لتنفيذها" (OECD 2020,) يشمل هذا التعريف مجموعة واسعة من الجرائم مثل القرصنة الإلكترونية، التسلل إلى أنظمة الكمبيوتر، والتسلل إلى المعلومات الحساسة.
- يعرف ألمركز الوطني للأمن السيبراني الأردني الجرائم الإلكترونية بأنها "الأنشطة الإجرامية التي تُنفذ بواسطة أجهزة الكمبيوتر أو عبر الشبكة العالمية (الإنترنت)، وتشمل مجموعة من الجرائم مثل السرقة الرقمية، الابتزاز الإلكتروني، الاحتيال الرقمي، وكذلك الهجمات على أنظمة الحماية الإلكترونية للمؤسسات" (المركز الوطني الأردني للأمن السيبراني)، هذا التعريف يعكس التحديات التي يواجهها الأمن الوطني في ظل تزايد الجرائم الإلكترونية التي تستهدف المؤسسات الحيوية في المملكة.
- يعرف المطيري الجرائم الإلكترونية بأنها "الأنشطة غير القانونية التي تتم باستخدام التكنولوجيا الرقمية والتي تتسبب في أضرار للأفراد أو المؤسسات أو الأنظمة، من خلال التلاعب بالمعلومات، التسلل إلى الأنظمة، أو استخدام الإنترنت بطرق غير مشروعة" (المطيري،

2023). يشمل هذا التعريف الجرائم التي تُنفذ بهدف تحقيق مكاسب مالية غير مشروعة، مثل الاحتيال الإلكتروني، أو تلك التي تهدد الأمن الشخصي للمواطنين مثل الابتزاز الإلكتروني.

- ويرى الباحثان أن الجرائم الإلكترونية هي الأنشطة غير القانونية التي تُرتكب باستخدام تكنولوجيا المعلومات والاتصالات، حيث يتم استغلال الأنظمة الرقمية أو الإنترنت كأداة لارتكاب الأفعال الإجرامية التي تتسبب في أضرار للأفراد، المؤسسات أو الحكومات. تتضمن هذه الجرائم مجموعة واسعة من الأنشطة مثل اختراق البيانات الشخصية أو المؤسسية، الاحتيال المالي الرقمي، الابتزاز الإلكتروني، الهجمات السيبرانية المنظمة، إضافة إلى استخدام البرمجيات الخبيثة أو الفيروسات لتحقيق مكاسب غير مشروعة أو إلحاق ضرر بالأمن المعلوماتي. تختلف الجرائم الإلكترونية في طبيعتها وأهدافها، حيث يمكن أن تشمل التلاعب بالمعلومات، تهديد الأمن الشخصي، أو تدمير الأنظمة التكنولوجية في البنية التحتية الحيوية. وتتميز الجرائم الإلكترونية بقدرتها على التسلل عبر الحدود الجغرافية بسهولة، ما يجعل مكافحتها تتطلب استراتيجيات دولية مشتركة وأطر قانونية متجددة لمواكبة التغيرات السريعة في تقنيات الاتصال.

ثانياً: أنواع الجرائم الإلكترونية

أ. **القرصنة الإلكترونية** :تشمل اختراق الأنظمة والشبكات بهدف الحصول على معلومات حساسة أو تدميرها. يقوم القراصنة بالاستفادة من الثغرات الأمنية في الأنظمة لاختراقها والسيطرة عليها.

ب. **الاحتيال الإلكتروني** :يشمل استخدام الإنترنت للحصول على الأموال أو المعلومات من الأفراد أو الشركات من خلال الخداع أو التضليل. من أبرز الأمثلة على الاحتيال الإلكتروني عمليات التصيد الاحتيالي (Phishing) والاحتيال عبر بطاقات الائتمان.

