المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)
العدد الرابع والخمسون (تشرين الأول) 2022
ISSN: 2617-9563
www.mecsj.com/ar/

الجرائم الإلكترونية: ماهيتها، وأنواعها، والتشريعات القانونية لمواجهتها في القانون العماني

أحمد سالم أحمد الغافري
طالب دكتوراه في القانون، كلية أحمد إبراهيم للحقوق، الجامعة الإسلامية العالمية ماليزيا.
الدكتورة حليمة بوكروشة
الأستاذ المساعد في الشريعة والقانون، كلية أحمد إبراهيم للحقوق، الجامعة الإسلامية العالمية ماليزيا.

ملخص البحث

يهدف البحث إلى مناقشة المسائل المتعلقة بالجرائم الإلكترونية، حيث إن معظم الجرائم الإلكترونية هي عبارة عن هجوم على المعلومات المتعلقة بالأفراد أو الشركات أو الحكومات، وقد تحدث البحث عن الجرائم في ولايات قضائية مختلفة تفصل بينها مسافات شاسعة، وتناول إشكالية في بحث مدى فعالية التشريعات القانونيةفي مواجهة الجرائم الإلكترونية في القانون العماني، من خلال فحص هذه القوانين ذات الصلة ومقارنتها بالقوانين الأخرى. وقد التزم الباحث في دراسته بالمنهج الاستقرائي، وذلك من خلال تتبع المعلومات، وأقوال الباحثين المتعلقة بتفاصيل موضوع البحث، وعرض آراءهم للمساعدة في استيعاب مشكلة البحث، واستخراج النظريات ذات الصلة من الجزئيات. كما تناول المنهج التحليلي، وذلك من خلال تحليل النصوص القانونية المتعلقة بالمسائل محل الدراسة، وكشف مواطن القوة للإشادة بها، ومواطن الضعف والنقص والقصور، وتقديم توصيات ومقترحات لمعالجتها وتلافيها، والمنهج المقارن، لمقارنة المبادئ القانونية المتعلقة بالجرائم الإلكترونية، وذلك بالرجوع إلى المصادر الأصلية، وبعض القوانين الأجنبية والعربية في المسائل المنوطة بهذه الجرائم الإلكترونية. وقد خلص البحث إلى أن الجرائم الإلكترونية تلحق أضراراً خطيرة بالأفراد والمؤسسات والشركات، حيث يشعر المستخدمون بالتهديد من جراء هذه الأعمال الإجرامية، وأن معظمهم يرى أن احتمال ارتكاب جرائم إلكترونية تؤدي إلى الإضرار بهم بشدة كبير، وأنه لا يؤثر ذلك على المستخدمين فحسب، بل يؤثر أيضا على أعمال التجارة الإلكترونية، وينتشر الخوف بين العملاء، وهو ما يؤدي إلى سقوط المستخدمين في شراك هذه الجرائم، وهذه الطريقة تخسر بها الصناعة مبالغ كبيرة من المال، ولم يتطرق قانون المعاملات الإلكترونية العماني في أحكامه للمسائل المتعلقة بالجرائم الإلكترونية ومكافحتها، وأن قانون مكافحة جرائم تقنية المعلومات هو الذي تتناول أحكامه مكافحة الجرائم الإلكترونية.

كلمات افتتاحية: الجرائم الإلكترونية، التشريعات القانونية، التجارة الإلكترونية، قانون المعاملات العماني.

المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)
العدد الرابع والخمسون (تشرين الأول) 2022
ISSN: 2617-9563
www.mecsj.com/ar/

ABSTRACT

The research aims to discuss issues related to cybercrime, where most cybercrimes are attacks on information pertaining to individuals, companies or governments. The search for crimes may occur in different jurisdictions separated by vast distances, and to the extent of the risks involved in conducting electronic business, and in terms of the risks associated with e-commerce represented by crimes in e-commerce, and legal legislation and its effectiveness in confronting those crimes in the Omani Law, compared to and benefiting from other laws, and that shortcomings taint the Omani Electronic Transactions Law in not making provisions related to electronic crimes and combating them. In his study, the researcher adhered to the inductive approach by tracking information and researchers' statements related to the details of the research topic, presenting their opinions to help in understanding the research problem, extracting relevant theories from the particles, and the analytical approach, by analysing legal texts related to the issues under study, and revealing Strengths to commend them, weaknesses, shortcomings and shortcomings, make recommendations and proposals to address and avoid them, and the comparative approach, to compare legal principles related to cybercrime, by referring to the original sources, and some Foreign and Arab Laws in the issues involved in cybercrime. The research concluded that cybercrime causes serious harm to individuals, institutions and companies, as the e-commerce industry should develop, as users feel threatened by these criminal acts, as most of them believe that the possibility of committing cybercrime leads to severe harm to them, and that they do not affect not only the users, but also the e-commerce business, as the fear spreads all over the customers, so this will lead to the downfall of the users in the industry, and in this way the industry loses a large amount of money. The Omani Electronic Transactions Law did not address in its provisions the issues related to combating cybercrime, and the Law on Combating Information Technology Crimes is the one whose provisions for combating cybercrime.

KeyWords: *Cyber Crimes, Legal Legislation, E-commerce, Omani Transaction Law*.

المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)
العدد الرابع والخمسون (تشرين الأول) 2022
ISSN: 2617-9563
www.mecsj.com/ar/

المقدمة

مع انتشار هذه الوسائل التكنولوجية الحديثة من الحاسب الآلي والهواتف الذكية بين أفراد المجتمعات وانتشار استخدامها وانتشار التعامل من خلالها، أصبح لكل فرد القدرة على التفاعل والتواصل دون أي حواجز أو جغرافيا، مع توافر القدرة على النقل، وأصبحت المعلومات والتقنيات والوصول إلى البيانات والبرامج، ومع العديد من المزايا والفوائد التي صاحبت ظهور هذه المجالات الجديدة والمتقدمة من العلم والمعرفة، ومع ذلك ترافق ذلك مع ظهور خبراء جدد، بالإضافة إلى تعريفهم ممن لديهم الخبرة والاحتراف في تكييف هذه التكنولوجيا للقيام بأعمال إجرامية أدت إلى إيقاظ الهمم من قبل العالم لإيجاد حلول للتصدي لهذه التحديات، ومكافحة تلك الجرائم الإلكترونية التي أزعجت الجميع. بالإضافة إلى الجريمة التقليدية، أصبحت الجرائم الإلكترونية أمراً منتشراً، ونوع من أنواع العمل الجنائي المعتمد على أساليب مبتكرة لم تكن معروفة من قبل،كما ظهرت العديد من المشاكل والسلبيات على شكل جرائم ارتكبها بعض مستخدمي التكنولوجيا، والتي تتميز بخطورتها وسهولة ارتكابها، وأصبحت معضلة عابرة للحدود الوطنية، حيث سميت بالجرائم العابرة للقارات و الجرائم السيبرانية.

لقد شهد العالم نمواً كبيرا في الإجرام السيبراني في شكل حملات واسعة في جميع بقاع العالم، حيث يسعى مجرمو الإنترنت إلى استغلال نقاط الضعف البشرية أو الأمنية لسرقة كلمات المرور أو البيانات أو الأموال بشكل مباشر. وتتناول التهديدات الإلكترونية الأكثر شيوعاً قرصنة وسائل التواصل الاجتماعي وكلمات مرور البريد الإلكتروني، ورسائل البريد إلكتروني المزيفة التي أصبحت تصل بشكل روتيني للمستخدمين، تطلب معلومات أمنية وتفاصيل شخصية وغيرها من الجرائم الإلكترونية.

