مجلة الدراسات القانونية والاقتصادية

# الأمن السيبراني وحماية الأنظمة الإلكترونية
## دراسة تحليلية تأصيلية

الدكتور/ راشد محمد المري
عضو هيئة التدريس بأكاديمية سعد العبد الله للعلوم الأمنية

الملخص باللغة العربية :

الأمن في الفضاء السيبراني أمر اهتمت به الدول في كل مكان في العالم، بغض النظر عن مدى تواجدهم في هذا الفضاء، مما يعنى ارتباط أمن المعلومات ارتباطاً عضوياً بالأمن القومي في معظم دول العالم، ذلك أن الاعتداء على البنى التحتية المهمة منها الاتصالات الأنظمة الإلكترونية يمكن أن يؤثر على كل الدول في منطقة جغرافية معينة، المؤثر بدوره المباشر على مصالح الدولة المعنية بالفضاء السيبراني، والتى تشكل بنيتها التحتية للاتصالات والمعلومات جزءاً من تركيبة البنية التحتية للفضاء السيبراني.

لذا احتل الاهتمام بأمن المعلومات المراكز الأولى في اهتمامات واضعي السياسات العامة في أغلب الدول، وعلى كل المستويات سواء الإقليمية أو المحلية، فالدولة لأنها المنتج الأكبر للبيانات والمعلومات العامة والخاصة، هي المعنية بالأمن السيبراني، كما أنها المتحكمة في وضع النظم والقواعد التى تحدد الضوابط والحدود.

ومما لا شك فيه أن العالم أصبح يعاني من مشكلات اجتماعية أفرزتها البيئة الرقمية، بيد أن هذه المشكلات أصبحت مساراً للبحث والدراسة لاسيما في مجال علم الاجتماع، ففي ظل ما يشهده العالم من تطور سريع ومتزايد في النظم الذكية والأجهزة الإلكترونية وما صاحبهما من هجمات وجرائم سيبرانية مثل الغزو الثقافي الرقمي، والجريمة السيبرانية، والابتزاز والتنمر عبر الأنظمة الإلكترونية، غدت الضرورة ملحة لنشر دعائم الأمن السيبراني وتأمين سلامة الممارسة الإلكترونية، وفي ضوء هذه البيئة المتغيرة ثمة حاجة ملحة لاتخاذ إجراءات على الصعيدين المحلي والدولي لحماية الاستهلاك والخصوصية ومجابهة تقنية المعلومات ضد جميع أشكال الجريمة السيبرانية.

**الكلمات المفتاحية:** الأمن السيبراني، الجرائم السيبرانية، البيئة الرقمية، الغزو الثقافي، الأنظمة المعلوماتية، الحاسب الآلي، المستندات الإلكترونية.

**Cyber Security and Protection of Electronic Systems**

(ISSN: 2356 - 9492)

**Abstract** :

Security in cyberspace is something that countries everywhere in the world have taken care of, regardless of their presence in this space, which means that information security is organically linked to national security in most countries of the world, because the attack on important infrastructures, including communications and electronic systems, can It affects all countries in a specific geographical area, which in turn directly affects the interests of the country concerned with cyberspace, whose communications and information infrastructure forms part of the composition of the infrastructure of cyberspace.

Therefore, interest in information security occupied the first positions in the concerns of public policy makers in most countries, and at all levels, whether regional or local. The state, because it is the largest producer of public and private data and information, is concerned with cybersecurity, and it also controls the development of systems and rules that define controls and limits.

There is no doubt that the world has become suffering from social problems produced by the digital environment. However, these problems have become a path for research and study, especially in the field of sociology, in light of the rapid and increasing development that the world is witnessing in smart systems and electronic devices, and the accompanying attacks and cybercrimes such as Digital cultural invasion, cybercrime, extortion and bullying through electronic systems, it has become an urgent need to spread the foundations of cybersecurity and ensure the safety of electronic practice, and in light of this changing environment there is an urgent need to take action at the local and international levels to protect consumption and privacy and confront information technology against all forms of cybercrime .

**Keywords:** cybersecurity, cybercrime, digital environment, cultural invasion, information systems, computers, electronic documents.

مقدمة :

مع بداية القرن العشرين برزت الثورة المعلوماتية، نتيجة التقدم العلمي التكنولوجي التقني استخدام الحاسب الآلي والأنظمة والشبكات العاملة عليه، وبالتالي ظهرت معه الجرائم الإلكترونية منذ نشأة الأجهزة الإلكترونية الحديثة وحتى وقتنا هذا، وصاحبت هذه الجرائم أيضاً ظهور البيانات والمعلومات والمستندات الإلكترونية بأشكالها وأنواعها المختلفة مثل العقود والشيكات والتوقيعات والسجلات الإلكترونية(١).

وأدى التطور والانفتاح التكنولوجي الذى نعيشه اليوم مع الأنظمة الإلكترونية إلى تزايد الاعتماد على هذه التكنولوجيات في التنمية الاقتصادية والاجتماعية، إلا أن الانفتاح جعلها عرضة للتعديات والأنشطة الإجرامية من قبل مخترقي الشبكات، لذلك من الضروري وضع الأطر القانونية والتنظيمية والإجرائية لمواجهة المخاطر السيبرانية وتوعية المؤسسات والأفراد حول المخاطر وآثارها على أعمالهم وحياتهم الشخصية(٢).

أهمية البحث:

تأتي أهمية البحث نظراً لأننا أمام مرحلة جديدة في مجال النظم المعلوماتية باعتبارها ظاهرة إنسانية واقتصادية واجتماعية لا يمكن أن تتطور بذاتها، كما تكمن أهمية الدراسة من خلال إلقاء الضوء على هذا الجاني، ومدى تأثير انتشار ثقافة أمن المعلومات وحماية الأنظمة الإلكترونية لأفراد المجتمع لمواجهة التحديات التى يحملها مستقبل الغد.

مشكلة البحث:

تتبلور إشكالية البحث في أن هذه الدراسة تثير قضية بحثية في مجال علم الاجتماع ألا وهي الأمن السيبراني، وفي ضوء هذه المخاطر ينطلق البحث الراهن للوقوف على أهم ركائز وممارسات الأمن السيبراني اجتماعياً ومجتمعياً من خلال:

(١) راشد محمد المري: الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر: دراسة مقارنة، القاهرة، دار النهضة العربية، ٢٠١٨، ص١٢.

(2) Fortin, Anne and Heroux, S., (2020), (Cybersecurity disclosure by the companies on the SPP/TSX60, index, vol:19, issue:2, June, pp:73-100.

(ISSN: 2356 - 9492)

١- ما هي الأبعاد الاجتماعية التى أدت لظهور الأمن السيبراني التى يبرز المخاطر والتهديدات الاجتماعية ؟

٢- ما هو تأثير التطورات التقنية للأنظمة الإلكترونية على الأمن السيبراني.

