International Journal of Law Research and Studies (IJLRS)
Vol. (3), No. (5)
IJLRS
November 2024
المجلة الدولية للبحوث والدراسات القانونية
الإصدار (3)، العدد (5)

الجرائم الإلكترونية والجرائم المعلوماتية: من وجهة نظر قانونية وتقنية

فريدة عبد الفتاح راضي
باحثة ماجستير، القانون العام، كلية الحقوق، جامعة عين شمس، جمهورية مصر العربية
Farida.radish@gmail.com

سالي عوض السقا
باحثة ماجستير، تكنولوجيا المعلومات، كلية الحاسبات والمعلومات، جامعة عين شمس، جمهورية مصر العربية
Salinn9090@yahoo.com

الملخص

الجرائم الإلكترونية هي أنشطة إجرامية تستهدف أجهزة الكمبيوتر أو الشبكات بهدف تعطيلها أو إتلافها، أو استخدام بياناتها بطرق غير قانونية، وغالباً ما تشمل هذه الجرائم إدخال فيروسات تؤثر على جهاز واحد ثم تنتشر إلى باقي الأجهزة على الشبكة، مما يؤدي إلى مجموعة من الأضرار المتنوعة. تُعرف الجرائم المعلوماتية، أو السيبرانية، والجرائم الإلكتروني بأنها الأنشطة الإجرامية التي تُرتكب باستخدام أجهزة الكمبيوتر أو أي أجهزة متصلة بشبكة الإنترنت، تهدف هذه الجرائم إلى الوصول غير الشرعي إلى المعلومات أو إلحاق الضرر بالأجهزة أو تعطيلها. مع انتشار الإنترنت على نطاق واسع تزايدت الجرائم الإلكترونية بشكل ملحوظ، ويتم تنظيم هذه الجرائم من قِبل أفراد أو مجموعات سواء كانوا مبتدئين أو محترفين، الدافع الأساسي وراء الجرائم المعلوماتية هو تحقيق الربح المالي، وتُنفَّذ من خلال وسائل متعددة مثل هجمات الفدية، الاحتيال عبر البريد الإلكتروني، وسرقة الحسابات البنكية وبطاقات الائتمان، وغيرها من الأشكال المتنوعة لهذه الأنشطة الإجرامية. يتناول هذا البحث الجرائم الإلكترونية والجرائم المعلوماتية من وجهة نظر قانونية مدعمة بالمفاهيم التقنية في محاولة لتوضيح الأنواع والفروق والأشكال لكل منها.

الكلمات المفتاحية: الجرائم الإلكترونية، الجرائم المعلوماتية، القانون، تكنولوجيا المعلومات.

International Journal of Law Research and Studies (IJLRS)
Vol. (3), No. (5)
IJLRS
November 2024
المجلة الدولية للبحوث والدراسات القانونية
الإصدار (3)، العدد (5)

Cybercrimes and Information Crimes: From a Legal and Technical Perspective

Farida Abdelfattah Rady
Master's Researcher, Public Law, Faculty of Law, Ain Shams University, Arab Republic of Egypt
Farida.radish@gmail.com

Sally Awad Elsakka
Master's Researcher, Information Technology, Faculty of Computers and Information, Ain Shams University, Arab Republic of Egypt
Salinn9090@yahoo.com

Abstract

Cybercrimes are criminal activities that target computers or networks with the aim of disrupting or damaging them, or using their data in illegal ways. These crimes often include introducing viruses that affect one device and then spread to the rest of the devices on the network, causing a variety of damages. Information crimes, or cybercrimes, and electronic crimes are known as criminal activities committed using computers or any devices connected to the Internet. These crimes aim to illegally access information or damage or disable devices. With the widespread spread of the Internet, cybercrimes have increased significantly, and these crimes are organized by individuals or groups, whether they are beginners or professionals. The primary motive behind cybercrimes is to achieve financial gain, and they are carried out through various means such as ransomware attacks, email fraud, theft of bank accounts and credit cards, and other various forms of these criminal activities. This research deals with cybercrimes and information crimes from a legal perspective supported by technical concepts in an attempt to clarify the types, differences and forms of each.

Keywords: Cybercrimes, Information Crimes, Law, Information Technology.