لا شك في أن الهجمات السيبرانية مدمرة مالياً ومزعجة للأفراد والشركات الحكومية، حيث الجريمة السيبرانية هي تهديد عالمي شامل، مما يجعل العالم يركز في حوادث الجرائم السيبرانية الخطيرة بالإضافة إلى الأنشطة طويلة المدى ضد المجرمين والخدمات والبرامج التي يعتمدون عليها. ويمكن منع معظم الهجمات الإلكترونية من خلال اتباع الخطوات الأمنية الأساسية، من حيث اختيار كلمات مرور قوية ولا يجب إعادة استخدامها لعمليات تسجيل دخول متعددة، وتثبيت برامج الأمان مثل برامج مكافحة الفيروسات الموثوقة.

وغالبًا ما يكون هذا النوع من البرامج متاحا مجاناً، ولكي يدخل الفعل في إطار الجرائم الإلكترونية يجب أن يقوم به جهاز الحاسب الآلي، ويقصد هنا بجهاز الحاسب الآلي والمكونات المنطقية للحاسب الآلي من معلومات وبرامج وكذلك جميع المكونات الأخرى التي تساعد في عملية المعالجة الآلية للمعلومات.

المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)
العدد الرابع والخمسون (تشرين الأول) 2022
ISSN: 2617-9563
www.mecsj.com/ar/

1. مشكلة البحث

تتمحور مشكلة هذا البحث في فحص فعالية التشريعات القانونية العمانية في مواجهة الجرائم الإلتكرونية، والمقارنة بينها وبين القوانين الأخرى.

2. أسئلة البحث

وفي هذا البحث، يتم الإجابة على الأسئلة التالية:

1. كيف يتم التعامل مع الجرائم الإلكترونية أو القضايا المتعلقة بهذه الجرائم؟
2. ما مدى خطورة وحجم الجرائم الإلكترونية التي يعاني منها العالم ككل؟
3. كيف يتم التعامل مع هذه الجرائم من المنظور القانوني؟

3. أهداف البحث

تتمثل أهداف البحث في الآتي:

1. التعريف بالجرائم الإلكترونية والأمن السيبراني.
2. الكشف عن التحديات والمشاكل المرتبطة بأمن التجارة الإلكترونية.
3. استكشاف مشكلات التجارة الإلكترونية وكيفية حلها من المنظور القانوني.

4. أهمية البحث

تمكن تصنيف أهمية هذا البحث على النحو التالي:

1. التحقق من مكافحة الجرائم الإلكترونية في التجارة الإلكترونية من خلال التشريعات القانونية الموجودة في سلطنة العمان.
2. توفير الأمن السيبراني لحماية التجارة الإلكترونية في سلطنة عمان، وحماية تجارة العملاء المنخرطون في أعمال التجارة.
3. الحماية القانونية للتجارة الإلكترونية لحماية نشاطات التجارة الإلكترونية في سلطنة عمان.

5. فرضيات البحث

تتمثل فرضية البحث في النقطة التالية:

وجود قصور يشوب قانون المعاملات الإلكترونية العماني في أحكامه، وأنه لم يتناول المسائل المتعلقة بالجرائم الإلكترونية ومكافحتها.

6. منهجية البحث

يعتمد الباحث في بحثه على المناهج الآتية:

1. **المنهج الاستقرائي:** وذلك من خلال تتبع المعلومات، وأقوال الباحثين المتعلقة بتفاصيل موضوع البحث، وعرض آرائهم للمساعدة في استيعاب مشكلة البحث، واستخراج النظريات ذات الصلة من الجزئيات.
2. **المنهج التحليلي:** وذلك من خلال تحليل النصوص القانونية المتعلقة بالمسائل محل الدراسة، وكشف مواطن القوة للإشادة بها ومواطن الضعف والنقص والقصور، وتقديم توصيات ومقترحات لمعالجتها وتلافيها.

المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)
العدد الرابع والخمسون (تشرين الأول) 2022
ISSN: 2617-9563
www.mecsj.com/ar/

3. **المنهج المقارن:** لمقارنة المبادئ القانونية المتعلقة بالجرائم الإلكترونية، وذلك بالرجوع إلى المصادر الأصلية، وبعض القوانين الأجنبية والعربية في المسائل المتعلقة بالجرائم الإلكترونية.

7. حدود البحث

تتمثل حدود البحث في:

1. **الحدود الموضوعية:** تشمل التطرق إلى القوانين المعنية بالجرائم الإلكترونية، كقانون المعاملات الإلكترونية لسلطنة عمان، رقم (٩٦)، لسنة ٢٠٠٨م، وغيرها من القوانين والتشريعات الدولية الخاصة بالجرائم الإلكترونية.
2. **الحدود الزمنية:** يتم إجراء البحث على القوانين العمانية، والتعليمات واللوائح المتعلقة بموضوع البحث، المعمول بها حالياً في سلطنة عمان.
3. **الحدود المكانية:** اقتصر الباحث على إجراء البحث على موضوع الجرائم الإلكترونية في سلطنة عمان.

8. الدراسات السابقة

ومن الدراسات التي اطلع عليها الباحث في هذا الموضوع، ومنها:

كتاب لطفي سعد، بعنوان : لطفي سعد، الجرائم الإلكترونية والقانون، تحدث الكاتب عن الجرائم الإلكترونية في المنظور القانوني، وأنها عملية غير قانونية يرتكبها المجرمون عبر الإنترنت، ويمكن أن تتراوح من التزوير إلى القرصنة وما إلى ذلك، كما تعتبر أيضاً الأنشطة الإجرامية والاحتيال والتزوير والتشهير والفساد من خلال الإنترنت أو الوسائط الإلكترونية من الجرائم الإلكترونية بموجب قانون تكنولوجيا المعلومات لعام 2000م، وعام 2008م وعام 2010م، حيث تعرضت الشبكات غير الآمنة لهجوم كاسح، وتعطّلت البنية التحتية لتكنولوجيا المعلومات. وحلل الكاتب بأن نقص الوعي لدى المستهلكين والمؤسسات تمنح الجرائم الإلكترونية فرصة واسعة للتغلغل في النظم المعلوماتية.

والجرائم الإلكترونية تحدث في جميع أنحاء العالم، ويستخدم هؤلاء المجرمون ميزة الإنترنت لمهاجمة الأفراد أو المنظمات أو حتى الحكومة. وفي الجرائم الإلكترونية يتم استخدام الكمبيوتر كسلاح للإرهاب الإلكتروني، يتم بواسطته تزوير بطاقات الإئتمان والخصم المباشر، وعمليات الاحتيال عبر تحويل الأموال الإلكتروني والكمبيوتر على الهدف، القرصنة وهجمات الفيروسات، ونظام التشغيل، وما إلى ذلك من أنواع الجرائم الإلكترونية التي يرتكبها المجرمين. إلا أن الكاتب لم يتحدث عن الجرائم الإلكترونية في النطاق القانوني العماني، أو المسار القانوني العربي.

كتاب عوض البنا، بعنوان: الجرائم الإلكترونية والتجارة الإلكترونية، الثورة الهواتف الذكية والأجهزة اللوحية أدت إلى زيادة معاملات التجارة الإلكترونية، ولكن مع تزايد مخاطر الجرائم الإلكترونية أيضاً حيث زادت الجرائم الإلكترونية بشكل كبير في السنوات الخمس الماضية مما يثير القلق بشأن توفير أحكام لربط الجرائم والقوانين بشكل ملائم، وقوة الوعي لدى الناس واستخدام التكنولوجيا ضرورية لمنع الأنشطة المسؤولة عن استخدامها في منظور سلبي، مع النمط الجديد لأنشطة الأعمال، على سبيل المثال، الخدمات المصرفية والتجزئة وما إلى ذلك، كل

هذا يعتمد على الوسائط الإلكترونية . والشركات التي تتجه نحو الإنترنت متحمسة بشأن نموها ومن ناحية أخرى تشعر بالقلق بشأن الأمن الإلكتروني.