٣- ما هي الأطر التشريعية والتنظيمية للأمن السيبراني التى تعكس آليات المواجهة وسبل الحماية التشريعية والتنظيمية في تلك الدول ؟

أهداف البحث:

يهدف إلى تحديد المفهوم السليم لمدلول ومعنى وفحوى وسائل التقنية الحديثة وأساليبها، وكذا الصور والأدوات التى تنتهك بالممارسات الخاطئة التى تشكل السلوك الإجرامي للجرائم المعلوماتية والوصول لأفضل السبل لمواجهة ذلك السلوك الإجرامي.

منهجية البحث:

قد انتهجت أسلوبين يكمل أحدهما الآخر، فبجانب الإجراءات الأمنية لمواجهة جرائم الأنظمة الإلكترونية، قام البحث بجهود متعددة في جمع البيانات والمعلومات حول المشكلة البحثية، وكذلك المنهج القانوني للأمن السيبراني في حماية الأنظمة الإلكترونية كلما دعت الحاجة إلى الدراسة، والمساهمة في إيصال الرسالة الهادفة من أجل تحقيق الأمن السيبراني وحماية الأنظمة الإلكترونية.

خطة البحث:

الفصل الأول: ماهية الأمن السيبراني ويشتمل على ثلاثة مباحث:

المبحث الأول: مدخل إلى الأمن السيبراني والجريمة السيبرانية

المبحث الثاني: البنية التحتية للأمن السيبراني في دول العالم

المبحث الثالث: مسئولية مقدمي خدمات الأمن السيبراني

الفصل الثاني: ويتناول حماية الأنظمة الإلكترونية ويشتمل على ثلاثة مباحث:

المبحث الأول: الجريمة السيبرانية كتهديد للأمن السيبراني

المبحث الثاني: تأثير الإعلام في الوعى بالأمن السيبرانى

المبحث الثالث: الحماية الجنائية بالتشريع الكويتي والتشريعات المقارنة

وذلك على التفصيل التالي:

## الفصل الأول

## ماهية الأمن السيبراني

**تمهيد وتقسيم:**

مع تراجع مبادئ الأخلاق وضعف البيئة القانونية الحاكمة للمجال الافتراضي أصبحت معايير الأمن من أهم متطلبات المعاملات الإلكترونية، حيث ظهرت العديد من الآثار السلبية للاقتصاد الرقمي على بيئة الأعمال، خصوصاً فيما يتعلق بالأمن، حيث ظهرت الجرائم الإلكترونية والغش التجاري وانتهاك الخصوصية وسرية المعلومات، ومن هنا جاءت الدراسة التى يحاول الباحث من خلالها تحليل أثر أمن المعلومات على حماية الأنظمة الإلكترونية، وذلك بتحديد المخاطر التى تتعرض لها المؤسسات الاقتصادية وكيفية مواجهة تلك المخاطر. (٣)

فضلاً عن ذلك فإن المستثمرين في أي دولة في العالم إذا لم يجدوا من الأنظمة والقوانين ما يواجه الجرائم السيبرانية التى تقوض الصناعات المعلوماتية، وإذا لم يجدوا دعماً من الدولة، وحضوراً لأجهزتها لتنفيذ تلك الأنظمة والقوانين؛ فإنهم يبدلوا واجهتهم للاستثمار في هذا المجال وتطويره في مكان آخر، وهو ما يؤثر بالسلب على الاقتصاد(٤).

ويتناول هذا الفصل تعريف الأمن السيبراني ودوره في حماية الأنظمة الإلكترونية وذلك في ثلاثة مباحث، المبحث الأول يتناول مدخل إلى الأمن السيبراني والجريمة السيبرانية وأبعادها وأسبابها وبعض صورها، والمبحث الثاني: البنية التحتية للأمن السيبراني في دول العالم، والمبحث الثالث يشتمل على مسئولية مقدمي خدمات الأمن السيبراني، وذلك على الترتيب التالي:

المبحث الأول: مدخل إلى الأمن السيبراني والجريمة السيبرانية

---

(٣) لطيفة نايف سالم الريدين، أثر أمن المعلومات على الاقتصاد الرقمي مع التطبيق على عينة من عملاء بنك الكويتي الوطني، الكويت، مجلة البحوث الإدارية، مجلد ٣٩، عدد ١، ٢٠٢١م، ص ٢.

(٤) كامل فتحي كامل خضر، وسمر المداح، العلاقة بين الاقتصاد الرقمي وأمن المعلومات، دراسة تطبيقية على عينة من عملاء البنك الأهلي المصري، المجلة العلمية للاقتصاد والتجارة، المجلد ٥٠، العدد ٣، ٢٠٢٠م، ص ١٣.

(ISSN: 2356 - 9492)

المبحث الثاني: البنية التحتية للأمن السيبراني في دول العالم

المبحث الثالث: مسئولية مقدمي خدمات الأمن السيبراني

## المبحث الأول

## مدخل إلى الأمن السيبراني

## والجريمة السيبرانية

**تقديم:**

يرتبط الأمن ارتباطاً وثيقاً بأمن المعلومات، فالوصول إلى أمن المعلومات أو بثها أو حتى مجرد الإطلاع عليها هو ما يقف في الغالب وراء عمليات الاختراق للشبكات، والحديث عن الأمن يستدعى تعريف الخطر أي التهديد الذى يتعرض له النظام، بالإضافة إلى نقاط الضعف أو الثغرات التى تعتريه، ثم اتخاذ الإجراءات الأمنية المفروض اتخاذها، لدفع الخطر(٥) من الاختراق لأية معلومات أمنية أو شخصية تؤثر على المجتمع والدولة من مخاطر ذلك الفضاء السيبراني(٦)

**الأمن السيبراني لغوياً:**

مكون من لفظين يعنيان " الأمن: وهو النقيض لكلمة الخوف، والأمن مصدر الفعل أمن أمناً وأماناً وأمنة: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أمن من الشر، أي سلم منه. قال تعالى في كتابه العزيز: { وَإِذْ قَالَ إِبْرَاهِيمُ رَبِّ اجْعَلْ هَذَا بَلَداً آمِناً وَارْزُقْ أَهْلَهُ مِنَ الثَّمَرَاتِ }.

ويعرفه الاتحاد الدولي للاتصالات بأنه: "مجموعة من المهمات، مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات وممارسات وتقنيات تستخدم لحماية البيئة السيبرانية والمؤسسات والمستخدمين"(٧).

---

(٥) هشام محمد خليل: الجوانب الإجرامية للجوانب المعلوماتية، مجلس الأمن والقانون، عدد ٢، شرطة دبي، ٢٠١٢، ص٣٨.