International Journal of Law Research and Studies (IJLRS)
Vol. (3), No. (5)
IJLRS
November 2024
المجلة الدولية للبحوث والدراسات القانونية
الإصدار (3)، العدد (5)

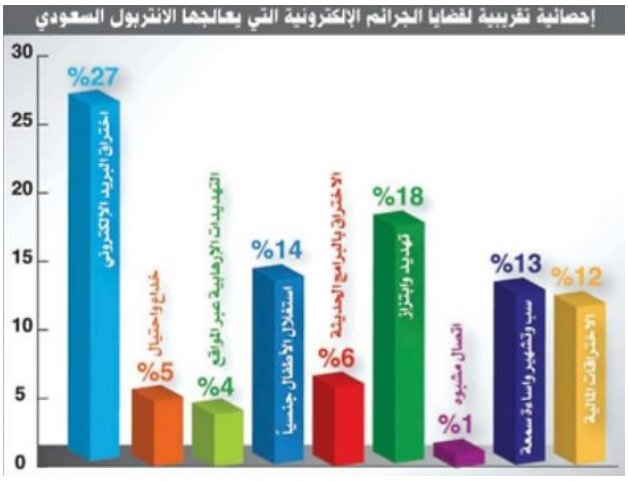
مقدمة

أصبحت الجرائم الإلكترونية من أكبر التهديدات لمستخدمي الإنترنت، حيث تعرّض ملايين الأشخاص لسرقة بياناتهم في السنوات الأخيرة، وقد صرح رئيس شركة IBM بأن الجرائم الإلكترونية تشكل تهديداً كبيراً لأي مهنة أو صناعة أو شركة على مستوى العالم، وتقدر نسبة انتهاك أمن البيانات الناتج عن هذه الجرائم بنحو 48%، مما يتطلب زيادة وظائف الأمن الحاسوبي بأكثر من ثلاثة أضعاف بحلول عام 2021.

تركز الجرائم الإلكترونية غالباً على تحقيق أرباح مادية، حيث يشكل الضرر المالي الخطر الرئيسي، فمع زيادة استخدام الإنترنت والخدمات المصرفية الرقمية يتصاعد خطر هذه الجرائم، لذلك تتزايد أهمية حماية البيانات الشخصية للشركات والأفراد والاحتفاظ بنسخ احتياطية وفقًا للإحصاءات.

مع انتشار الإنترنت على نطاق واسع تزايدت الجرائم الإلكترونية بشكل ملحوظ، ويتم تنظيم هذه الجرائم من قِبل أفراد أو مجموعات سواء كانوا مبتدئين أو محترفين، الدافع الأساسي وراء الجرائم المعلوماتية هو تحقيق الربح المالي، وتُنفَّذ من خلال وسائل متعددة مثل هجمات الفدية، الاحتيال عبر البريد الإلكتروني، وسرقة الحسابات البنكية وبطاقات الائتمان، وغيرها من الأشكال المتنوعة لهذه الأنشطة الإجرامية.

الجرائم المعلوماتية: هي الأنشطة غير القانونية التي تستهدف انتهاك الأجهزة الإلكترونية والحواسيب المتصلة بالإنترنت، حيث يستغل المجرم الشبكة للوصول إلى المعلومات الشخصية للأفراد، ففي العصر الحديث تُعتبر هذه الأجهزة مخزناً ضخماً للبيانات والمعلومات، كما أن الكثير من الأعمال والصفقات التجارية تتم عبر الإنترنت، لذلك، فإن زيادة الوعي بحماية البيانات والمعلومات على الشبكة أمر ضروري. الشكل رقم (1) يوضح إحصائية الجرائم الإلكترونية التي يعالجها الإنتربول السعودي. والشكل رقم (2) يعرض إحصائية الجرائم الإلكترونية في الأردن لعام 2022



شكل (1): إحصائية الجرائم الإلكترونية التي يعالجها الإنتربول السعودي

شكل (2): إحصائية الجرائم الإلكترونية في الأردن لعام 2022

أنواع الجرائم الإلكترونية

يمكن تصنيف الجرائم الإلكترونية إلى الأنواع التالية [1]:

- **هجمات الحرمان من الخدمات (DDoS):**

تُنَفَّذ هذه الهجمات عبر استغلال عدد كبير من أجهزة الكمبيوتر التي يتم التحكم بها عن بُعد من قِبل مستخدمين مشتركي النطاق الترددي، والهدف من هذه الهجمات هو إغراق الموقع المستهدف بكمية ضخمة من البيانات في نفس الوقت، مما يؤدي إلى إبطاء الموقع أو تعطل وصول المستخدمين إليه.

- **التصيد الاحتيالي:**

يعد هذا النوع من الجرائم هو الأكثر شيوعاً حيث يتم إرسال رسائل بريد إلكتروني تحتوي على روابط لمواقع أو مرفقات ضارة، بمجرد نقر المستخدم على هذه الروابط أو فتح المرفقات يتم تحميل برامج ضارة إلى جهاز الكمبيوتر الخاص به.