ت. **الابتزاز الإلكتروني** :يشمل تهديد الأفراد أو الشركات بنشر معلومات حساسة أو التسبب في أضرار إلكترونية إذا لم يتم دفع فدية. يتم ذلك عبر البريد الإلكتروني أو تطبيقات المراسلة أو حتى مواقع الويب الخاصة بالابتزاز.

ث. **التجسس الإلكتروني** :يتضمن سرقة البيانات أو المعلومات الحساسة من أنظمة حكومية أو شركات أو أفراد، ويشمل هذا النوع من الجرائم غالبًا التجسس الصناعي أو المخابرات.

ج. **البرمجيات الخبيثة** :(Malware) تُستخدم البرمجيات الخبيثة مثل الفيروسات، الديدان، وأحصنة طروادة لاختراق الأجهزة وأنظمة المعلومات بهدف تدمير البيانات أو سرقتها.

ثالثاً: أسباب انتشار الجرائم الإلكترونية

أ. **التطور التكنولوجي** :مع زيادة استخدام الإنترنت وتكنولوجيا المعلومات، ظهرت العديد من الفرص لارتكاب الجرائم الرقمية. تُعتبر التقنيات مثل الإنترنت، شبكات التواصل الاجتماعي، وتطبيقات الهواتف الذكية بيئة خصبة لارتكاب الجرائم الإلكترونية (بن عمروش، وآخرون 2023).

ب. **الغياب الكامل للرقابة** :كثيرًا ما تفتقر الشبكات الإلكترونية إلى الأنظمة الأمنية الكافية لحمايتها، مما يسهل على المهاجمين التسلل إلى الأنظمة من خلال الثغرات الأمنية. كما أن الوعي الأمني لدى الأفراد والمؤسسات لا يزال ضعيفًا في العديد من الحالات.

ت. **العولمة** :الإنترنت ليس له حدود جغرافية، مما يجعل من الصعب محاكمة الجناة عبر الحدود الدولية. يمكن أن يرتكب المهاجمون الجرائم من أي مكان في العالم، مما يعيق تطبيق القوانين الوطنية والدولية (Goni O,2022).

ث. **الاستغلال المالي** :كثير من الجرائم الإلكترونية تهدف إلى تحقيق مكاسب مالية، سواء عن طريق السرقة المباشرة للمال أو من خلال استغلال المعلومات المالية للأفراد والشركات (سلامة، 2023).

رابعاً: الآثار السلبية للجرائم الإلكترونية

أ. **الآثار المالية** :يعد الخطر المالي من أكثر الآثار وضوحًا، حيث قد يتسبب اختراق البيانات في سرقة أموال الشركات والأفراد أو تحميلهم خسائر مالية ضخمة نتيجة للأنشطة غير القانونية التي تتم عبر الإنترنت، وتشير بعض الدراسات إلى أن الخسائر المالية الناتجة عن الهجمات الإلكترونية تقدر بمليارات الدولارات سنويًا (عماد، بلغيث 2021).

ب. **الآثار الاجتماعية** :تعكس الجرائم الإلكترونية تهديدًا للأمان الاجتماعي من خلال تسهيل عمليات النصب والاحتيال وابتزاز الأفراد. هذه الجرائم تضر الثقة بين الأفراد وتضعف التفاعل الآمن في الفضاء الرقمي.

ت. **الآثار القانونية** :من أبرز التحديات التي تواجه الحكومات في مجال الجرائم الإلكترونية هو تطبيق قوانين فعالة لمكافحة هذه الجرائم. تتطلب هذه القوانين تشريعات دقيقة تتماشى مع التكنولوجيا المتطورة وتراعي الفوارق الدولية التي تصعب من عملية تنفيذ القانون عبر الحدود (wall, D.S,2024)

المبحث الثاني: الإجراءات القانونية المتخذة لمكافحة الجرائم الإلكترونية

المطلب الأول: الإجراءات القانونية على المستوى العالمي

في ظل تزايد الجرائم الإلكترونية على مستوى العالم، أصبح من الضروري تطوير إطار قانوني متكامل لمكافحة هذه الأنواع من الجرائم التي تمثل تهديدًا كبيرًا للأفراد، المؤسسات، والأمن القومي. وفي هذا السياق، قامت العديد من الدول بتطوير قوانين وتشريعات تهدف إلى محاربة الجرائم الإلكترونية. وسنستعرض في هذا البحث الإجراءات القانونية المتخذة لمكافحة الجرائم الإلكترونية على مستوى العالم، وكذلك الإجراءات المتبعة في المملكة الأردنية الهاشمية.