(٦) نورة الصانع وآخرين: العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية لتلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف، مجلة البحث العلمي في التربية، ٢١ (٤)، الطائف ٢٠٢٠م، ص ٢٧٨-٣٠٦.

(٧) هشام محمد خليل: الجوانب الإجرامية للجوانب المعلوماتية، مجلس الأمن والقانون، عدد ٢، شرطة دبي، ٢٠١٢، ص٣٨.

**السيبرانية في الاصطلاح:**

تعددت التعاريف التى تناولت مصطلح السيبرانية كل حسب الزاوية التى نظر إليها منها، إلا أنها اشتركت في مضمون واحد متقارب في المعنى وهو "استهداف مواقع إلكترونية من خلال وسائل إلكترونية أخرى"،وهى مجموعة من الممارسات التى ترمى إلى حماية الأنظمة والشبكات والبرامج من الهجات الرقمية أياً كان نوعها، وهذه الممارسات متنوعة إلى تدابير احتياطية استباقية قبل وقوع الخلل، وعلاجية بعد وقوع الخلل. (٨)

ومفهوم الأمن السيبراني من المفاهيم التى لاقت اهتماماً كبيراً في الآونة الأخيرة نظراً لظهور تقنيات تكنولوجية جديدة، واستخدامها بشكل واقع في كافة المنشآت، وقد عرف NIST الأمن السيبراني بأنه حماية الأصول المعلوماتية من خلال معالجة التهديدات التى تتعرض لها المعلومات التى تتم معالجتها وتخزينها ونقلها بواسطة أنظمة المعلومات المتداخلة بين الشبكات(٩).

وقد عرفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI وهي وكالة مكلفة بالدفاع السيبراني الفرنسي، بأنه فضاء التواصل المشكل من خلال الربط البيني العالمي للمعدات المعالجة الآلية للمعطيات الرقمية، وأنه لا يقتصر ذلك فقط على شبكة الإنترنت، إنما يشمل شبكات عالمية وخاصة مثل (Gps/ AcARs/ swift/ psth (١٠)، وعرفه الكابتان Lento Martti & Nettaanmaki Pekka في كتابهما Automation and technology, Analytics: security cyber بأنه مجموعة من الإجراءات التى

(٨) حسين بن سليمان بن راشد الطيار، الأمن السيبراني في منظور مقاصد الشارع: دراسة تأصيلية، المملكة العربية السعودية، جامعة الطائف، مجلة جامعة الطائف للعلوم الإنسانية، المجلد ٦، العدد ٢١، ٢٠٢٠م، ٢٦٤.

(9) National institute of standards and technology (NIST) (2018), a Glossary of key information security terms National institute of standards and technology interagency or internal report. available at http://csrc.nist.gov/publications

(١٠) تغريد صفاء، لبنى خميس مهدي: أثر السيبرانية في تطور القوة، مجلة حامورابي للدراسات، بغداد، مركز حمورابي للبحوث والدراسات الإستراتيجية، ع٣٣-٣٤، السنة ٨، ٢٠٢٠م، ص١٤٩.

(ISSN: 2356 - 9492)

تتخذ في الدفاع ضد الهجمات السيبرانية، وعواقبها، وتنفيذ التدابير المضادة المطلوبة. [١١]، وفي تكوين رؤي حول كيفية تحسين وحوكمة أمن معلومات المنشأة وجهود إدارة المخاطر [١٢]

**مصطلحات البحث:**

الأمن السيبراني أو أمن الحاسوب أو أمن المعلومات أوCybersecurity، وهو أحد الفروع لعلم التكنولوجيا التى تهدف للوصول إلى المعلومات أو تغييرها أو إتلافها أو ابتزاز الأشخاص والدول للحصول على الأموال أو تعطيل العمليات التجارية[١٣]. وهناك العديد من المصطلحات المرتبطة بالأمن السيبراني نذكر منها[١٤]: " يعرّف على أنه منع الأعمال الضارة :(Cyber Deterrence) الردع السيبراني ضد الأصول الوطنية[١٥] في الفضاء الرقمي والأصول التي تدعم العمليات الفضائية، وهو أيّ فعل يقوّض من قدرات ووظائف :(Cyber Attacks) الهجمات السيبرانية"[١٦].

ويعرف إجرائياً: بأنه حماية الأفراد وبياناتهم وحساباتهم من الهجمات الإلكترونية، بهدف الحفاظ على سلامة ونزاهة المعلومات المخزنة داخل هذه الأنظمة الإلكترونية.

---

(١١) صاح مهدي هادي الشمري، زيد محمد علي إسماعيل، الأمن السيبراني كمرتكز جديد في الإستراتيجية العراقية، العراق، مجلة قضايا سياسية، السنة ١٢، العدد ٦٢، جامعة النهرين، كلية العلوم السياسية، ٢٠٢٠م، ص٢٧٧.

(12) Ramirez, M, Ariza, L., and Miranda, M., The disclosure of information on rsecurity in listed companies in Latin America- proposal for a cyber security disclosure index), journal of sustainability 2022, 14(3).

(١٣) الإستراتيجية الوطنية للأمن السيبراني ٢٠١٨-٢٠٢٣، وزارة الاتصالات وتكنولوجيا المعلومات، الأردن. ٢٠٢١م، ص ١٨.

(١٤) الأمن السيبراني: هيئة الإعلام، الكويت، قسم الدراسات والاتصال والعلاقات العامة، ٢٠٢١، ص ٢.

(١٥) ماجد بن خلاف حمود العنزي: الإرهاب السيبراني وانعكاساته على الأمن الوطني، جامعة نايف العربية للعلوم الأمنية، تم الاسترجاع بتاريخ ٢٠٢١/١/٣ على الموقع:
https://www.repository.nauss.edu.sa/handle/123456789/66752

(16) EVELYNE, JACQUES. (2020) REGULATING CYBERSECURITY What civil liability in case of cyber-attacks, p. 231.

الركـائز التـى يقـوم عليهـا الاقتصـاد الرقمـي: [١٧] هنـاك أربعـة ركـائز يقـوم عليهـا الاقتصاد الرقمي كالتالي:

١- البنية التحتية والتجهيزات التقنية.

٢- توفير البيئة القانونية المنظمة لتأمين المنافسة العادلة.

٣- قدرة القطاع المالي على توفير وتطوير الاستثمارات ورؤوس الأموال.

٤- القدرات البشرية والتى يمكن تسميتها رأس المال البشري.