- **مجموعات الاستغلال:**

يتمثل هذا النوع في استخدام برامج صُممت لاستغلال الثغرات الأمنية في أجهزة الكمبيوتر، يمكن العثور على هذه البرامج في الشبكة المظلمة، أو قد يقوم القراصنة باختراق مواقع ويب شرعية لاستدراج الضحايا.

- **برامج الفدية:**

تعمل هذه البرامج على قفل ملفات المستخدم المخزنة على القرص الصلب، وتطلب دفع مبلغ مالي كفدية لاستعادة الوصول إلى هذه الملفات.

- **القرصنة:**

تشير القرصنة إلى الوصول غير المصرح به إلى بيانات ومعلومات موجودة على أجهزة الكمبيوتر أو الشبكات عبر استغلال نقاط ضعف النظام [2].

- **سرقة الهوية:**

تحدث هذه الجريمة عندما يحصل شخص على معلومات شخصية لشخص آخر بطريقة غير قانونية ويستخدمها لأغراض غير مشروعة مثل الاحتيال أو السرقة [2].

- **الهندسة الاجتماعية:**

تعتمد هذه الجرائم على التلاعب النفسي بالضحية لدفعها إلى القيام بأعمال غير قانونية أو الكشف عن معلومات سرية، وتُستخدم هذه الأساليب بشكل شائع من قِبل مجرمي الإنترنت لارتكاب عمليات الاحتيال [2].

- **قرصنة البرمجيات:**

تعني استخدام وتوزيع البرمجيات دون الحصول على إذن من الجهة المالكة، وتشمل أشكال قرصنة البرمجيات ما يلي [2]:

- إنشاء برمجيات تجارية مزيّفة واستخدام العلامة التجارية للبرمجيات الأصلية.
- تحميل نسخ غير قانونية من البرمجيات.
- انتهاك شروط استخدام البرمجيات التي تحدد عدد المستخدمين المسموح لهم بالنسخة الواحدة.

- **البرمجيات الخبيثة:**

هي البرمجيات التي تؤثر سلباً على أداء أجهزة الكمبيوتر [2]، وتشمل أشهر أنواع البرمجيات الخبيثة [3]:

- الفيروسات: برامج ترتبط ببرامج أخرى وتسبب ضرراً مباشراً للنظام، مثل حذف الملفات أو تعطيل النظام.

- دودة الحاسوب: تشبه الفيروسات ولكنها لا تعدل النظام بل تتكاثر وتؤدي إلى إبطاء النظام، ويمكن التحكم فيها عن بُعد.
- حصان طروادة: برنامج خفي يسرق المعلومات المهمة للمستخدم، مثل المعلومات التعريفية للبريد الإلكتروني.
- برمجيات أخرى: تشمل برمجيات الإعلانات، وبرمجيات التجسس، والبرمجيات الخبيثة الهجينة التي تجمع بين أكثر من نوع من البرمجيات السابقة [2].

ما هي الجرائم الإلكترونية؟

الجرائم الإلكترونية هي أنشطة إجرامية تستهدف أجهزة الكمبيوتر أو الشبكات بهدف تعطيلها أو إتلافها، أو استخدام بياناتها بطرق غير قانونية، وغالباً ما تشمل هذه الجرائم إدخال فيروسات تؤثر على جهاز واحد ثم تنتشر إلى باقي الأجهزة على الشبكة، مما يؤدي إلى مجموعة من الأضرار المتنوعة [4].

الفئات التي تستهدفها الجرائم الإلكترونية

يمكن تصنيف الجرائم الإلكترونية وفقًا للفئة المستهدفة كما يلي [5]:

- الجرائم ضد الأفراد: تشمل هذه الفئة الأنشطة التي تستهدف الأفراد بشكل مباشر، مثل الإزعاجات والمضايقات عبر الإنترنت، نشر المحتوى غير الأخلاقي، الاحتيال على بطاقات الائتمان، سرقة الهوية الإلكترونية، الاستغلال، والتشهير أو الإساءة عبر مواقع الإنترنت.
- الجرائم ضد الممتلكات: تستهدف هذه الجرائم أجهزة الكمبيوتر والخوادم لسرقة محتوياتها أو تدميرها، كما تشمل انتهاك حقوق النشر والملكية الفكرية مما يؤدي إلى تدمير ممتلكات رقمية قيمة.
- الجرائم ضد الحكومات: تهدف هذه الجرائم إلى انتهاك سيادة الدول وسرقة أو تسريب المعلومات السرية، ويمكن أن تشمل أيضًا هجمات إلكترونية يمكن أن تصل للعمليات الإرهابية والحروب.