وصناعة التجارة الإلكترونية تختلف عن بقية الصناعات من حيث العمليات، لذا فهي تواجه تحديات ومخاطر فريدة حيث أن الغياب المادي يزيد من فرص الاحتيال والجرائم. هناك العديد من الأسباب في جميع أنحاء العالم لعمليات الاحتيال الإلكترونية غير المنضبطة في التجارة الإلكترونية، وتستمر تكلفة الجرائم الإلكترونية في الزيادة مع تحرك المزيد من الشركات عبر الإنترنت، ومع تجمع المستهلكين والمؤسسات في الفضاء الإلكتروني. تزداد مخاطر سرقة الملكية الفكرية مما يؤدي إلى تكرار المنتجات معنا، كما أن سرقة التكنولوجيا تتسبب في خسائر فادحة للشركات. وقدم الكاتب حلولاً منها: أنه يجب على الحكومات اتخاذ احتياطات أكثر جدية لمواجهة تحديات الجرائم الإلكترونية، وإلا ستلحق التكنولوجيا الضرر بالأعمال، وتتسبب الجرائم الإلكترونية على مستوى العالم في خسارة لا تحمد عقباها. إلا أن الكتاب لم يتحدث عن الجرائم الإلكترونية في المنظور القانوني العماني.

كتاب عبد القادر شاة، بعنوان: كيفية التعامل مع الجرائم الإلكترونية، ومن الحلول التي قدمها الكاتب بأنه يمكن السيطرة على الجرائم الإلكترونية من خلال التعاون المتبادل بين المنظمات ومستخدمي الإنترنت، وينبغي على المنظمات والحكومات توفير السلامة والدعم الفني للمستخدمين لمنع هذه الجرائم، على مستخدمي الإنترنت أيضاً اتخاذ بعض الاحتياطات حتى لا يقعوا ضحية لعمليات الاحتيال الجرائم الإلكترونية، وأن يتحد الإنترنت بحثاً عن عالم تقني أفضل وآمن .

ومنها: بأن تغيير كلمة المرور بشكل مختلف يساعد على حماية معظم المعلومات إن لم تكن جميع المعلومات الشخصية، ربما إذا قام المجرم الإلكتروني باختراق أحد مواقع الويب التي قد يكون آمناً على الآخر، لا يتمكن من الوصول إلى جميع المواقع بسبب تلك الكلمات السرية المختلفة. استخدام المواقع الآمنة تجعل من الصعوبة بمكان على المجرمين الوصول إلى الموقع لسرقة المعلومات، لذلك فهذه طريقة جيدة جدًا لحماية المعلومات من هذه الأعمال الإجرامية.

التجنب من فتح رسائل البريد الإلكتروني المشبوهة، حيث يستخدم المجرمون هذه الطريقة كوسيلة للإيقاع بضحيتهم، حيث يعدونهم بفوز يانصيب أو الفوز بألعاب المقامرة الثابتة فقط حتى يتمكنوا من الحصول على المعلومات ثم يختفون بالمعلومات المالية المسروقة. تغيير كلمات المرور بشكل متكرر، لأنه من غير الآمن استخدام نفس كلمة المرور على النظام الأساسي لفترة طويلة، لذلك سيكون من الآمن تغيير كلمات المرور بشكل متكرر. التسوق من خلال المواقع الموثوقة: سيكون من الصعب مهاجمة المواقع الموثوقة من قبل هؤلاء المجرمين. بيد أن الكاتب قدم حلولاً تكنولوجية فحسب وليست قانونيةً، وهذا ما سيقوم به الباحث من إيجاد حلولاً مناسبةً من المنظور القانوني من خلال القوانين العمانية.

المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)
العدد الرابع والخمسون (تشرين الأول) 2022
ISSN: 2617-9563
www.mecsj.com/ar/

خطة البحث

وتقتضي طبيعة البحث أن يكون في مقدمة، وأساسيات البحث، وفي مبحثين، ومطالب، وفروع، ثم خاتمة، ونتائج، وتوصيات، ومراجع.

المبحث الأول: ماهية الجرائم الإلكترونية وخصائصها
المطلب الأول: ماهية الجرائم الإلكترونية
الفرع الأول: تعريف الجرائم الإلكترونية
المطلب الثاني: خصائص الجرائم الإلكترونية
المبحث الثاني: أركان الجرائم الإلكترونية وأنواعها
المطلب الأول: أركان الجرائم الإلكترونية
المطلب الثاني: أنواع الجرائم الإلكترونية

المبحث الأول: ماهية الجرائم الإلكترونية وخصائصها

المطلب الأول: ماهية الجرائم الإلكترونية

تعد ظاهرة الجريمة السيبرانية ظاهرة إجرامية ناشئة نسبياً تدق أجراس الإنذار لتنبيه المجتمعات الحالية إلى حجم المخاطر وفداحة الخسائر الناتجة عنها، حيث تهدف إلى مهاجمة البيانات بمعناها الفني الواسع البيانات والمعلومات والبرامج بجميع أنواعها؛ إنها جريمة تقنية تنشأ سراً، يرتكبها مجرمون أذكياء، يمتلكون أدوات معرفية تقنية، موجهة لتقويض الحق في المعلومات، يحث تؤثر هجماتها على بيانات الكمبيوتر المخزنة والمعلومات المنقولة عبر أنظمة وشبكات المعلومات، وفي مقدمتها الإنترنت.

الفرع الأول: تعريف الجرائم الإلكترونية

يمكن تعريف الجريمة الإلكترونية على أنها: ((هجوم على بيانات الكمبيوتر المخزنة والمعلومات المنقولة عبر أنظمة وشبكات المعلومات، وخاصة الإنترنت، وحددتها منظمة التعاون الاقتصادي والتنمية (OECD) على أنها: (كل فعل أو إغفال من شأنه مهاجمة الأموال المادية والمعنوية الناتجة بشكل مباشر أو غير مباشر عن تدخل تكنولوجيا المعلومات)).

والمشرع العماني لم يُعرّف الجرائم الإلكترونية بطريقة مباشرة، وإنما ذكر الأفعال المتعلقة بتلك الجريمة، حيث يعتبر ذلك تعريفاً لهذه الجريمة بشكل غير مباشر.

وفي المادة (٥٢) من قانون المعاملات الإلكترونية على أنه: يتم معاقبة:

1. كل من تسبب عمداً في تعديل غير مرخص به في محتويات أي حاسب آلي بقصد إضعاف فاعليته أو منع أو تعويق الدخول إلى أي برنامج أو بيانات محفوظة فيه أو إضعاف فاعلية ذلك البرنامج أو إضعاف الاعتماد على تلك البيانات إذا تم ذلك التعديل بإحدى الطرق الآتية:
   أ. شطب أي برنامج أو بيانات محفوظة في الحاسب الآلي.
   ب. إضافة أي برنامج أو بيانات إلى محتويات الحاسب الآلي.

المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)
العدد الرابع والخمسون (تشرين الأول) 2022
ISSN: 2617-9563
www.mecsj.com/ar/

ج. أي فعل يسهم في إحداث ذلك التعديل.

ومن الملاحظ أن كل ما ذكرته هذه المادة من الأفعال تعتبر من الجرائم الإلكترونية. كأن المادة تقول: بأن الجرائم الإلكترونية هي شطب أي برامج محفوظ في الحاسب الآلي، وأي فعل يساعد في وقوع ذلك.