**أهمية الأمن السيبراني:**

يرتبط الأمن المعلوماتي بالجريمة الإلكترونية التى هي أساس الأمن المعلوماتي الذى يعمل على مكافحتها، وعي عبارة عن جرائم ذكية تنشأ في البيئة الإلكترونية أو الافتراضية، حيث قوم بها أفراد أو منظمات لديهم درجة عالية من الذكاء ويمتلكون المعرفة والتقنية، مما يتسبب في خسائر فادحة للمجتمع، وتظهر أهميته في عالمنا المترابط بواسطة الشبكة العنكبوتية، حيث أصبح يمثل عنصراً مهماً في الحياة الإنسانية على كافة المستويات السياسية والاقتصادية والاجتماعية، فهو الآن عصب الحياة الحالية التى تعتمد عليها الدول والأفراد في كل معاملاتها، بل بات ينظر إليه بأنه رافد جديد للأمن القومي، وجزء من الأمن الجماعي، بما أن العلاقة بين الأمن والتكنولوجيا علاقة مترابطة ومتزايدة، مع إمكانية تعرض المصالح الإستراتيجية إلى مخاطر إلكترونية، الأمر الذى يهدد بتحول دور الأنظمة الإلكترونية لوسيط ومصدر لأدوات الصراع الدولي، ودوره في تغذية التورات الدولية. [١٨]

**خصائص الجريمة السيبرانية:**

الجريمـة السـيبرانية هـي امتـداد طبيعـي لنمـو أجهـزة الكمبيـوتر، وقـد نمـت الجريمـة السيبرانية بشكل هائل على مدى العقدين الماضيين، وتطورت الجريمة من قضية ثانوية

(١٧) حسين بن سليمان بن راشد الطيار، الأمن السيبراني في منظور مقاصد الشارع: دراسة تأصيلية، المملكة العربية السعودية، جامعة الطائف، مجلة جامعة الطائف للعلوم الإنسانية، المجلد ٦، العدد ٢١، ٢٠٢٠م، ٢٦٤.

(١٨) علاء الدين فرحان، من الردعه النووي إلى الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في القضاء السيبراني، الجزائر، جامعة بسكرة، مجلة الفكر، المجلد ١٦، العدد ١، ٢٠٢١م، ص ٢٢٤٦.

(ISSN: 2356 - 9492)

إلى ظاهرة عالمية، مما يؤثر على أعداد غير مسبوقة من الأفراد وتسبب الملايين من حالات الإيذاء في كل عام، ومن آثار هذه الجرائم السيبرانية تتراوح الخسارة المالية بالمليارات وخسارة الكثير من الوقت في سرقة الهوية والاحتيال، وتتسبب في الاضطراب العاطفي المرتبط بالقلق، والاكتئاب، أو حتى الأفكار الانتحارية مثل التحرش عبر الانترنت أو العنف الإلكتروني والتعريض لوسائل الإعلام المتطرفة. (١٩)

وتمتاز الجريمة السيبرانية بطائفة من الخصائص التى جعلتها متفردة في صورتها عن باقي الجرائم الأخرى، بالنظر إلى مجموعة المعطيات الخاصة بها بالدرجة الأولى، سواءاً من ناحية أداء ارتكابها أو مرتكبيها، أو حتى كيفية إثباتها ومعاينتها. (٢٠) وتتمثل تلك المعطيات فيما يلي:

١- إن طبيعة الجرائم السيبرانية وتمييزها عن الجرائم التقليدية يرجع إلى البيئة التى ترتكب فيها الجريمة وهي الأداة أو الوسيلة التى استخدمها الجاني في ارتكاب فعله غير المشروع، وتتطلب توفر معرفة أو حد أدنى من الثقافة التقنية لدى الجاني، وهي لا تخرج عن كونها سلوك إجرامي جرمه القانون، وتتجه إرادة الجاني إليه، رغم وجود نص قانوني يجرم السلوك. (٢١)

٢- الجريمة الإلكترونية ذات بعد دولي، عابرة للحدود، فهي تتجاوز الحدود الجغرافية بسبب تنفيذها عبر الشبكة المعلوماتية، وهوما يثير في كثير من الأحيان تحديات قانونية فنية، بل سياسية بشأن مواجهتها، لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية. (٢٢)

(١٩) راشد محمد المري، أثر تكنولوجيا المعلومات في النظام الأمني والرقابة الداخلية، مجلة الشريعة والقانون بدمنهور، العدد ٤٠، ٢٠٢٣م، ص ١٨.
(٢٠) الأمن السيبراني: هيئة الإعلام، قسم الدراسات والاتصال والعلاقات العامة، ٢٠٢١، ص ٢.
(٢١) مهدي رضا، الجرائم السيبرانية وآليات مكافتها في التشريع الجزائري، الجزائر، مجلة إليزا للبحوث والدراسات، المجلد ٦، العدد ٢، ٢٠٢١م، ص ١١٤.
(٢٢) إبراهيم رمضان إبراهيم عطايا، الجريمة الإلكترونية وسبل مواجهتها في التشريع الإسلامي والأنظمة الدولية، دراسة تحليلية تطبيقية، طنطا، مجلة كلية الشريعة والقانون، المجلد ٣٠، العدد ٢، ٢٠١٥م، ص٣٧٣.

٣- صعوبة الكشف عن مرتكب الجريمة السيبرانية إلا بأساليب أمنية وتقنية عالية. (٢٣)

## المبحث الثاني

## البنية التحتية للأمن السيبراني في دول العالم

يشمل الأمن السيبراني وجود إستراتيجية تشمل استعراضاً عاماً أولياً لمدى كفية الممارسات الوطنية الحالية والنظر في دور جميع أصحاب المصلحة في هذه العملية، ولأسباب تتعلق بالأمن القومي والرفاه الاقتصادي، تحتاج الحكومات إلى المساعدة في عملية حماية البنية التحتية لمعلوماتها الحيوية، وتعزيز هذه الحماية وضمانها(٢٤).

وتواصل الحكومات في كثير من الأحيان الاضطلاع بدور قيادي في أمن الشبكات، فإن مما له أهميته الخاصة ضماناً لإدماج أصحاب المصلحة الآخرين المعنيين، ومن شأن هذا الإدماج مضاعفة الثقة وتطوير وتطبيق السياسات(٢٥)، أما على الصعيد الدولي تقتضى حماية البنية التحتية للمعلومات وتعزيز الأمن السيبراني(٢٦) التعاون والتنسيق بين الدول على الساحة الدولية.