على المستوى العالمي، هناك العديد من القوانين التي تم تطويرها لمكافحة الجرائم الإلكترونية، والتي تهدف إلى تعزيز التعاون بين الدول في مواجهة هذه الجرائم، من أبرزها:

1. **قانون الجرائم الإلكترونية في الولايات المتحدة الأمريكية (CFAA)**

في الولايات المتحدة الأمريكية، يعد قانون مكافحة الجرائم الإلكترونية (CFAA) من أبرز التشريعات التي تم تبنيها لمكافحة الجرائم الإلكترونية، تم إصدار هذا القانون في عام 1986، ويشمل مجموعة من الجرائم التي ترتكب باستخدام أجهزة الكمبيوتر، كما يعاقب هذا القانون كل من يستخدم الكمبيوتر لأغراض غير قانونية، مثل الحصول على بيانات مالية أو معلومات سرية (U.S. Dp, 2020) .

2. **التعاون بين المنظمات الدولية** علاوة على الاتفاقيات الوطنية، هناك العديد من المنظمات الدولية التي تساهم في مكافحة الجرائم الإلكترونية، مثل:

الإنتربول: التي تعمل على تعزيز التعاون بين الدول في التحقيقات المتعلقة بالجرائم الإلكترونية.

ITU : الذي يقدم دعمًا تقنيًا للدول لمكافحة الجرائم الإلكترونية، ويعمل على وضع استراتيجيات للتعامل مع هذه الجرائم من خلال التقنيات الحديثة.

OECD: التي تركز على تطوير أطر سياسات دولية لمكافحة الجرائم الإلكترونية وتقديم الاستشارات الحكومية في هذا المجال.

المطلب الثاني: الإجراءات القانونية في المملكة الأردنية الهاشمية

أما على المستوى الوطني، فقد أدركت المملكة الأردنية الهاشمية التحديات المرتبطة بالجرائم الإلكترونية واتخذت مجموعة من الإجراءات القانونية التي تهدف إلى مكافحة هذه الجرائم وحماية الأمن الوطني والمجتمعي. ولتحقيق ذلك، طورت المملكة تشريعات متكاملة تشمل القوانين الوطنية والأجهزة الأمنية المختصة في مجال مكافحة الجرائم الإلكترونية.

1. قانون الجرائم الإلكترونية رقم (17) لسنة 2023م.

تم نشر قانون الجرائم الإلكترونية رقم (17) لسنة 2023 في عدد خاص من الجريدة الرسمية بتاريخ 13 آب 2023 .وبموجب المادة 2 من القانون، يبدأ سريانه بعد 30يومًا من تاريخ نشره، أي اعتبارًا من 12أيلول 2023 .

ويهدف هذا القانون في مواده والتي بلغت (18) مادة إلى مواجهة الجرائم المرتكبة عبر الوسائل الإلكترونية، مثل: نشر الأخبار الكاذبة، انتهاك الخصوصية، الابتزاز، والتشهير، وغيرها من الجرائم التي تؤثر على الأمن والسلم المجتمعي مراعياً ومواكباً لتطور وتنوع هذه الجرائم وموضحاً جميع الحالات والعقوبات التي تقع على فاعليها.