2. اخترق جهاز حاسب آلي أو منظومة حاسبات آلية أو موقع على الإنترنت أو شبكة إنترنت وترتب على ذلك:

أ تعطيل أنظمة تشغيل جهاز الحاسب الآلي أو منظومة الحاسبات الآلية.

ب إتلاف برامج الحاسب الآلي أو الحاسبات الآلية وما تحتويه من معلومات.

ج سرقة المعلومات.

د استخدام المعلومات التي تتضمنها مخرجات الحاسبات الآلية في أغراض غير مشروعة.

ه إدخال معلومات غير صحيحة.

وكل هذه الأفعال التي ذكرتها هذه المادة هي من الأفعال التي تمثل الجرائم الإلكترونية.

3. دخل بطريق الغش إلى نظام معلومات أو قاعدة بيانات بغرض العبث بالتوقيعات الإلكترونية.
4. قام بطريقة غير مشروعة بكشف مفاتيح لفض التشفير أو فض تشفير معلومات مودعة لديه.
5. استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بتوقيع غيره.
6. اخترق أو اعترض معلومات أو بيانات مشفرة أو قام بفض شفرتها عمداً دون مسوغ قانوني، وتضاعف العقوبة إذا كانت المعلومات أو البيانات تتعلق بسر من أسرار الدولة.
7. قام عمداً بفض معلومات أو بيانات مشفرة بأية طريقة في غير الأحوال المصرح بها قانوناً.
8. قام عمداً بإنشاء أو نشر شهادة أو زود بمعلومات إلكترونية غير صحيحة لغرض غير مشروع.
9. قدم بيانات غير صحيحة عن هويته أو تفويضه لمقدم خدمات التصديق بغرض طلب إصدار أو إلغاء أو تعليق شهادة.
10. قام عمداً – بغير سند قانوني – بكشف بيانات سرية تمكن من الوصول إليها بما له من سلطات بموجب هذا القانون أو أي قانون آخر.
11. مارس نشاط مقدم خدمات تصديق بدون ترخيص.
12. استعمل بصفة غير مشروعة أداة إنشاء توقيع متعلقة بتوقيع شخص آخر.
13. قام بالدخول غير المشروع إلى حاسب آلي بقصد ارتكاب جريمة أو تسهيل ارتكاب جريمة سواء بواسطته أو بواسطة شخص آخر.

المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)
العدد الرابع والخمسون (تشرين الأول) 2022
ISSN: 2617-9563
www.mecsj.com/ar/

14. زور سجلاً إلكترونياً أو توقيعاً إلكترونياً أو استعمل أياً من ذلك مع علمه بتزويره.
15. قام عمدا بطريقة غير مشروعة بنشر أو تسهيل نشر أو استعمال سجل إلكتروني أو توقيع إلكتروني أو فض شفرته. وتضاعف العقوبة إذا كان مرتكب الجريمة أميناً على ذلك السجل أو التوقيع بمقتضى مهنته أو وظيفته).

وقانون مكافحة تقنية المعلومات العماني قدم تعريفاً بأنه (كل من دخل عمداً ودون وجه حق موقعا إلكترونياً أو نظاماً معلوماتياً أو وسائل تقنية المعلومات أو جزءا منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك).

وعرّفها المشرع الإماراتي بأنها: (كل من ارتكب جريمةً أو فعلاً باستخدام وسيلة إلكترونية...). ويُفهم من هذا التعريف بأنها جريمة ترتكب باستخدام وسائل الإلكترونية، بغض النظر عن نوع وشكل هذه الجريمة.

و يلاحظ مما سبق ذكره إلى ما تم سرده آنفاً، نجد بأن المشرع العماني والمشرع الإماراتي هما على نفس الخطى، حيث لم يتم تعريف الجرائم الإلكترونية بشكل مباشر سواء من قبل المشرع العماني أو الإماراتي، إلا أنه تم التنصيص على الأفعال التي تمثل الجرائم لإلكترونية من قبل القانونيين.

أما عن تعريف الأمم المتحدة، حيث عرفها المنظمة بأنها (أي جريمة يمكن أن يرتكبها نظام حاسوبي أو شبكة كمبيوتر أو داخل نظام حاسوبي، وتشمل تلك الجريمة من حيث المبدأ جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية).

ومن الملاحظ فيما سبق من التعريفات أنها تتفق في معناها لمفهوم وتعريف الجريمة الإلكترونية أو الجرائم الإلكترونية. وأنه يمكن تعريفها بأنها: كل فعل أو نشاط يُرتكب عبر وسائل التكنولوجيا الحديثة، سواء من الحاسب الآلي أو الجوال أو غيرها من وسائل التكنولوجيا المعاصرة، وهدفها يكون الإضرار بالآخرين، وقد تصل تلك الجرائم إلى الإرهاب الإلكتروني.

المطلب الثاني: خصائص الجرائم الإلكترونية

للجرائم الإلكترونية خصائص متعددة تجعلها تختلف عن الجرائم العادية، وهي ترتكب بواسطة شبكة الإنترنت، وأنها جريمة عابرة للحدود وذات بعد دولي، الجرائم الالكترونية تتسم بالخطورة البالغة، وصعوبة التحري والتحقيق في هذه الجرائم ومن ثم محاكمة مرتكبها، والدافع لارتكاب جرائم الإنترنت يختلف عن دافع الجرائم التقليدية، وهي جرائم ناعمة بعيدة عن العنف، إنها جريمة يرتكبها مجرمون على درجة عالية من التخصص والكفاءة في استخدام أجهزة الكمبيوتر والإنترنت، واسع الأفق وواسع الحيلة، وتتصف بصعوبة الإثبات، وهذه الجرائم لا تترك الجريمة الإلكترونية آثاراً مادية، وصعوبة الحفاظ على أدلة الجرائم الإلكترونية، تحتاج الجرائم الإلكترونية إلى الخبرة الفنية ليتم اكتشافها، وتحدث جريمة المعلومات أثناء المعالجة الآلية للبيانات في مرحلة إدخال البيانات أو أثناء مرحلة المعالجة أو أثناء مرحلة إخراج المعلومات في مرحلة إدخال المعلومات، تتم ترجمة المعلومات إلى لغة يفهمها الجهاز. من السهل إدخال البيانات التي لا علاقة لها تمامًا بالبيانات

المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)
العدد الرابع والخمسون (تشرين الأول) 2022
ISSN: 2617-9563
www.mecsj.com/ar/

الأساسية ومسح البيانات المراد إدخالها. في مرحلة المعالجة، حيث يمكن إدخال بيانات غير مصرح بها واستبدالها ببيانات أساسية، أو قد يتم إطلاق برامج جديدة تلغي جزئياً أو كلياً عمل البرامج الأصلية.

المبحث الثاني: أركان الجرائم الإلكترونية وأنواعها

المطلب الأول: أركان الجرائم الإلكترونية

وفي جميع القوانين، سواء في النظام القانوني الإنجليزي أو النظام القانوني الفرنسي لا بد من توافر أركان الجريمة الثلاثة، وهذا ما ينص عليه القانون الجنائي العماني، التي هي:

1. قانونية الجريمة، بحث تكون الجريمة قد سبق تجريمها قانونياً.
2. الركن المادي.
3. والركن المعنوي.

وهذه الأركان الثلاث لا بد من أن تتوفر في جميع الجرائم دون استثناء، لأنها سلوك تطوعي ناشئ عن الإنسان مثل أي سلوك بشري، حيث له جانبان:

أ الجانب المادي

ب والجانب الخارجي.