**البنية التحتية الوطنية الحساسة:**

يتكون الإنترنت من مجموعة من الشبكات المستقلة تتصل ببعضها البعض باستخدام معايير مفتوحة لضمان إمكانية التشغيل البيئي، وكذلك تمثل البيئة التحتية لشبكة المعلومات العناصر التى تشكل وتعين على نقل البيانات القابلة للاستخدام عبر تلك الشبكات، ونظراً لاعتماد معظم اقتصاد الدول ومجتمعاتها وخدماتها الأساسية حالياً

(٢٣) زينب طرفي العنزي، الجريمة الإلكترونية في ميزان الفقه والقانون، العراق، مجلة الدراسات الإسلامية والبحوث الأكاديمية، العدد ٩٩، ٢٠٢٢م، ص ١١٢.
(٢٤) خالد ممدوح إبراهيم: الجرائم المعلوماتية، الإسكندرية، دار الفكر الجامعي، الطبعة الأولى، ٢٠١٩، ص ٣٣.
(٢٥) نرمين محمد صالح: محددات فعالية المراجعة الداخلية للأمن السيبراني، المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة (تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين) للفترة من ١٠-٢٠٢٢/١١م.
(٢٦) على زايد محمد الجبيري الشهري: الإطار القانوني للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، رسالة دكتوراه، جامعة نايف للعلوم الأمنية، كلية العلوم الإستراتيجية، قسم الدراسات الإستراتيجية، تخصص دراسات إستراتيجية، ٢٠١٩م، ص٣٣.

(ISSN: 2356 - 9492)

على الإنترنت، فقد أصبح المحافظة على إمكانية الاتصال يمثل أولوية قصوى. [٢٧] وفيما يلي العناصر الأساسية للبنية التحتية لشبكة الإنترنت:

**١- البروتوكولات والخدمات:**

البرتوكولات هي معايير فنية تتيح لمختلف أنظمة الحواسب إمكانية التواصل مع بعضها البعض، وتمثل البرتوكولات والخدمات عناصر أساسية لضمان أمن البنية التحتية لشبكة الإنترنت، فبدونها لا يمكننا إرسال البيانات واستقبالها أو التنقل بين صفحات الإنترنت للوصول إلى المعلومات ومشاركتها أو التواصل مع مع الآخرين، وتمثل مجموعة TCP/IP التى تشكل أساس الإنترنت مثالاً رئيساً على تلك البروتوكلات. [٢٨]

**٢- البرمجيات والمعدات الحاسوبية:**

وتمثل أنظمة التشغيل والبرامج الثابتة، وتنطوى البرمجيات على ثغرات أمنية يجب معالجتها من خلال التحديث المنتظم وتصحيح الأخطاء وغيرها من الوسائل، ويقصد بالمعدات الحاسوبية الآلات والتوصيلات السلكية عبر أجهزة الشبكات مثل المفاتيح وأجهزة التوجيه وجدران الحماية والبوابات والخوادم والحواسب الشخصية والأجهزة اللوحية والهواتف النقالة. [٢٩]

وقد يؤدى فقدان تلك العناصر الأساسية للبنية التحتية (أي الأصول، والمرافق، والنظم، والشبكات، والعمليات، والعاملون الأساسيون الذين يقومون بتشغيلها ومعالجتها)، أو تعرضها لانتهاكات أمنية إلى:

---

(٢٧) لمزيد من الإطلاع: متاح على الموقع الإلكتروني :
https://infowatch.com/sites/default/files/report/analytics/a_study_of_data_leaks_in_the_middle_east_in_2017-2018_.pdf

(٢٨) تعمل مجموعة مهندسي شبكة الإنترنت IETF وهي منظمة للمعايير المفتوحة، على تنظيم وتطوير بروتوكول التحكم بالنقل TCP وبرتوكول الإنترنت IP .

(٢٩) المبادئ التوجيهية المتعلقة بأمن البنية التحتية للإنترنت في الدول العربية، مارس ٢٠٢٠م، ص ١١، ولمزيد من الإطلاع: https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc/

- أثر سلبي كبير على توافر الخدمات الأساسية أو تكاملها أو تسليمها، بما في ذلك الخدمات التى يمكن أن تؤدى في حال تعرضت سلامتها للخطر إلى خسائر كبيرة في الممتلكات والأرواح، مع مراعاة الآثار الاقتصادية والاجتماعية الكبيرة.
- تأثير كبير على الأمن القومي والدفاع الوطني واقتصادها ومقدراتها الوطنية. (٣٠)

**خطوات تحديد أهداف الأمن السيبراني(٣١):**

يعد إنشاء قدرة وطنية لإدارة الحوادث مهمة طويلة الأجل تبدأ بإنشاء مجموعة فرق وطنية للاستجابة لحوادث الأنظمة الإلكترونية منها تحديد أو إنشاء قدرات وطنية لفرقة Cyber Incident Response Team:(٣٢) ووضع آليات داخل الحكومة الوطنية للتنسيق بين القطاعين المدني والحكومي. (٣٣)

ولم تنشئ أغلب الدول العربية هيئة وطنية الأمن السيبراني باستثناء بعض الدول التي بعثت مثل هذه الهيئات بتسميات مختلفة، أما في بعض الدول العربية الأخرى، فنلاحظ إحداث مجالس وهيئات عدة لها دور هام في تحديد الرؤية الإستراتيجية الوطنية للأمن السيبراني وفي وضع البرامج العملية لتحقيقها، تتخذ في بعض الأحيان شكل مجالس، وفي أحيان أخرى شكل هيئات إدارية تابعة لرئاسة الجمهورية أو للوزارة المكلفة بالأمن أو بالدفاع الوطني أو بالعدل، مثلما هو الشأن في مصر متمثل في المجلس الأعلى للأمن السيبراني التابع لمجلس الوزراء، والجزائر متمثل في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، أما في الكويت فتباشر الهيئة العامة للاتصالات وتقنية المعلومات الاختصاص المتعلق بمهام ومسئوليات الأمن السيبراني وغيرها في مجال حماية البيانات الشخصية، نلاحظ بأن بعض الدول العربية

(٣٠) الضوابط الأساسية للأمن السيبراني، الهيئة الوطنية للأمن السيبراني، 2018 : 1-ECC
(٣١) على بهلوان: استخدام قاعدة البيانات ومنتج التطبيقات، القاهرة، دار الكتب العلمية للنشر والتوزيع، الطبعة الثانية، ٢٠١٨م، ص١٨.
(٣٢) خالد ممدوح إبراهيم: الجرائم المعلوماتية، الإسكندرية، دار الفكر الجامعي، الطبعة الأولى، ٢٠١٩، ص ٣٧.
(٣٣) عبدالفتاح بيومي حجازي: مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي: دراسة قانونية متعمقة في القانون المعلوماتي، الإسكندرية، دار الفكر الجامعي، ٢٠٢٠، ص٣٢.