2. الأجهزة الأمنية

هناك العديد من الهيئات الأمنية التي تتولى مهمة التحقيق والتعامل مع الجرائم الإلكترونية في الأردن، مثل وحدة مكافحة الجرائم الإلكترونية التابعة لمديرية الأمن العام الأردني. تقوم هذه الوحدة بدور كبير في جمع المعلومات، التحقيق في الحوادث، والتعاون مع الجهات الدولية لمكافحة الجرائم

الإلكترونية. وتشمل مهام الوحدة مكافحة جميع أنواع الجرائم الإلكترونية مثل التسلل إلى الأنظمة الرقمية، الاحتيال الإلكتروني، والتشهير عبر الإنترنت.

3. المركز الوطني للأمن السيبراني

تأسس المركز الوطني للأمن السيبراني في الأردن لتعزيز جهود مكافحة الجرائم الإلكترونية وحماية البنية التحتية الرقمية في المملكة. يعد المركز نقطة محورية في تنظيم وتنسيق جهود الدولة لمكافحة الهجمات الإلكترونية، ويقوم بتوفير التدريب والتوعية حول كيفية التصدي لهذه الجرائم. كما يعمل المركز على تطوير استراتيجيات لمكافحة الهجمات السيبرانية وحماية المؤسسات الوطنية من التهديدات الرقمية (المركز الوطني للأمن السيبراني).

4. تعاون الأردن مع المنظمات الدولية

تحرص المملكة الأردنية على تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، حيث تشارك في الاتفاقيات الدولية مثل اتفاقية بودابست وتنسق مع منظمة الإنتربول والاتحاد الدولي للاتصالات لتحقيق الأهداف المشتركة في هذا المجال.

المبحث الثالث: واقع حال الجرائم الإلكترونية في المملكة الأردنية الهاشمية ودور الأجهزة الأمنية في مواجهتها

المطلب الأول: واقع حال الجرائم الإلكترونية في المملكة الأردنية الهاشمية

أثرت الجرائم الإلكترونية بشكل كبير على المملكة الأردنية الهاشمية، حيث شهدت البلاد زيادة في عدد الحوادث الإلكترونية المقرونة بنشاطات إجرامية عبر الإنترنت، مما أثار قلقًا واسعًا لدى الأفراد والمؤسسات والحكومة على حد سواء. إذ تحولت الجرائم الإلكترونية إلى مشكلة معقدة تتطلب استجابة فعالة من جميع القطاعات لتحقيق الأمان الرقمي والحفاظ على الاستقرار الاجتماعي والاقتصادي؛ وفي هذا السياق يمكن النظر إلى تأثير الجرائم الإلكترونية على المملكة الأردنية خلال الأعوام (2023-2024) من عدة جوانب، بما في ذلك الأضرار الاقتصادية، والخسائر المالية، وأثرها على الأفراد والمجتمع ككل، وكذلك على الأمن الوطني.

تتزايد الجرائم الإلكترونية في المملكة الأردنية، سجلت المملكة ارتفاعًا ملحوظًا في عدد الحوادث المرتبطة بالجرائم الإلكترونية في السنوات الأخيرة. ففي عام 2023، أظهرت الإحصائيات الرسمية أن الجرائم الإلكترونية في الأردن شهدت زيادة بنسبة تتجاوز (25%) مقارنةً بالعام 2022، حيث تشير إلى تصاعد الأنشطة الإجرامية عبر الإنترنت، مثل الاحتيال المالي، والابتزاز، واختراق الحسابات الشخصية، وهو ما يعكس التحديات الأمنية المتزايدة التي تواجهها المملكة .

وتتمثل الأضرار التي تترتب على الجرائم الإلكترونية في المملكة الأردنية الهاشمية أيضًا في التأثير النفسي على الأفراد المتضررين، وفقًا للدراسات التي أجرتها المركز الوطني للأمن السيبراني، يعاني العديد من الأفراد الذين تعرضوا للاحتيال الإلكتروني أو الابتزاز من مشاعر القلق والاكتئاب نتيجة لتعرضهم للإهانة والتهديدات من قبل المهاجمين، في بعض الحالات، قد يؤثر ذلك على سمعة الأفراد وعلاقاتهم الاجتماعية، خاصة في حالات التسريب غير المشروع للصور الشخصية أو المعلومات الخاصة (المركز الوطني للأمن السيبراني).