وفيما يلي بعض التفصيل لهذه الأركان:

أولاً: الركن الشرعي

تهتم الشريعة الإسلامية والقوانين الوضعية بحماية حقوق الأفراد والمجتمعات. يتميز هذا العصر بالسرعة المذهلة في تطوير تكنولوجيا المعلومات واعتماد معظم المجالات عليها، وما تحققه للفرد والمجتمع في توفير الوقت والسرعة في إنجاز العمل. يتم فرض هذه الفوائد على جميع مكونات المجتمع، بما في ذلك الأفراد والمؤسسات العامة والخاصة، لاستخدام هذه التكنولوجيا، حيث أصبح الاستفادة من الشبكة العالمية للمعلومات والتكنولوجيا المرتبطة بها من أجهزة الكمبيوتر والشبكات الأخرى عرضة للهجمات. تقف النصوص التقليدية عاجزة في وجه هذه الاعتداءات على خصوصية الفرد وأسراره، لذلك أصبحت هناك حاجة ملحة لملء الفراغ التشريعي في حماية المعلومات والأسرار المتداولة على هذه الشبكة، وحماية الاتصالات والمراسلات بين الناس.

ثانياً: الركن المعنوي

هي الحالة العقلية للمجرم، أي وجود سوء نية وإرادة حرة وواعية للوصول إلى الشبكة، مما يسبب الضرر أو الوصول بقصد سرقة وإتلاف البيانات وغيرها من الجرائم، مثل مهاجمة المعلومات الخاصة بالمنظمات الحكومية أو الخاصة أو المملوكة للأفراد بقصد تدميرها كلياً أو جزئياً أو التقليل من فائدتها مما يؤدي إلى إلحاق الضرر بمالكي المعلومات، ويمكن تقسيم الركن المعنوي إلى محورين هما:

1. الاعتداء على نظام تشغيل بخلق مشكله تؤدي إلى تباطؤ النظام في تنفيذ العمليات المطلوبة مثل معالجة المعلومات واسترجاعها وإرسالها، ما يكون له الأثر السلبي على أداء المنظمة.
2. الوصول غير المصرح به إلى الأنظمة الإلكترونية للمؤسسة، وفي هذه الحالة يتم تدمير البيانات والمعلومات الموجودة في النظام تماماً، أو يعد تعديل

المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)
العدد الرابع والخمسون (تشرين الأول) 2022
ISSN: 2617-9563
www.mecsj.com/ar/

وتشويه البيانات والمعلومات عقبة أمام المنظمة لمواصلة تنفيذ عملياتها أو تقييد الصوت. صناعة القرار. الهجوم على المعلومات هو احتيال وجريمة متعمدة، والمكون الأخلاقي في هذا النوع من الجريمة هو النية الإجرامية التي يجب أن تتحقق في الجريمة.

ثالثاً: الركن المادي

هذه الركيزة هي النشاط الإيجابي والسلوك المادي المتعلق بالبيئة الرقمية واتصال الشبكة، ومعرفة الهدف وطريقة ونتائج هذا النشاط، مثل تشغيل الكمبيوتر وتوصيله بالإنترنت، وإعداد البرامج اللازمة، لهذا يخترق الأجهزة المستهدفة، أو يحضر ويحقن فيروسات مدمرة بهدف الإضرار بهذا الهدف، حيث يرتبط بالتدمير الجزئي أو الكلي للجانب المادي لأنظمة المعلومات التي تفقد القدرة على أداء عمل المنظمة، وبالتالي لا تحقق الفائدة التي من أجلها تم إنشاء هذا النظام الإلكتروني.

المطلب الثاني: أنواع الجرائم الإلكترونية

للجرائم السيبرانية أشكال كثيرة ومتعددة، وتختلف الآراء في تحديد أنواع الجرائم الإلكترونية، وهناك العديد من التصنيفات بعضها مصنّف حسب موضوع الجريمة ، والقسم الآخر حسب طريقة ارتكابها، لكنهم جميعاً متفقون على الوسائل المستخدمة في ارتكابها، ألا وهي التكنولوجيا الحديثة، التي هي أجهزة مثل أجهزة الكمبيوتر وما شابهها كلها مصنوعة عبر الإنترنت.

هناك العديد من أشكال الهجمات والجرائم، ووسائل وأهداف ارتكابها، بما في ذلك الوصول غير القانوني، وتخريب المعلومات، ومنع الوصول إلى معلومات الكمبيوتر، ومصادرة المواد أو المعلومات الحاسوبية، ما يفعله الكمبيوتر والإنترنت وأنظمة المعلومات، وبالتالي أشكال وصور هذه الهجمات تتضاعف بتعدد الإجراءات التي يمكن القيام بها من خلال استخدام الكمبيوتر والإنترنت، مثل السرقة والاحتيال، وغسل الأموال، والقدح، والذم، والتزوير وغيرها من الجرائم المتعلقة بالأمن القومي.

أولاً: الجرائم الواقعة على الأموال.

وسيتم تناول هذه الجرائم كما يلي:

1. **جرائم التحويل الإلكتروني للأموال:** ويهدف نظام التحويل الإلكتروني إلى منح البنك سلطة إجراء التحويلات الدائنة والمدينة إلكترونياً من حساب مصرفي إلى حساب مصرفي آخر. حددت لجنة الأمم المتحدة للقانون التجاري الدولي نظام التحويل الإلكتروني للأموال بأنها: (عملية تبادل القيم المادية، يتم فيها تنفيذ مرحلة أو أكثر بالوسائل الإلكترونية، بعد أن تم تنفيذ هذه المرحلة في الماضي بالطرق التقليدية والوسائل المكتوبة).

تتم سرقة الأموال من قبل وسائل الإعلام من خلال اختلاس البيانات والمعلومات الشخصية للضحايا، واستخدام شخصية الضحية لتنفيذ عملية التخفي، مما يؤدي بالبنك إلى تحويل الأموال الإلكترونية أو المادية إلى الجاني، ويستخدم الجاني الكمبيوتر للوصول إلى الإنترنت والوصول إلى البنوك وتحويل أموال العميل إلى حسابات أخرى.

المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)
العدد الرابع والخمسون (تشرين الأول) 2022
ISSN: 2617-9563
www.mecsj.com/ar/

ومن أبرز شبكة التحويلات المالية شبكة السويفت (Swift) حيث يقصد بنظام الفريد الإلكتروني للأموال بمعنى System Electronic Funds Transfer Swift، وهو نظام يستخدم على نطاق واسع في البنوك الوطنية لتسوية المدفوعات المالية بالوسائل الإلكترونية، حيث يتم ذلك عن طريق توجيه أمر من المدين إلى مصرفه للدفع من حسابه إلى الدائن إلكترونياً، أو عن طريق اتخاذ الإجراءات المصرفية اللازمة لتحويل مبلغ معين إلى الحساب المصرفي للمستفيد، أو عن طريق توجيه الدائن لأمر حسابه، أو أن يقوم البنك بتحصيل مبلغ من حسابه المدين بناءً على تفويض مسبق بوسائل إلكترونية.

2. **غسيل الأموال تمارس عبر الأنترنت:** ويستفيد الجناة مما وصلت إليه التقنية المعلوماتية لتوسيع نشاطهم الغير مشروع في غسيل أموالهم، بتوفير السرعة، وتفادي الحدود الجغرافية، والقوانين المعيقة لغسيل الأموال، وكذا لتشفير عملياتهم وسهولة نقل الأموال واستثمارها لإعطائها الصبغة الشرعية.

ولقد عرّف المشرع العماني جريمة غسيل الأموال بأنها (كل فعل من الأفعال المنصوص عليها في المادة (٦) من هذا القانون).