(ISSN: 2356 - 9492)

أحدثت هيئات وطنية لمراقبة البيانات الشخصية من ذلك الدول التالية: تونس والإمارات العربية المتحدة والمغرب ومصر والأردن، ولكن من المفيد التأكيد على عدم خضوع هذه الهيئات إلى نفس النظام القانوني، وعدم تمتعها بنفس الصالحيات والإمتيازات مع الملاحظ أن هناك بعض الدول العربية التي أوكلت مهمة مراقبة البيانات الشخصية إلى مصالح وزارة مثلما هو الشأن بالنسبة لدولة قطر، حيث جعل المشرع من الوحدة القانونية لوزارة الإتصالات المصلحة المختصة في هذا المجال. (٣٤)

**مهام إدارة البحوث والمراقبة في الأمن السيبراني:**

يقع على عاتق الحكومة إنشاء أو تحديد منظمة وطنية تعمل كجهة اتصال وذلك لضمان الفضاء السيبراني والعمل على حماية البنية التحتية الحيوية للبيانات والمعلومات، تتضمن مهام هذه المنظمة المراقبة والإنذار والاستجابة وجهود التعايش وتيسير التعاون بين الكيانات الحكومية والقطاع الخاص؛ بالإضافة إلى الدوائر الأكاديمية والمجتمع الدولي. (٣٥)

وركزت العديد من الدراسات على المسئولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعي وتحديد جرائم الاعتداء على الحياة الخاصة، والسب والقذف، والمسام بالقيم الدينية، وبالاعتماد على تحليل قوانين مكافحة جرائم تقنية المعلومات أظهرت النتائج أن المشرع حرص في كل من عمان والكويت وقطر والإمارات العربية المتحدة على تجريم الآراء التى تؤدى إلى الفتنة بين أفراد المجتمع، أو التى تمس القيم الدينية أو النظام العام في الدولة، كما جرم الاعتداء على الحياة الخاصة والسب والقذف باستخدام وسائل التواصل الاجتماعي، ويتم ذلك من خلال قانون مكافحة جرائم تقنية المعلومات في كل بلد. (٣٦)

(٣٤) الرؤية العربية للأمن السيبراني: الواقع – التحديات – الفرص، تونس، المنظمة العربية لتكنولوجيا الاتصال والمعلومات، ٢٠٢١م، ص ٢٥.
(٣٥) تغريد صفاء، لبنى خميس مهدي: أثر السيبرانية في تطور القوة، مرجع سابق، ص١٥١.
(٣٦) حمدي محمد محمود حسين، المسئولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعي، برلين، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي، المجلد ٢، العدد ٨، ٢٠١٨م، ص ١٠٤٩.

**نشر خدمات الأمن السيبراني:**

وفقاً لما أوردته تقارير منظمة التعاون والتنمية في الميدان الاقتصادي، فإن القوى الدافعة الرئيسية لأي ثقافة للأمن على المستوى الوطني تتمثل في تطبيقات الحكومة الإلكترونية وخدماتها، وحماية البنية التحتية الحيوية للمعلومات، ونتيجة لذلك، ينبغي للإدارات الوطنية تنفيذ تطبيقات وخدمات الحكومة الإلكترونية من أجل تحسين عملياتها الداخلية وتوفير الخدمات الأفضل للقطاع الخاص والمواطنين، كعنصر مضاعف نحو تعزيز نشر ثقافة الأمن.(٣٧)

وكان قرار الجمعية العامة للأمم المتحدة رقم ٥٧/٢٣٩ بإرساء الثقافة العالمية للأمن السيبراني، والقرار ٥٨/١٩٩، بإرساء ثقافة عالمية لأمن الفضاء الحاسوبي وحماية البنى التحتية الحيوية للمعلومات والبيانات قراراً يروج لثقافة الأمن السيبراني على مستوى الأشخاص والدول، وذلك عن طريق توعية القطاع الخاص والمجتمع المدني والأفراد بتأمين تشغيل واستخدام البنية التحتية للمعلومات، بما في ذلك المعلومات والبيانات الحكومية، ويشتمل ذلك على تدريب مستخدمي الشبكات في الأنظمة الحكومية والخاصة، مع إدخال تحسينات مستقبلية على الجوانب الأمنية(٣٨).

فيجب اعتماد الدول من خلال أنشطتها التعاونية على نهج متعدد التخصصات ومتعدد أصحاب المصلحة لتنفيذ عملية الأمن التى يقوم بعضها بإنشاء هيكل إدارة رفيع المستوى لتنفيذ السياسات الوطنية، كما يكتسى التعاون الدولي أهمية بالغة في تعزيز تلك الثقافة، جنباً إلى جنب مع دور المنظمات الإقليمية في تيسير التفاعلات والتبادلات الدولية وتوعية المستخدمين ومسئوليتهم تجاه القضايا الرئيسية(٣٩).

(٣٧) وليد الزيدي: القرصنة على الإنترنت والحاسوب، عمان، دار أسامة للنشر، الطبعة الثالثة، ٢٠١٩م، ص ١٥.
(٣٨) عبدالفتاح بيومي حجازي: مرجع سبق ذكره، ص٣٥.
(٣٩) على حسن طوال: مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، دراسة مقارنة، الأردن، مركز الإعلام الأمني، ٢٠١٩م، ص ١٥.

(ISSN: 2356 - 9492)

المبحث الثالث

مسئولية مقدمي خدمات الأمن السيبراني

يشهد العالم جملة من التغيرات والتطورات والتحولات في كافة مناحي الحياة وتؤثر بدورها علي عمل مؤسسات القطاعين العام والخاص على حد سواء شأنها في ذلك شأن مختلف قطاعات المجتمع، ولعل أبرز هذه التغيرات تتمثل في تطور تكنولوجيا الاتصالات وتقنية المعلومات والشبكة العالمية الانترنت التي ساهمت في إحداث تغير ملحوظ في عمليات القطاعين العام والخاص على حد سواء، ووفقاً لأهمية جودة الخدمات الإلكترونية ودورها الهام في تسهيل وتسريع العمليات والخدمات، فلم يعد هناك حاجه للوقوف والانتظار طويلاً للحصول علي خدمة أو معاملة، وهذا أدي إلى توفير الوقت والجهد والتقليل قدر الإمكان من الموارد المستهلكة في موسسات في حالة الخدمات التقليدية. (٤٠)

يضاف إلى ذلك ما تقدمه الإنترنت من إمكانات وقدرات للمجالات العلمية والثقافية والخدماتية، حيث تسمح بالوصول إلى مناطق بعيدة، وإلى فئات محددة، ككبار السن والمرضى وغيرهم من ذوى الاحتياجات الخاصة، هذا عدا عن الدور الذى يمكن أن تؤديه في تبادل المعلومات، في أوقات الأزمات الإنسانية والكوارث، بحيث تتأمن المساعدات وتوزع بالسرعة المطلوبة، ولا تقف الأبعاد الاجتماعية عند حدود توفير اطمئنان المواطن إلى حياته اليومية، والإفادة من طاقات تقنيات المعلومات والاتصالات، في تطوير نشاطاته المختلفة، بل تتعداها إلى صيانة القيم الجوهرية في المجتمع، كالانتماء والمعتقدات، بالإضافة إلى العادات والتقاليد عبر إنشاء المجموعات التى تهتم بنشر الوعي حول هذه المسائل. (٤١)

إن الحقيقة الواضحة أمامنا تقودنا إلى القول بأن هذا الجدل لا يمكن ان يؤدى بأي شكل من الأشكال إلى استبعاد مسئولية مقدمي الخدمات، بحيث يصبح الممنوع

(٤٠) مزيان عبدالقادر، أثر محددات جودة العملاء على رضا العملاء، مذكرة الماجستير، الجزائر، جامعة تلمسان، ٢٠١٢م، ص٩.
(٤١) على النقروز، جرائم نظم المعلومات، الأردن، دار السناء للنشر، ٢٠١٧م، ص ١١٤.