الحماية من الجرائم الإلكترونية

لحماية أجهزة الكمبيوتر من الجرائم الإلكترونية، يمكن اتخاذ الخطوات التالية [6]:

- تحديث البرامج وأنظمة التشغيل بانتظام.
- استخدام برامج مضادة للفيروسات وتحديثها بانتظام.
- توظيف كلمات مرور قوية ومعقدة لتقليل فرص اختراق الحسابات.
- تجنب النقر على الروابط أو المرفقات في رسائل البريد الإلكتروني العشوائية.

- الحذر من تقديم المعلومات الشخصية إلا إذا كان من المؤكد أن استخدام هذه المعلومات آمن.
- التواصل مباشرةً مع الشركات عند استلام أي طلبات مشبوهة.
- مراقبة الأنشطة المصرفية بانتظام.

أضرار الجرائم الإلكترونية

- **الأضرار المادية:**

تركز الجرائم الإلكترونية غالباً على تحقيق أرباح مادية، حيث يشكل الضرر المالي الخطر الرئيسي، فمع زيادة استخدام الإنترنت والخدمات المصرفية الرقمية يتصاعد خطر هذه الجرائم، لذلك تتزايد أهمية حماية البيانات الشخصية للشركات والأفراد والاحتفاظ بنسخ احتياطية وفقًا للإحصاءات [7]:

- يُتوقع أن تصل التكلفة العالمية للجرائم الإلكترونية إلى حوالي 6 تريليون دولار بحلول عام 2021.
- تُقدَّر خسائر شركات تحليل البيانات بنحو 4 ملايين دولار لكل خرق وفقًا لدراسة معهد بونيمون لعام 2016.
- من المتوقع أن تصل تكلفة برامج الفدية إلى 11.5 مليار دولار في عام 2019.

- **الأضرار على المجتمع:**

أصبحت الجرائم الإلكترونية من أكبر التهديدات لمستخدمي الإنترنت، حيث تعرّض ملايين الأشخاص لسرقة بياناتهم في السنوات الأخيرة، وقد صرح رئيس شركة IBM بأن الجرائم الإلكترونية تشكل تهديداً كبيراً لأي مهنة أو صناعة أو شركة على مستوى العالم، وتقدر نسبة انتهاك أمن البيانات الناتج عن هذه الجرائم بنحو 48%، مما يتطلب زيادة وظائف الأمن الحاسوبي بأكثر من ثلاثة أضعاف بحلول عام 2021 [7].

أمثلة على الجرائم الإلكترونية

هناك الكثير من الأمثلة على الجرائم الإلكترونية التي حدثت في العالم وفيما يلي أشهرها الأمثلة الآتية التي تشمل بعض الجهات التي تعرضت لاختراق أو هجمات مع توضيح السنة والأضرار الناتجة عن الاختراق [8]:

جدول رقم (1): أمثلة لأشهر الجرائم الإلكترونية في العالم

السنة	الجهة التي تعرّضت للاختراق	الأضرار الناتجة عن الاختراق
2014م	متاجر التجزئة الأمريكية اختُرقت أنظمة نقاط البيع، وسرق المهاجمون 50 مليون بطاقة ائتمانية شخصية وحصلوا على تفاصيلها.	اختُرقت أنظمة نقاط البيع، وسرق المهاجمون 50 مليون بطاقة ائتمانية شخصية وحصلوا على تفاصيلها.
2016م	أكبر المواقع الإلكترونية	استُخدم في هذا الهجوم أكثر من مليون جهاز كمبيوتر متصل على الإنترنت واختُرق أغلبها باستغلال ثغرات أمنية على البرامج، وأدّى الهجوم لإيقاف مجموعة كبيرة من أكبر المواقع على الإنترنت.
2017م	مختلف مستخدمي الإنترنت	غلقت خلال هذا الهجوم محتوى 300,000 جهاز كمبيوتر حول العالم، وطُلب من المستخدمين دفع مبالغ مالية مقابل فكّ التشفير وإتاحة وصولهم لبياناتهم مرّةً أخرى.

ما هي الجرائم المعلوماتية

تعريف الجرائم المعلوماتية

تُعرف الجرائم المعلوماتية، أو السيبرانية (Cyber Crime)، والجرائم الإلكترونية (Electronic Crime) بأنها الأنشطة الإجرامية التي تُرتكب باستخدام أجهزة الكمبيوتر أو أي أجهزة متصلة بشبكة الإنترنت [9]، تهدف هذه الجرائم إلى الوصول غير الشرعي إلى المعلومات أو إلحاق الضرر بالأجهزة أو تعطيلها.