من جهة أخرى، يُظهر التقرير أن المجرمين يستخدمون أساليب حديثة ومتطورة لتهديد الأفراد، مثل الهجمات الإلكترونية على الأجهزة المحمولة أو الهجمات التي تستخدم تقنيات التصيد الاحتيالي عبر الرسائل الإلكترونية المزيفة. هذا يعكس التحديات المتزايدة التي تواجه الأفراد في حماية بياناتهم الشخصية. وقد أظهرت نتائج الدراسة أن الأفراد الذين تعرضوا لهذه الأنواع من الجرائم الإلكترونية قد عانوا من اضطرابات نفسية جراء الانتهاك الذي تعرضوا له (التقرير السنوي الصادر عن مديرية الأمن العام الأردنية).

وعلى صعيد الأمن الوطني، تعرضت المملكة الأردنية لعدد من الهجمات السيبرانية التي استهدفت البنية التحتية الحيوية، بما في ذلك المؤسسات الحكومية وأنظمة الأمن الداخلي. ورغم أن الجهات المختصة استطاعت التعامل مع الحادث بسرعة، فإن هذا الحدث يسلط الضوء على حجم التهديدات التي تواجهها المملكة في ظل الهجمات المستمرة من قبل جماعات إلكترونية معادية (موسى وآخرون،2023).

المطلب الثاني: دور الأجهزة الأمنية في مواجهة الجرائم الإلكترونية

أولاً: دور مديرية الأمن العام في مكافحة الجرائم الإلكترونية

تعد مديرية الأمن العام في المملكة الأردنية الهاشمية من الجهات الأمنية الرئيسية المسؤولة عن مكافحة الجرائم الإلكترونية والتي تعتبر أحد أخطر التهديدات التي تواجه الأفراد والمجتمعات وقد ظهرت أشكال جديدة من الجرائم التي يتم ارتكابها عبر الشبكات الإلكترونية، مثل الاحتيال الإلكتروني،

القرصنة، الابتزاز، الهجمات السيبرانية، والتجسس الإلكتروني. وتقوم المديرية بتنفيذ مهام متنوعة لضمان حماية الأمن السيبراني، ومن أبرز هذه المهام:

أ. **تأسيس وحدة الجرائم الإلكترونية**

ب. **التعاون مع الجهات المحلية والدولية**

ت. **التوعية المجتمعية**

ثانياً: التحديات التي تواجه مديرية الأمن العام

رغم الجهود الكبيرة التي تبذلها مديرية الأمن العام في مكافحة الجرائم الإلكترونية، إلا أن هناك العديد من التحديات التي تواجهها ومنها:

أ. **التطور السريع للتكنولوجيا**

يعد التطور السريع في تقنيات الإنترنت والتكنولوجيا من أكبر التحديات التي تواجهها المديرية. مع الابتكارات المستمرة في عالم التكنولوجيا، يتغير شكل الجرائم الإلكترونية بسرعة، مما يتطلب من الأجهزة الأمنية تحديث مهاراتها وأدواتها بشكل مستمر لمواكبة هذه التغييرات.

ب. **الجرائم العابرة للحدود**

بما أن الجرائم الإلكترونية يمكن أن تحدث من أي مكان في العالم، فإن التنسيق بين الدول يصبح أمرًا معقدًا. يصعب تتبع الجرائم الإلكترونية التي تتم عبر الحدود، مما يتطلب تعاونًا أكبر بين الدول والمؤسسات الدولية لملاحقة المجرمين.