مشروعاً، والواقع أن المسئولية يمكن أن تجد أسساً مختلفة مثل الإخلال بالالتزام العقدي أو انتهاك حقوق الملكية الفكرية، أو عن طريق أفشاء أسرار مهنية، أو المساس بحرمة الحياة الخاصة، أو عبارات السب والقذف، فإزاء هذه المخالفات المتعددة يثور التساؤل حول الطريقة الأنسب لمعالجتها(٤٢).

فهل من الأمثل الأخذ بعين الاعتبار خصوصية بعض المخالفات، كتلك المتعلقة بحقوق الملكية الفكرية مثلاً، وبالتالي تخصيص النصوص القانونية لمعالجة كل مخالفة وحدها؟ أم من الأفضل وضع قواعد عامة للمسئولية المرتكبة على الأمن السيبراني بصرف النظر عن مضمونها.

ويمكن للمسئولية في مقدمي الخدمات الأمنية السيبرانية أن تجد أسساً مختلفة مثل الإخلال بالالتزام العقدي أو انتهاك حقوق الملكية الفكرية، فإزاء هذه المخالفات المتعددة يثور التساؤل حول الطريقة الأنسب لمعالجتها(٤٣). وساعد التقدم الكبير في مستوى التقنية المعلوماتية في توظيف هذه التقنية من أجل تسهيل الولوج إليها، ولهذه الاعتبارات فإن الفقه والقضاء المقارن يرى أن من شأن زيادة استخدام التقنيات الرقيمة يظهر الاحتياج إلى قانون جديد للإجراءات الجنائية يختلف في قواعده عن القوانين المطبقة حالياً(٤٤).

وتمثل الخدمات الخصائص الوظيفية التى تجعل من الإنترنت أداة جذابة ومفيدة من خلال تيسير عملية تبادل المحتوى عبر الإنترنت، وتتضمن خدمات البنية التحتية لشبكة الإنترنت "العنونة" وهو النظام العالمي لتحليل أسماء النطاقات التى يستخدم نظام أسماء النطاقات DNS، والذى يتيح لنا التنقل بين صفحات الإنترنت، وتشمل وظائف مثل

(٤٢) أشرف توفيق شمس الدين: شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة، الطبعة الخامسة، ٢٠١٩م، ص٨٥.
(٤٣) أشرف توفيق شمس الدين: شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة، ط ٥، ٢٠١٩م، ص٨٥.
(٤٤) أشرف توفيق شمس الدين: مخاطر العملات الافتراضية في نظر السياسة الجنائية، مطبعة اكتوبر ، ٢٠١٩م، ص٥٢.

(ISSN: 2356 - 9492)

التوجيه واستخدام برتوكول البوابة الحدودية BGP، وخدمات التطبيقات مثل الشبكة العنكبوتية العالمية. (٤٥)

**ماهية مزودي خدمات الاتصالات الإلكترونية:**

مزود الخدمة أو متعهد الوصول هو الموزع لخدمة الإنترنت، والذى يتيح من خلال حاسباته المتصلة بالشبكة للمستخدمين الوصول إلى خدمة الإنترنت، وتوصيل المستخدم بالمواقع التى يرغب في الوصول إليها(٤٦) ويمكن لمزودي خدمات الإنترنت توفير خدمات أخرى كتخزين البيانات عن بعد لعملائهم(٤٧). ويمكن تداخله إذا لاحظ مخالفات تشكل جرائم يعاقب عليها القانون(٤٨).

يتضح من ذلك أن مقدمي خدمات الإنترنت لا يقدموا المعلومات، إنما يحققوا اتصال الغير بالشبكة فقط ليس إلا، وليس له سيطرة على المادة محل البحث، لكن يمكن تدخله لقطع هذا الاتصال إذا لاحظ مخالفات تتعلق بتلك المادة محل البحث أو المنشورة(٤٩).

ومن الناحية الفنية فيربط مقدمي خدمات الإنترنت بزبائه باستخدام تقنية نقل البيانات لنظام الإنترنت مثل الاتصال الهاتفي، وخط المشترك الرقمي للاتصال، وكابل المودم ولاسلكية الوصلات المخصصة عالية السرعة، وهو يوفر حسابات البريد الإلكتروني للمستخدمين والتى تسمح لهم بالتواصل مع بعضهم البعض، عن طرق إرسال واستقبال الرسائل الإلكترونية من خلال مزود الشبكة، وكجزء من خدمة البريد

(٤٥) أكرم محمد رضا الطويل، هضبمة عبد الواحد سلطان الجنابي، التوزيع المادي وعناصر خدمة العميل، الطبعة الأولى، دار الحامد للنشر، عمان – الأردن، ٢٠١٥، ص٧١، ولمزيد من الإطلاع: متاح على الموقع الإلكتروني : - https://www.cybersecurity-review.com/news-may-2018/phishing-spy-campaign-targets-top-mideast-officials/

(٤٦) جمعي فريحة: المسئولية المدنية والجنائية لمقدمي خدمة الإنترنت، مذكرة التخرج لنيل شهادة ماجستير، التخصص قانوني اجتماعي، الجزائر، كلية الحقوق والعلوم السياسية، جامعة د.مولاي الطاهر، ٢٠١٧-٢٠١٨م، ص٨.

(٤٧) خالد ممدوح إبراهيم: حجية البريد الإلكتروني في الإثبات، دراسة مقارنة، الإسكندرية، دار الفكر الجامعي، الطبعة الأولى، ٢٠١٨م، ص٥ وما بعدها.

(٤٨) عبدالفتاح بيومي حجازي: النظام القانوني للحكومة الإلكترونية، الكتاب الأول،الإسكنرية، دار الفكر الجامعي، ٢٠١٩، ص٣٢.