وتنص المادة (6) من هذا القانون على أنه: (يعد مرتكباً لجريمة غسل الأموال كل شخص، سواء أكان هو مرتكباً للجريمة الأصلية أم شخص آخر، يقوم عمداً بأحد الأفعال الآتية، مع أنه يعلم، أو كان عليه أن يعلم أو يشتبه بأن الأموال عائدات جريمة:

أ- استبدال أو تحويل الأموال بقصد تمويه أو إخفاء طبيعة ومصدر تلك العائدات غير المشروعة، أو مساعدة شخص قام بارتكاب الجريمة الأصلية للإفلات من العقوبة.

ب- تمويه أو إخفاء الطبيعة الحقيقية للأموال أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو ملكيتها أو الحقوق المتعلقة بها.

ج- تملك الأموال أو حيازتها أو استخدامها عند تسلمها).

إذن، وتُعرف جريمة غسيل الأموال بأنها: (مجموعة عمليات معينة ذات طبيعة اقتصادية أو مالية تؤدي إلى إدخال الأموال دائرة الاقتصاد الشرعي رؤوس أموال ناتجة من أنشطة غير مشروعة تقليدياً متعلقة بالمتاجرة بالمخدرات أو الإتجار بالبشر واليوم أصبحت نواتج كل جريمة جنائية ذات جسامة أو خطورة). وأن هذا التعريف شامل ومختصر مقارنة بالتعريف الموجود في القانون العماني.

وتمر عملية غسيل الأموال بالمراحل التالية:

- **مرحلة الإيداع أو التوظيف:** حيث يتم إيداع الأموال الناتجة عن أنشطة غير مشروعة في الشركات أو البنوك المالية، مما يعني إيداع الأموال غير المشروعة في المؤسسات أو البنوك.
- **مرحلة التقييم والتمويه:** حيث يتم إجراء سلسلة من العمليات لإخفاء المصدر غير المشروع للأموال، حيث يقوم الغاسل بإنشاء مجموعات متعددة من الصفقات التجارية والتحويلات مثل الاستثمار في عدة دول أجنبية.
- **مرحلة التكامل:** وتهدف هذه المرحلة إلى إضفاء الشرعية على تلك الأموال وإعادة الأموال في شكل عوائد نظيفة لا تخضع للضريبة.الاستعمال الغير

المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)
العدد الرابع والخمسون (تشرين الأول) 2022
ISSN: 2617-9563
www.mecsj.com/ar/

الشرعي للبطاقات الائتمانية رافق استخدام البطاقات الائتمانية، الاستيلاء عليها باعتبارها نقود إلكترونية، إما بسرقة أرقام البطاقات ثم بيع المعلومات للآخرين، من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الحاسب الآلي للضحية عن طريق الاحتيال، وذلك بإيهامه بحصول ربح، فيقدم الضحية معلومات تمكن الجاني من التصرف في ماله، أو إساءة استخدام الغير للبطاقات الائتمانية، كأن يقوم السارق استعمال البطاقة للحصول على السلع والخدمات أو سحب مبالغ مالية بموجبها من أجهزة التوزيع الآلي أو السحب باستخدام بطاقات مزورة.

ثانياً: الجرائم الواقعة على الأشخاص

رغم إيجابيات الحاسب الآلي والشبكة المعلوماتية، إلا أنها جعلته أكثر عرضة للانتهاك، وفيما يلي عرض بعض الجرائم التي ترتكب بواسطة النظام المعلوماتي عن طريق الإنترنت.

1. **انتحال الهوية:** هو استخدام شخصية الفرد للاستفادة من ماله أو سمعته أو مركزه، وقد اتسم بسرعة انتشاره خاصة في الأوساط التجارية. يتم جمع قدر كبير من المعلومات الشخصية المراد انتحالها، لاستخدامها في ارتكاب جرائمه عن طريق إغراء الشخص بتقديم معلوماته الشخصية الكاملة، مثل الاسم والعنوان الشخصي ورقم بطاقة الائتمان ليتمكن من الوصول إلى أمواله أو السمعة من خلال الاحتيال.

2. **انتحال شخصية أحد المواقع:** ويتم ذلك عن طريق اختراق أحد المواقع للسيطرة عليه، ليقوم بتركيب برنامج خاص به هناك، باسم الموقع المشهور.

3. **جرائم العنف على الإنترنت:** وجد العاملون في مجال المواد الإباحية ونشر الصور الإباحية على الإنترنت طريقة فعالة وجذابة ومغرية للدعوة إلى الفجور والدعارة، من خلال الإعلانات الإلكترونية على مواقع الإنترنت المنتشرة على الإنترنت، ضمن إطار من التقنية الفنية التي يستخدمها الجاني في ارتكابه الجريمة وصعوبة اكتشاف هذه الجرائم وتحديد مصدرها وإثبات الأدلة عليها، إضافة إلى عدم وجود تشريعات حديثة لمواجهة مثل هذه الجرائم الأخلاقية التي تُرتكب عبر الإنترنت، وانتشار الجرائم ضد المواطنين. والأخلاق والمواد الإباحية على الإنترنت هي نشر الصور غير الأخلاقية والممارسات الفاسدة.

4. **جريمة التهديدات:** وهي التهديدات التي يقصد بها بث الخوف في النفس بالضغط على إرادة الشخص وإخافته من الأذى الذي قد يصيبه أو من تربطه به علاقة أو أموال الغير، والضرر الفعلي غير مطلوب، أي تنفيذ التهديدات، لأنه يشكل جريمة أخرى في حد ذاتها خارج إطار التهديدات على التنفيذ الفعلي، وقد تكون التهديدات مصحوبةً بجرم الذي هو طلب للتصرف أو الامتناع عن فعل شيء ما، أو لمجرد الانتقام. أصبح الإنترنت وسيلة

لارتكاب جرائم تهديدات والتي تحتوي في حد ذاتها على عدة وسائل لإيصال التهديدات للضحية بسبب النوافذ الموجودة في المعرفة مثل البريد الإلكتروني أو الويب.

5. **التعدي على الحياة الخاصة**: تتمتع الحياة الخاصة للأشخاص بحماية دستورية وقانونية، ويمكن استخدام نظام المعلومات للهجوم على قدسية الحياة الخاصة، كما لو أن شخصاً يعمل في نظام المعلومات قد أعد ملفاً يحتوي على معلومات عن شخص دون علمه وبدون إذنه، وهذا الشخص أفشاها للآخرين دون إذن المالك، كما في حالة الأسرار المودعة لدى المحاسبين أو المحامين أو الأطباء، فكل هذه الأسرار محمية بالقانون وتم إفشاؤها بشكل غير قانوني بدون موافقة المالك. ويمكن ارتكاب جريمة التعدي على الخصوصية وكشف الأسرار أو إفشاؤها عن طريق نشر المعلومات على جهاز الكمبيوتر وفتح السجلات الإلكترونية وعرضها من خلال شاشة الكمبيوتر. وضمن نطاق جرائم التعدي على الحياة الخاصة جريمة تسجيل المحادثات الشخصية أو مراقبتها بأي وسيلة، حيث نجد أن بعض المتسللين يمكنهم اختراق الإنترنت بوسائل غير مشروعة والتنصت على هذه المكالمات. ويعتبر السر معلومات أو أخباراً، والإفشاء هو جوهر نقل المعلومات ونوع من الأخبار ووسيلة للآخرين للوصول إلى المعلومات التي تعتبر نوعاً من الأسرار الشخصية التي لا يرغب المالك في إبلاغ الآخرين بها ورغبته في إخفاء هذا السر، وهذه الرغبة هي ما يحترمه المشرع، وهي خلل في إفشاء الأسرار على الإنترنت.