ت. **محدودية الوعي الرقمي لدى المجتمع**

لا يزال الوعي بالجرائم الإلكترونية وأمن المعلومات في بعض قطاعات المجتمع محدودًا. هذا الوعي الضعيف يمكن أن يزيد من عدد الضحايا، حيث يقع العديد من الأفراد في فخ الاحتيال الإلكتروني بسبب قلة المعرفة حول طرق الوقاية.

الخاتمة

تعد الجرائم الإلكترونية من أكبر التحديات التي تواجه المجتمعات المعاصرة في عصر الثورة الرقمية، حيث تتزايد خطورتها بفضل التطور السريع في تقنيات الإنترنت والأجهزة الرقمية. كما أنها تهدد الأفراد، المؤسسات، والأمن القومي على حد سواء، مما يستدعي اتخاذ إجراءات قانونية وأمنية حاسمة لمكافحتها. في هذا السياق، قامت العديد من الدول، بما في ذلك المملكة الأردنية الهاشمية، باتخاذ خطوات قانونية حثيثة لمواجهة هذه التهديدات، سواء من خلال تطوير التشريعات الوطنية أو عبر التعاون الدولي في إطار معاهدات واتفاقيات متخصصة.

وعلى الصعيد المملكة الأردنية الهاشمية، فقد سعت الحكومة الأردنية إلى تطوير منظومة قانونية متكاملة لمكافحة الجرائم الإلكترونية من خلال إصدار قانون الجرائم الإلكترونية لعام 2023، الذي يحدد الجرائم الرقمية بشكل واضح ويضع العقوبات المناسبة لها. بالإضافة إلى ذلك، تم تأسيس المركز الوطني للأمن السيبراني ووحدة مكافحة الجرائم الإلكترونية، مما يعكس التزام المملكة بتعزيز الأمن الرقمي وتطوير آليات مكافحة الجريمة الإلكترونية.

وفي الختام، يجب على الدول أن تواصل تحديث تشريعاتها لمواكبة التطورات التكنولوجية المتسارعة وتوسيع التعاون الدولي لمكافحة الجرائم الإلكترونية بشكل فعال. كما أن الوعي المجتمعي والتدريب المستمر يعدان من الركائز الأساسية في بناء مجتمع قادر على مواجهة هذه التحديات الرقمية.

النتائج التوصيات

أولاً: النتائج

1. تزايد ملحوظ في الجرائم الإلكترونية في العالم العربي، وخاصة في السنوات الأخيرة، نتيجة للتوسع في استخدام الإنترنت، ووسائل التواصل الاجتماعي، والتقنيات الحديثة، دون وعي كافٍ بالمخاطر المصاحبة.
2. ضعف الإطار التشريعي في بعض الدول العربية وعدم مواكبته للتطورات التقنية، مما يخلق فجوات قانونية تُستغل من قبل مرتكبي الجرائم الإلكترونية.
3. انخفاض مستوى الوعي المجتمعي بخطورة الجرائم الإلكترونية، وبخاصة لدى فئة الشباب، ما يسهل استدراجهم لعمليات احتيال أو استغلال إلكتروني.
4. تحديات تقنية وأمنية معقدة، أبرزها استخدام أدوات إخفاء الهوية (VPN، TOR)، وانتشار الجرائم عبر الحدود مما يصعّب عملية الملاحقة القانونية.
5. قصور في التعاون الإقليمي والدولي لمكافحة الجرائم الإلكترونية، رغم وجود اتفاقيات دولية مثل اتفاقية بودابست.
6. الابتزاز الإلكتروني أصبح من أكثر الجرائم شيوعًا، ويستهدف بشكل خاص النساء والقُصَّر، نتيجة استخدامهم غير الواعي للإنترنت.
7. تطور أساليب المجرمين الإلكترونيين بسرعة تفوق قدرة الأجهزة التقليدية على المواجهة، مما يتطلب تقنيات أكثر تطورًا لرصد التهديدات والتعامل معها.
8. غياب الإطار الأخلاقي والقيمي لدى بعض مستخدمي الإنترنت، خاصة فئة الشباب، يجعلهم عرضة للتورط في أعمال إلكترونية إجرامية دون إدراك لعواقبها القانونية والاجتماعية.
9. قلة الأبحاث والدراسات المتخصصة في مجال الجريمة الإلكترونية في الدول العربية، ما يترك فجوة في الفهم العلمي والعملي لأبعاد الظاهرة وطرق التعامل معها.
10. غياب تشريعات إقليمية موحدة في العالم العربي لمكافحة الجرائم الإلكترونية، يجعل الملاحقة القضائية صعبة، خصوصًا عندما يكون المجرم أو الخوادم خارج الدولة المتضررة.
11. ضعف حماية حقوق الضحايا الرقمية، حيث تركز بعض القوانين فقط على معاقبة الجناة دون توفير دعم قانوني أو نفسي أو مادي للضحايا.
12. الذكاء الاصطناعي والروبوتات الرقمية بدأت تُستخدم في تنفيذ بعض الجرائم الإلكترونية (مثل التصيّد الصوتي والتزوير الآلي)، مما يصعّب على القوانين التقليدية ملاحقتها.