مع انتشار الإنترنت على نطاق واسع تزايدت الجرائم الإلكترونية بشكل ملحوظ، ويتم تنظيم هذه الجرائم من قِبل أفراد أو مجموعات سواء كانوا مبتدئين أو محترفين، الدافع الأساسي وراء الجرائم المعلوماتية هو تحقيق الربح المالي، وتُنفَّذ من خلال وسائل متعددة مثل هجمات الفدية، الاحتيال عبر البريد الإلكتروني، وسرقة الحسابات البنكية وبطاقات الائتمان، وغيرها من الأشكال المتنوعة لهذه الأنشطة الإجرامية [10].

أشكال الجرائم المعلوماتية

تشمل الجرائم المعلوماتية مجموعة متنوعة من الأنشطة الإجرامية التي تُرتكب عبر أجهزة الكمبيوتر والإنترنت، من بين الأشكال المختلفة لهذه الجرائم [9]:

- إنشاء وتوزيع محتوى غير قانوني يهدف إلى استغلال الأطفال.
- سرقة أو استخدام المعلومات التي تحميها حقوق النشر دون إذن.
- ممارسة مضايقات أو تهديدات تجاه أشخاص آخرين عبر الشبكة.
- محاولة تجاوز الأنظمة الأمنية التي تحمي المعلومات والبيانات.
- التهديد والابتزاز للضغوط على الأفراد أو المؤسسات لطلب أموال أو مزايا أخرى.

- تطوير وتوزيع برامج الفيروسات والبرمجيات الخبيثة.
- التجسس على الأفراد عبر الإنترنت.
- تعديل السجلات المالية أو المعلومات الأخرى بطرق غير قانونية.
- بيع أو شراء المواد المحظورة.
- الحصول على معلومات بحثية أو علمية من دون إذن.
- إرسال رسائل بريد إلكتروني مزعجة.
- الوصول إلى أنظمة أو بيانات محمية دون الحصول على إذن.

مرتكبو الجرائم المعلوماتية

الأفراد الذين يقومون بالتحايل على أنظمة الأمان للوصول إلى معلومات غير مصرح بها يُطلق عليهم اسم "الهاكرز Hackers، ويُصنَّف الهاكرز إلى ثلاثة أنواع رئيسية [11]:

1. الهاكرز ذو القبعات البيضاء (White Hat Hackers): هؤلاء المتخصصون يساعدون الشركات والمنظمات في تعزيز أمان أنظمتهم الحاسوبية.
2. الهاكرز ذو القبعات (Black Hat Hackers): هؤلاء الأفراد يتبعون طرقاً غير قانونية للوصول إلى البيانات والمعلومات بسرية.
3. الهاكرز ذو القبعات الرمادية (Grey Hat Hackers): هؤلاء يختارون إجراء عمليات اختراق لإظهار براعتهم ومهاراتهم دون أن يسعوا لتحقيق مكاسب.

الفرق بين الجرائم المعلوماتية والجرائم الإلكترونية

يخلط الكثيرون بين مفهومي الجرائم المعلوماتية والجرائم الإلكترونية، لكن هناك اختلافات جوهرية بينهما [12]:

الجرائم المعلوماتية:

هي الأنشطة غير القانونية التي تستهدف انتهاك الأجهزة الإلكترونية والحواسيب المتصلة بالإنترنت، حيث يستغل المجرم الشبكة للوصول إلى المعلومات الشخصية للأفراد، ففي العصر الحديث تُعتبر هذه الأجهزة مخزناً ضخماً للبيانات والمعلومات، كما أن الكثير من الأعمال والصفقات التجارية تتم عبر الإنترنت، لذلك، فإن زيادة الوعي بحماية البيانات والمعلومات على الشبكة أمر ضروري [13].

الجرائم الإلكترونية:

هي الجرائم التي تُرتكب ضد أفراد أو جماعات أو مؤسسات باستخدام وسائل الاتصال الحديثة والحوسبة، تهدف هذه الجرائم عادةً إلى ابتزاز الأفراد، تشويه سمعتهم، أو إلحاق الضرر بهم لتحقيق مكاسب مالية أو أهداف سياسية، أو إفشاء أسرار أمنية تتعلق بالمؤسسات [14].

أنواع الجرائم المعلوماتية

تتنوع دوافع ارتكاب الجرائم المعلوماتية، وتتمثل أبرزها في [14]:

- **الدافع المادي:**

يهدف المجرم هنا إلى تحقيق مكاسب مالية مثل سرقة المال أو البيانات القابلة للتداول، ويمكن أن يكون هذا الدافع فردياً أو جماعياً حسب الهدف.