6. **جرائم القذف:** والقذف هو إسناد حقيقة معينة تستوجب العقاب لمن ينسب إليه أو يحتقره بإسناد عام وعمودي يشير إلى إسناد الأمر إلى الشخص على سبب التثبيت. يشمل السب والقذف نسب حقيقة معينة إلى شخص ما ولا يشمل ذلك القذف، أو الإضرار بشرف الآخرين وسمعتهم ومراعاة الآخرين، والسب والقذف كتابة، أو بالطباعة أو الرسم، عبر البريد الإلكتروني، أو ملفات صوتية، أو صفحات ويب تتعلق بالشرف ينشر المجرم معلومات خاطئة عن الضحية، وقد يكون شخصاً طبيعياً أو اعتبارياً، بحيث تصل المعلومات المراد نشرها إلى أعداد كبيرة من مستخدمي الإنترنت.

7. **التشهير**: التشهير هو أن ينشر المجرم معلومات يحتمل أن تكون سرية أو مضللة أو خاطئة عن ضحيته، والتي قد تكون فرداً أو شركة أو منظمة سياسية، أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين، وتشمل هذه الجرائم أيضاً التشهير والشائعات والأخبار الكاذبة لمحاربة الرموز السياسية والفكرية وحتى الدينية حتى يشكك الناس في مصداقية هؤلاء الأفراد وقد يكون الهدف ابتزازهم.

المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)
العدد الرابع والخمسون (تشرين الأول) 2022
ISSN: 2617-9563
www.mecsj.com/ar/

ثالثاً: جرائم متعلقة بالأمن القومي

1. **الإرهاب:** تستخدم الجماعات الإرهابية حالياً تكنولوجيا المعلومات لتسهيل الأشكال النموذجية للأعمال الإجرامية، ولا تتردد في استخدام وسائل متطورة مثل الاتصال والتنسيق، وبث الأخبار الكاذبة، وتوظيف بعض الشباب، وتحويل بعض الأموال لتحقيق أهدافها. يستخدم الإرهابيون الإنترنت لاستغلال مؤيدي أفكارهم، وجمع الأموال لتمويل برامجهم الإرهابية، والاستيلاء على مواقع الويب الحساسة، وسرقة المعلومات، والقدرة على نشر الفيروسات بسبب العدد المتزايد من برامج الكمبيوتر القوية وسهلة الاستخدام التي يمكن تنزيله مجانًا.
2. **التجسس:** يقوم المجرمون بالتجسس على الدول والمنظمات والشخصيات والمؤسسات الوطنية أو الدولية، وتستهدف، وخاصة التجسس العسكري، والسياسي، والاقتصادي، وذلك باستخدام التقنية المعلوماتية تمارس من قبل دولة على دولة أخرى، أو من شركة على شركة، وذلك بالاطلاع على المعلومات الخاصة المؤمنة في جهاز آلي، وغير مسموح بالاطلاع عليها، كأن تكون من قبيل أسرار الدولة.

وأخيراً، من خلال هذا البحث، استطاع الباحث استخلاص النتائج والتوصيات التالية:

المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)
العدد الرابع والخمسون (تشرين الأول) 2022
ISSN: 2617-9563
www.mecsj.com/ar/

أولاً: النتائج

1. لم يتطرق قانون المعاملات الإلكترونية العماني في أحكامه المسائل المتعلقة بالجرائم الإلكترونية ومكافحتها، وأن قانون مكافحة جرائم تقنية المعلومات هو الذي تسود أحكامه لمكافحة الجرائم الإلكترونية.
2. أن الجرائم الإلكترونية تلحق أضراراً خطيرة بالأفراد والمؤسسات والشركات، حيث ينبغي أن تطور صناعة التجارة الإلكترونية، حيث يشعر المستخدمون بالتهديد من جراء هذه الأعمال الإجرامية، حيث أن معظمهم يرى من أن احتمال ارتكاب جرائم إلكترونية تؤدي إلى الإضرار بهم بشدة.
3. لا يؤثر ذلك على المستخدمين فحسب، بل يؤثر أيضاً على أعمال التجارة الإلكترونية، حيث ينتشر الخوف في جميع أنحاء العملاء، لذا سيؤدي ذلك إلى سقوط المستخدمين في الصناعة، وبهذه الطريقة تخسر الصناعة مبلغاً كبيراً من المال.
4. وفي معظم الحالات التي يتم تنفيذ الجرائم الإلكترونية، يكون الشخص المسؤول متسللاً، أو لديه بعض الخبرة في مجال الكمبيوتر نسبياً.
5. تشمل الجرائم الإلكترونية الإرهاب الإلكتروني والسرقة الإلكترونية والتجسس والاحتيالات الخطيرة.

ثانياً: التوصيات

1. على المشرع العماني وضع أحكاماً منوطة بمكافحة الجرائم الإلكترونية في قانون المعاملات الإلكترونية العماني، وأن قانون مكافحة جرائم تقنية المعلومات لا يُترك وحده لمكافحة الجرائم الإلكترونية، لكون هذه الجرائم لها علاقة بالتجارة الإلكترونية.
2. اتخاذ خطوات جادة للقضاء على الجرائم الإلكترونية، كونها تلحق أضراراً خطيرة، حيث ينبغي أن تطور صناعة التجارة الإلكترونية، حتى يشعر المستخدمون بالتهديد من جراء هذه الأعمال الإجرامية، لكي لا تؤدي هذه الجرائم إلى الإضرار بهم.
3. الحاجة الماسة والملحة للتعاون وتدخل الحكومات ومؤسسات الأمن السيبراني الخاصة من أجل تأمين الإنترنت وجعله آمناً لاستخدام الجميع.
4. إيجاد تشريعات حديثة لمواجهة مثل هذه الجرائم الأخلاقية التي تُرتكب عبر الإنترنت، وانتشار الجرائم ضد المواطنين. والأخلاق والمواد الإباحية على الإنترنت هي نشر الصور غير الأخلاقية والممارسات الفاسدة.

المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)
العدد الرابع والخمسون (تشرين الأول) 2022
ISSN: 2617-9563
www.mecsj.com/ar/

المراجع

1. إبراهيم الخضيري. (2004م). **الجرائم المعلوماتية**. بيروت: دار العلم. ط1.
2. إبراهيم السقا. (2008م). **جريمة التزوير في المحررات الإلكترونية**. الإسكندرية: دار الجامعة الجديدة. ط1.
3. إبراهيم شاكر. **جرائم الإنترنت**. الأردن: دار المسرة. ط1.
4. اتفاقية بودابست المتعلقة بالإجرام الالكتروني "الإجرام المعلوماتي" والموقعة من الاتحاد الأوروبي، لعام 2001م.
5. اتفاقية بودابست المتعلقة بالإجرام الإلكتروني "الإجرام المعلوماتي" والموقعة من الاتحاد الأوروبي، لعام 2001م.
6. أحمد خليفة الملط. (2006م). **الجرائم المعلوماتية**.الإسكندرية: دار الفكر الجامعي. ط1.
7. أحمد وهدان. (2004م). تقييم فعاليات المواجهة التشريعية لجرائم الإنترنت. الشارقة. القيادة العامة لشرطة الشارقة. مركز بحوث الشرطة. **دورية الفكر الشرطي**. العدد 1. المجلد 13.
8. أسامة المناعسة وآخرون. (2001م). **جرائم الحاسب الآلي والإنترنت: دراسة تحليلية مقارنة.** عمان: دار وائل. ط1.
9. جودة حسين محمد. **(2000م). "المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية: دراسة مقارنة".** بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت. بكلية الشريعة والقانون. جامعة الإمارات العربية المتحدة.
10. حسن أحمد الشهري. (2009م). قانون دولي موحد لمكافحة الجرائم الإلكترونية: تصور مقترح، **المجلة العربية للدراسات الأمنية والتدريب.** العدد 53. المجلد 27.
11. حسين بن سعيد الغافري. (2009م). **السياسة الجنائية في مواجهة جرائم الإنترنت: دراسة مقارنة.** القاهرة: دار النهضة العربية. ط1.
12. خالد ممدوح إبراهيم. (2009م). **الجرائم المعلوماتية**. الإسكندرية: دار الفكر الجامعي. ط2.
13. رامي متولي القاضي. (2011م). **مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية**. القاهرة: دار النهضة العربية. ط1.
14. سالم مدني. (2007م). مدى إمكانية تطبيق الحدود على الجرائم الإلكترونية. ورقة عمل مقدمة إلى ندوة المجتمع والأمن: الجرائم الإلكترونية: الملامح والأبعاد. الرياض.