ثانياً: التوصيات

1. تعزيز التعاون الدولي والإقليمي في تبادل المعلومات، وتنسيق الجهود الأمنية والقانونية لمحاربة الجرائم الإلكترونية العابرة للحدود.
2. إطلاق حملات توعية مجتمعية واسعة النطاق للتعريف بأشكال الجرائم الإلكترونية وأساليب الوقاية منها، مع التركيز على الفئات الأكثر عرضة (الأطفال، الشباب، كبار السن).
3. دمج موضوعات الأمن الرقمي والجرائم الإلكترونية في المناهج التعليمية في المدارس والجامعات، بهدف بناء ثقافة أمنية إلكترونية من سن مبكرة.
4. تشجيع الاستثمار في التكنولوجيا المحلية لتطوير أدوات وبرمجيات أمنية تساعد في الكشف المبكر عن التهديدات الإلكترونية.
5. وضع استراتيجية وطنية شاملة للأمن السيبراني، تُشرف عليها جهة مركزية وتتكامل فيها الأدوار بين المؤسسات الأمنية والقانونية والتعليمية والإعلامية.

6. تحفيز البحث العلمي في مجال الأمن السيبراني من خلال تمويل مشاريع جامعية، ودعم شراكات مع شركات تكنولوجيا محلية وعالمية.
7. إطلاق برامج تأهيل نفسي واجتماعي للضحايا، خاصة في حالات الابتزاز أو التشهير، لتقليل الأثر النفسي والمعنوي ولضمان عدم التكرار.
8. العمل مع شركات التكنولوجيا الكبرى مثل Google، Meta، وغيرها، لتعزيز آليات التبليغ عن الجرائم الإلكترونية ومنع المحتوى الضار قبل انتشاره.
9. تعزيز برامج التدريب المستمر للقضاة والمدعين العامين ورجال الشرطة لفهم طبيعة الجرائم الإلكترونية والإلمام بالتطورات التقنية والقانونية.
10. تبني أدوات الذكاء الاصطناعي في كشف ومنع التهديدات السيبرانية، وخاصة في القطاعات الأمنية، المصرفية، والطاقة، والنقل.
11. إطلاق منصات إلكترونية حكومية لتبليغ المواطنين عن الجرائم الإلكترونية بسهولة وسرعة، مع ضمان السرية وحماية هوية المبلغين.
12. إعداد مدونة سلوك إلكترونية (Cyber Ethics Code) تُعتمد في المؤسسات التعليمية والمهنية، لتعزيز القيم الأخلاقية عند استخدام الإنترنت.
13. تعزيز التعاون بين الجهات الأمنية والقضائية والمؤسسات التقنية، وذلك لضمان سرعة الحصول على البيانات الرقمية وحمايتها من العبث أو الضياع، وبما يضمن قوة الدليل الرقمي أمام المحاكم ويُسهم في تحقيق العدالة ومكافحة الجرائم الإلكترونية بفاعلية.