- **دافع الانتقام:**

يشمل المجرم الذي يمتلك معلومات حساسة حول فرد أو مؤسسة، ويُعتبر هذا النوع من الجرائم خطيراً بسبب المعلومات القيمة التي يتم استغلالها.

- **الدافع السياسي:**

تستهدف الجرائم المعلوماتية هنا المؤسسات الحكومية أو المواقع ذات الصلة بالأنظمة السياسية. يقوم بها مهاجمون يعارضون السياسات أو الأنظمة الدولية.

- **دافع التسلية:**

يرتكب المجرم هذه الجرائم لأسباب ترفيهية دون هدف مادي أو سياسي، مستمتعاً بالقرصنة كنوع من التحدي أو المرح.

- **دوافع ذهنية:**

يسعى المجرم في هذه الحالة لإثبات مهاراته في اختراق الأنظمة وتحدي الأمان الإلكتروني دون أهداف مادية أو سياسية واضحة.

- **الرغبة في التعلم:**

يتطلع المجرم هنا إلى اكتساب خبرة في القرصنة والاختراق بهدف تحسين مهاراته وتعلم كيفية تنفيذ العمليات الأمنية.

مخاطر الجرائم المعلوماتية والجرائم الإلكترونية

ينجم عن انتشار الجرائم المعلوماتية والإلكترونية مخاطر متعددة بسبب سرقة المعلومات الحساسة وتدمير الأنظمة، مما يؤدي إلى خسائر مالية كبيرة وتعطيل العمليات في الشركات، كما يُمكن أن يؤدي الحصول على البيانات الشخصية للأفراد إلى انتحال الهوية، مما قد يسبب مشاكل عائلية وأضرارًا شخصية نتيجة نشر أخبار كاذبة، كما قد تتسبب هذه الجرائم في تدمير أمن واقتصاديات الدول [15].

طرق مكافحة الجرائم المعلوماتية والجرائم الإلكترونية

لمكافحة الجرائم المعلوماتية والإلكترونية، يُنصح باتباع الإجراءات التالية [15]:

- تشفير المعلومات: استخدام تقنيات التشفير لحماية البيانات الحساسة.
- حماية المعلومات الشخصية: تجنب نشر المعلومات الشخصية والبيانات العامة على الإنترنت.
- التوعية والتدريب: توعية الأفراد عبر وسائل الإعلام حول أسباب الجرائم المعلوماتية وكيفية الوقاية منها.
- التحقق من المصادر: عدم فتح روابط أو رسائل من مصادر غير موثوقة أو غير معروفة.
- تحديث كلمات المرور: تغيير كلمات المرور بانتظام وعدم مشاركتها، سواء لحسابات مصرفية أو بطاقات ائتمان أو حسابات على الإنترنت.

القضايا الإلكترونية

تعريف القضية:

القضية هي مسألة تتعلق بنزاع أو خلاف بين طرفين أو مجموعة أطراف، حيث يُدعى الطرف الأول (المدعي) إلى تقديم الدعوى ضد الطرف الثاني (المدعى عليه)، ويتم النظر في القضايا من قِبل المحاكم المختصة التي تصدر الأحكام بناءً على الأدلة والوقائع المقدمة.

منذ القدم كان الناس يلجؤون إلى الحكام والمسؤولين لحل النزاعات، ومع تطور النظام القضائي نشأت المحاكم التي تنظر في الجرائم، والتي تشمل أي تصرف مخالف للقانون سواء كان مخالفة بسيطة، جنحة، أو جناية، والجرائم تشمل السرقة، القتل، النصب والاحتيال، وغيرها من الأفعال التي يعاقب عليها القانون بعقوبات محددة.

مع ظهور تكنولوجيا المعلومات برز نوع جديد من القضايا يُعرف بالقضايا الإلكترونية، تختلف هذه القضايا عن القضايا التقليدية بأنها تتعامل مع الجرائم التي تُرتكب باستخدام التكنولوجيا الحديثة، مثل الحاسوب، الأجهزة الذكية، الإنترنت، وتطبيقات ومواقع التواصل الاجتماعي، تتناول المحاكم في هذه

القضايا الجرائم الرقمية مثل اختراق البيانات، الاحتيال الإلكتروني، والتهديدات الإلكترونية، ويُحكم فيها بناءً على الظروف والأسباب التي أدت إلى حدوثها.