15. سرحان حسن المعيني. (2011م). التحقيق في جرائم تقنية المعلومات، الشارقة. القياد العامة لشرطة الشارقة. **دورية الفكر الشرطي.** المجلد 2. العدد 4. 79.
16. صالحة العمري. (2000م). جريمة غسيل الأموال وطرق مكافحتها. **مجلة الاجتهاد القضائي**. العدد 5. المجلد 7. جامعة محمد خيضر. بسكرة.
17. صغير يوسف. (2013م). **"الجريمة المرتكبة عبر الإنترنيت".** بحث مقدم ومتطلب لنيل درجة الماجستير في قانون الأعمال. كلية الحقوق والعلوم السياسية. قسم الحقوق،. جامعة مولود معمري. تيزي وزو.
18. عباس أبو شامة. (1999م). التعريف بالظواهر الإجرامية المستحدثة: حجمها، أبعادها، ونشاطها في الدول العربية، الندوة العلمية للظواهر الإجرامية المستحدثة وسبل مواجهتها. تونس. جوان.
19. عبد العال الدريبي. (2013م). **الجريمة الإلكترونية بين التشريع والقضاء في الدول الغربية**. القاهرة: المركز العربي لأبحاث القضاء الإلكتروني. ط1.
20. عبد الفتاح بيومي حجازي. (2006م). **مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي**. الإسكندرية: دار الفكر الجامعي. ط1.
21. عبد القادر شاة. (2019م). **كيفية التعامل مع الجرائم الإلكتروني.** القاهرة: دار الحقوق. ط2.
22. عبد اللطيف محمود ربايعة. (2016م). الجرائم الإلكترونية: التجريم والملاحقة والإثبات. بحث مقدم إلى المؤتمر الأول للجرائم الإلكترونية في فلسطين، المنعقد في جامعة النجاح الوطنية. نابلس.
23. عزت الشحات. (2003م). **الجرائم الإلكترونية.** القاهرة: دار أمين. ط1.
24. عوض البنا. (2008م). **الجرائم الإلكترونية والتجارة الإلكترونية.** القاهرة: دار الكتب الجامعية. ط1.
25. غازي عبد الرحمن هيان الرشيد. (2004م). **"الحماية القانونية من جرائم المعلوماتية: الحاسب والإنترنت".** بحث مقدم ومتطلب لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية. كلية الحقوق. قسم الحقوق. لبنان.
26. فاديا سليمان. (2005م). الجرائم المعلوماتية وأثرها على العمليات المالية والمصرفية. **مجلة الدراسات المالية والمصرفية.** العدد 1. المجلد 3. الأكاديمية العربية للعلوم المالية والمصرفية. عمان. الأردن.

27. فايز بن عبد الله الشهري. (2000م). التحديات الأمنية لوسائل الاتصال الجديدة: دراسة الظاهرة الإجرامية على شبكة الإنترنت. **المجلة العربية للدراسات الأمنية والتدريب**. العدد 39. المجلد 20.
28. فتوح الشاذلي. (2003م). **جرائم الكمبيوتر**. بيروت: منشورات الحلبي الحقوقية. ط1.
29. قانون الجزاء العماني، بمرسوم سلطاني رقم (٧)، لسنة ٢٠١٨م.
30. قانون المعاملات الإلكترونية العماني لعام 2008م.
31. قانون المعاملات والتجارة الإلكترونية رقم (2) لسنة 2002م.
32. قانون مكافحة غسل الأموال وتمويل الإرهاب، بمرسوم سلطاني رقم (٣٠)، لسنة ٢٠١٦م.
33. لطفي سعد. (2012م). **الجرائم الإلكترونية والقانون.** القاهرة: دار القانون. ط1.
34. محمد الشوابكة. (2004م). **جرائم الحاسوب والإنترنت الجريمة المعلوماتية.** الأردن: دار الثقافة. ط1.
35. محمد أمين الرومي. (2004م). **جرائم الكمبيوتر والإنترنت**. القاهرة: دار المطبوعات الجامعية. ط1.
36. محمد بن عبد الله بن علي المنشاوي. (2003م). **"جرائم الإنترنيت في المجتمع السعودي".** بحث مقدم ومتطلب لنيل درجة الماجستير في العلوم الشرطية. أكاديمية نايف العربية للعلوم الأمنية. الرياض.
37. محمد حماد الهيتي. (2004م). **التكنولوجيا الحديثة والقانون الجنائي.** الأردن: دار الثقافة. ط1.
38. محمد سامي الشواء. (2002م). **السياسة الجنائية في مواجهة غسيل الأموال**. القاهرة: دار النهضة العربية. ط1.
39. محمد شاهاتة. (20005م). **المذكرة التفسيرية للاتفاقية الأوروبية حول الجريمة الافتراضية**. القاهرة: دار الترجمة. ط1.
40. محمد علي العريان. (2004م). **الجرائم المعلوماتية**. الإسكندرية: دار الجامعة الجديدة. ط1.
41. محمد محمد شتات. (2001م). **فكرة الحماية الجنائية لبرامج الحاسب الآلي.** الإسكندرية: دار الجامعة الجديدة. ط1.
42. محمود عبابنة. (2010م). **جرائم الحاسوب وأبعادها الدولية.** الأردن: دار الثقافة. ط1.
43. مصطفي محمد موسي. (2008م). **التحقيق الجنائي في الجرائم الإلكترونية**. القاهرة: دار النهضة العربية. ط1.

44. مفيد الزيدي. (2003م). **قضايا العولمة والمعلوماتية**. الأردن: دار أسامة. ط1.
45. نائلة عادل فريد. (2005م). **جرائم الحاسب الاقتصادية: دراسة نظرية وتطبيقية**. بيروت: منشورات الحلبي الحقوقية. ط1.
46. هشام محمد فريد رستم. (2000م). **"القانون والكمبيوتر والإنترنت".** بحث مقدم ومتطلب لنيل درجة الماجستير في القانون. جامعة الإمارات العربية المتحدة. كلية الحقوق. قسم الحقوق.
47. هلال عبد الله أحمد. (2002م). **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة.** القاهرة: دار النهضة العربية. ط1.
48. هلالي عبده. (2007). **الجرائم المعلوماتية عابرة الحدود.** القاهرة: دار النهضة. ط1.
49. يونس عرب. (2009م). التدابير التشريعية العربية لحماية المعلومات والمصنفات الرقمية. ورقة عمل مقدمة أمام الندوة العلمية الخامسة حول دور التوثيق والمعلومات في بناء المجتمع العربي. النادي العربي للمعلومات. دمشق.
50. يونس عرب. (2002م). جرائم الكمبيوتر والإنترنت. ورقة عمل مقدمة إلى مؤتمر الأمن العربي. تنظيم المركز العربي للدراسات والبحوث الجنائية. أبو ظبي.