المصادر والمراجع

أولاً: المصادر والمراجع العربية

سلامة، نسرين سيد. (2023). الجرائم الإلكترونية وأثرها على المجتمع. *مجلة القاهرة للخدمة الاجتماعية*, *39*(2), 389-422.

عماد، بلغيث. *الجريمة الإلكترونية والضرر الاجتماعي* (Doctoral dissertation, Université de M'Sila-Mohamed Boudiaf).

بن عمروش، فريدة، جاب الله، حكيمة. (2023). الجريمة الالكترونية: المفهوم، الأشكال والآليات. *المجلة العلمية للتكنولوجيا وعلوم الإعاقة*, *5*(4), 21-44.

نادين محمود محمد الشايب .(2023) .*التفتيش في الجرائم الإلكترونية: دراسة تحليلية مقارنة* .(Doctoral dissertation)

معاذ الزعبي. (2023). جرائم الذم والقدح والتحقير الإلكترونية بموجب قانون الجرائم الإلكترونية الأردني . *International Review of Law*, *12*(1).

المطيري، & سعد فهد سعد ادبيس. (2023). مفهوم الجرائم الإلكترونية وسماتها. *المجلة القانونية*, *16*(5), 1235-1274.

قانون الجرائم الإلكترونية الأردني، *رقم (17) لسنة 2023م.*

إدارة البحث الجنائي، *وحدة مكافحة الجرائم الإلكترونية، كتاب رقم وك/9/86/ت/4782 تاريخ 2025/4/30م.*

الشربيني، محمد عبد الفتاح. التحقيق في الجرائم المعلوماتية: دليل إجرائي وفني. القاهرة: دار الفكر العربي، 2021.

النجار، محمود عبد الله. (2019). الجرائم الإلكترونية والتحديات القانونية والفنية في الإثبات الرقمي. دار الفكر المعاصر.

أبو شنب، فايز. الجرائم الإلكترونية وأدلة الإثبات الرقمية. عمان: دار الثقافة للنشر والتوزيع، 2020.

حمدي، سامي عبد الرحمن. (2020). الجرائم الإلكترونية وطرق الكشف والتحقيق الجنائي الرقمي. دار الفكر العربي

محمد، أحمد عبد العزيز. (2018). الجرائم الإلكترونية والدليل الرقمي: دراسة فقهية وقانونية مقارنة دار النهضة العربية

التقرير السيبراني الوطني للربع الثاني من عام 2023 /المركز الوطني السيبراني الأردني.

موسى، محمود علي؛ أبو عكار، محمد نائف. (الخوف من الجريمة الإلكترونية المستهدفة للأفراد وعلاقته بالقلق الاجتماعي لدى عينة من الشباب) المجلة العربية للدراسات الأمنية، المجلد 39، العدد 2 (ديسمبر 2023)، صـــ153–163.)

المرجع التقرير السنوي الصادر عن مديرية الامن العام لعامي 2022 و2023

ثانياً: المصادر والمراجع الأجنبية

Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age*. John Wiley & Sons.

Goni, O., Ali, M. H., Showrov, M. M. A., & Shameem, M. A. (2022). The basic concept of cybercrime. *Journal of Technology Innovations and Energy*, *1*(2), 16-24.

Goni, O. (2022). Cybercrime and its classification. *Int. J. of Electronics Engineering and Applications*, *10*(1), 17.

Shafik, W. (2024). Predicting future cybercrime trends in the metaverse era. In *Forecasting cybercrimes in the age of the metaverse* (pp. 78-113). IGI Global Scientific Publishing.

U.s Department of justice.