القضايا الإلكترونية:

القضايا الإلكترونية هي تلك التي تُحاكم وفقًا للقانون وتتعلق بالأنشطة التي تحدث عبر الإنترنت أو باستخدام وسائل إلكترونية، وفي السنوات الأخيرة تزايدت هذه القضايا عالميًا بسبب سوء التعامل مع الوسائل الرقمية مما أدى إلى تسرب المعلومات الشخصية ونشرها، وبالتالي تعرض الأفراد لجرائم إلكترونية بسبب عدم الوعي بخطورة مشاركة المعلومات عبر الإنترنت دون تحقق.

تُنظر القضايا الإلكترونية في المحاكم المتخصصة إذا كانت متاحة في الدولة التي وقعت فيها الجريمة، أو في المحاكم العامة المختصة بالجرائم، قد تواجه هذه القضايا تحديات في إيجاد حكم مناسب بسبب الطبيعة الافتراضية للإنترنت خصوصًا عندما يكون المتورطون في بلدان مختلفة، لذلك غالبًا ما تخضع هذه القضايا لأحكام القانون الدولي لتوفير حل مناسب لها.

أنواع القضايا الإلكترونية

1. **النصب والاحتيال الإلكتروني:**

يتضمن هذا النوع من القضايا استخدام الرسائل الإلكترونية المخادعة، مثل إشعارات الفوز بجوائز وهمية، لجعل الضحايا يدفعون مبالغ مالية إلى حسابات مزورة، مما يجعل من الضروري توخي الحذر وحذف أي رسائل غير موثوقة لتجنب الاحتيال.

2. **التشهير والابتزاز:**

يستغل البعض وسائل التواصل الاجتماعي للتشهير أو الابتزاز عن طريق سرقة الصور الشخصية وتهديد أصحابها بنشرها إذا لم يدفعوا مبالغ مالية، لذلك يجب على المستخدمين توخي الحذر عند مشاركة الصور الخاصة لحماية أنفسهم من هذه الجرائم.

3. **السرقة الإلكترونية:**

تشمل سرقة الحسابات البنكية وتحويل الأموال إلى حسابات غير مشروعة، لذلك يُنصح بعدم مشاركة المعلومات المالية الشخصية على الإنترنت لحماية الحسابات البنكية من السرقة.

4. **الاختراق والتخريب:**

يقوم بعض المجرمين باختراق مواقع الإنترنت أو حسابات البريد الإلكتروني لأغراض التسلية أو للحصول على أموال مقابل إعادة الحسابات المخترقة، مما يجعل من الضروري على الأفراد حماية كلمات المرور والمعلومات السرية لمنع الاختراقات.

قانون الجرائم الإلكترونية الأردني

صدر قانون الجرائم الإلكترونية الأردني في عام 2015 بموجب قرار ملكي من الملك عبد الله الثاني، وتمت الموافقة عليه من قبل مجلس النواب ومجلس الأعيان وفقًا للمادة 31 من الدستور الأردني، ينص القانون على معاقبة كل من يدخل إلى نظام معلوماتي أو شبكة معلوماتية بهدف مخالفة القوانين أو تغيير أو إتلاف أو حجب أو نسخ المعلومات دون إذن [16].

تنص المادة 12 منه على أنه يمكن تفتيش المواقع والأجهزة المرتبطة بالجريمة بعد الحصول على إذن من المدعي العام أو المحكمة المختصة، كما تنص المادة 15 على إمكانية مضاعفة العقوبة في حال تكرار الجريمة الإلكترونية [16].

مصطلحات خاصة بقانون الجرائم الإلكترونية الأردني

يشمل قانون الجرائم الإلكترونية الأردني مجموعة من المصطلحات التي تُعرَف على النحو التالي [17]:

- نظام المعلومات: هو مجموعة من البرامج والأدوات التي تُستخدم لإنشاء، إرسال، تخزين، ومعالجة المعلومات والبيانات، وعرضها عبر المواقع الإلكترونية.
- المعلومات والبيانات: تُعرَف البيانات بأنها الحروف، الأرقام، الرموز، أو الصور التي لا تحمل معنى محددًا بمفردها، أما المعلومات فهي البيانات التي أُعطت معنى معينًا من خلال معالجتها.
- الموقع الإلكتروني: هو المساحة أو الحيز على شبكة الإنترنت التي تُنشر عليها المعلومات باستخدام عنوان معين.
- التصريح: هو الحصول على موافقة من صاحب العلاقة للدخول إلى نظام المعلومات الخاص به، وذلك بهدف تغيير، نشر، حذف، أو تعديل محتويات الموقع.

عقوبات قانون الجرائم الإلكترونية الأردني

ينص قانون الجرائم الإلكترونية الأردني على مجموعة من العقوبات التي تشمل الحبس، الغرامة المالية، أو كلاهما وفقًا للجرم المرتكب، والجدول التالي يوضح بعض الأمثلة لهذه العقوبات [18]:

جدول رقم (2): بعض الأمثلة لعقوبات قانون الجرائم الإلكترونية الأردني

الجريمة	مدة الحبس	الغرامة المالية
الدخول إلى أي موقع إلكتروني دون أي تصريح	من أسبوع إلى 3 أشهر	بين 141 إلى 282 دولار أمريكي
الدخول لموقع إلكتروني بغاية التدمير، أو الإضافة، أو الحذف، أو النقل، أو نسخ البيانات، أو تعطيل عمل الموقع، أو انتحال صفة مالكه	من سنة إلى 3 سنوات	بين 705 إلى 2820 دولار أمريكي
الشطب أو التنصت أو اعتراض أي من الأمور المرسلة على شبكة الإنترنت	من 3 أشهر إلى سنة	بين 282 إلى 1410 دولار أمريكي
اعتراض أي من الأمور المتعلقة بتحويل الأموال أو الدفع أو أي من الخدمات المصرفية التى تقدمها البنوك بالإضافة لأي من الحالات السابقة	سنوات على الأقل 5	بين 7050 إلى 2115 دولار أمريكي
نشر الأعمال الإباحية المسموعة، أو المقروءة، أو المرئية	من 3 أشهر إلى سنة	بين 423 إلى 7050 دولار أمريكي

الخاتمة

تناول هذا البحث الجرائم الإلكترونية والجرائم المعلوماتية من وجهة نظر قانونية مدعمة بالمفاهيم التقنية في محاولة لتوضيح الأنواع والفروق والأشكال لكل منها. وقد استعرض التعريفات المتداولة للجرائم الإلكترونية والجرائم المعلوماتية، وأشكال كل منهما، مع عرض أمثلة للعقوبات قانون الجرائم الإلكترونية الأردني. حاول البحث أن يرصد التعريفات بطريقة سلسة وواضحة تجمع بين الرؤية القانونية المستنيرة بالخلفية التقنية.

المراجع

1. "Cybercrime", softwarelab.org, Retrieved 13-2-2021.
2. أ ب ت ث ج ح "5 Types of Cyber Crime: How Cybersecurity Professionals Prevent Attacks", online.norwich.edu,6-5-2020 ،Retrieved 13-2-2021.
3. "Difference between Virus, Worm and Trojan Horse", www.geeksforgeeks.org,15-6-2020 ،Retrieved 13-2-2021.
4. أ ب Kate Brush (2020) ،"cybercrime" ،searchsecurity.techtarget.com, Retrieved 13-2-2021.

5. "What Are the Three Types of Cyber Crimes?", www.swierlaw.com, Retrieved 19-2-2021.
6. "Tips on how to protect yourself against cybercrime", www.kaspersky.com ،Retrieved 13-2-2021.
7. أ ب "Types of Cybercrime", www.pandasecurity.com, Retrieved 13-2-2021.
8. VICKY NGO-LAM (24-12-2019) ،"Cyber Crime: Types, Examples, and What Your Business Can Do" ،www.exabeam.com, Retrieved 13-2-2021.
9. أ ب Computer Hope (22-6-2018), "Computer crime" ,www.computerhope.com, Retrieved 1-2-2019.
10. Margaret Rouse, "Cybercrime" ،searchsecurity.techtarget.com, Retrieved 1-2-2019.
11. "Hacker", www.techopedia.com, Retrieved 1-2-2019.
12. "Forms of cybercrime", government, Retrieved 17/4/2022.
13. "ما هي الجرائم المعلوماتية "، سايبر ون ، اطّلع عليه بتاريخ 2022/1/14.
14. أ ب "ما هي الجرائم الإلكترونية "، مؤسسة دعائم تقنية للحاسب الآلي، تاريخ الزيارة بتاريخ 2022/1/14.
15. أ ب "مخاطر الجرائم المعلوماتية "، سيبرون، تاريخ الزيارة بتاريخ 2022/1/14.
16. أ ب ت "قانون الجرائم الإلكترونية"، الجريدة الرسمية، تاريخ الزيارة بتاريخ 2022/1/15.
17. "قانون الجرائم الإلكترونية الأردني"، القوانين الأردنية، تاريخ الزيارة بتاريخ 2022/1/15.
18. "قانون جرائم أنظمة المعلومات"، خارجون على المهنة، تاريخ الزيارة بتاريخ 2021/1/15.