(٤٩) زينة حازم خلف الجبوري: القانون الواجب التطبيق على مسئولية مزودي خدمات الإنترنت، مجلة جامعة تكريت للحقوق، السنة الأولى، المجلد الأول، العدد ٤، الجزء ٢، ٢٠١٧م، ص٣٨٥.

الإلكتروني ما يوفر مزود الخدمة وعميل البريد الإلكتروني حزمة البرامج التى طورت داخلياً أو خارجياً عن طريق ترتيب عقد خارجي، كما يمكن لمزودي خدمات الإنترنت توفير خدمات أخرى كتخزين البيانات عن بعد لعملائهم(٥٠).

مما سبق يتضح أن متعهد توصيل الخدمة هو الشخص الطبيعي أو الاعتباري الذى يملك خدمة الاتصال مباشرة بالشبكة الدولية للمعلومات، وتقتصر المهمة لديه على تمكين الأفراد الذين يبرمون عقداً معه من الاتصال بالشبكة للإطلاع على مختلف المواقع من أجل الوصول إلى خبر أو معلومة معينة، فهو لا يقدم المعلومات ولكنه يحقق اتصال الغير بالشبكة، وليس له سيطرة على المادة محل البحث ولكن يمكن تداخله إذا لاحظ مخالفات تتعلق بمحتوى المادة التى يتم بثها، أو إذا كانت تشكل جرائم يعاقب عليها القانون(٥١).

**التزامات مقدمي خدمات الإنترنت:**

١- يجب على مزودي الخدمة في حالة نشر أي بيانات أو معلومات من شأنها تهديد الامن القومي أو الاقتصادي للدولة أو نشر المواد الإباحية او التحريض على الاتجار في البشر، وجميع الأنشطة غير القانونية، إبلاغ السلطات بعناوين هؤلاء الأشخاص والبريد الإلكتروني والصفحة الشخصية، الأمر الذي يتعين معه إلزام مزودي الخدمات مدير تحرير الموقع بالحصول على المعلومات الشخصية للمستخدمين مسبقاً عند إنشاء صفحات التواصل(٥٢).

٢- يلتزم مقدمي الخدمة باحترام الحق في الخصوصية وسرية المراسلات(٥٣).

---

(٥٠) خالد ممدوح إبراهيم: حجية البريد الإلكتروني في الإثبات، دراسة مقارنة، دار الفكر الجامعي، الطبعة الأولى، ٢٠١٨م، ص٥ وما بعدها.

(٥١) عبدالفتاح بيومي حجازي: النظام القانوني للحكومة الإلكترونية، الكتاب الأول، دار الفكر الجامعي، الإسكندرية، ٢٠١٩، ص٣٢.

(٥٢) BOUDER Hadjira: Quel cadre juridique pour la lutte contre la criminalité liée aux TIC en Algérie, séminaire national sur le cadre juridique des TIC en Algérie; entre opportunité et contraintes, CERIST, Alger, du 16 au 17 mai 2012, p. 4.

(٥٣) Jérôme Bossan: Le droit pénal confronté à la diversité des intermédiaires de l'internet, RSC, N° 02 du 16/08/2013, p. 295.Rights and Liabilities Involving Online Speech, available at:http:// www.knox.edu/offices-and-

(ISSN: 2356 - 9492)

٣- يجب على مقدمي الخدمة مراقبة المعلومات التى تشكل جريمة تهدد سلامة أمن الدولة، وإبلاغ السلطات المختصة عنها.

٤- إذا ورد بلاغ لمقدمي الخدمة كالتشهير أو بيانات غير قانونية يتعين عليهم الامتناع عن تخزينها.

٥- عدم جواز نسخ أي بيانات أو نقلها إلى الجمهور دون موافقة أصحاب حقوق الطبع والنشر.

٦- عدم جواز إلغاء أو حذف أو تعديل أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات.

٧- يلتزم مقدمي الخدمة بتقديم بيانات عملائهم إلى سلطات التحقيق إذا طلب منه ذلك، وعدم فتح أي اشتراك لأي عميل دون الحصول على بيانات تحقيق شخصيته، ويترتب على الإخلال بهذا الالتزام انعقاد المسئولية الجنائية لمقدمي خدمات الإنترنت(٥٤).

**التزامات مزودى خدمات الاتصالات في التشريع الكويتي:**

كما عرف مقدمي خدمة الإنترنت بأنه: " يشمل مقاهي الإنترنت ومراكز التسلية ومحلات ومراكز خدمات الكمبيوتر وأية هيئات أو جهات أو مراكز عامة أو خاصة تقدم خدمات الإنترنت بجميع أنواعها سواء كانت بمقابل أو بدون، ويبدو أن المشرع الكويتي ميز بين مزودي الخدمة ومقدمي خدمة الإنترنت. (٥٥) يتضح ذلك فيما يلي:

حدد قانون تنظيم الاتصالات ضوابط بشأن تسوية أي نزاع ينشأ بين مقدمي خدمات الاتصالات، فنصت المادة ٢٩، على أنه إذا نشأ نزاع بين مقدمي الخدمات فى شأن اتفاقيات الترابط المبرمة بينهم، عرض هذا النزاع على الجهاز لإصدار قرار فيه وفق أحكام هذه الاتفاقيات، وبما لا ينطوى على تمييز بين مقدمى الخدمة أو فيما يتحملونه

---

services/information-technology services/computer-use-policies/online-speech.html.

(٥٤) أشرف توفيق شمس الدين: شرح قانون العقوبات، مرجع سبق ذكره، ص٩١.

(٥٥) الجريدة الرسمية، ملحق العدد ٤١، بتاريخ ٢٠٠٢/٧/٢٣م.

من تكاليف الترابط، وبحيث لا يكون تجاوز التكاليف الفعلية للترابط وخدماته وتجهيزاته إلا بما يحقق عائدًا استثماريًا معقولاً. (٥٦)

وتنص المادة ٣٠، على أن يحظر على مقدمى أكثر من خدمة اتصالات مرخص بها دعم إحدى هذه الخدمات على حساب خدمة أخرى، ويسرى هذا الخطر حتى ولو كانت الخدمة المدعومة لا تحتاج إلى ترخيص أو كان الدعم موجهًا إلى منتج معين يتصل بالخدمة المقدمة، ولمجلس إدارة الجهاز، ومع مراعاة القواعد المنصوص عليها فى المادة (٢) من هذا القانون، أن يستثنى من هذا الحظر خدمة من خدمات الاتصالات وذلك بقرار مسبب ولمدة محددة. (٥٧)

## الفصل الثاني
## حماية الأنظمة الإلكترونية

**تمهيد وتقسيم:**

ساهم التطور التكنولوجي في مجال الاتصالات وتقنيات المعلومات في سرعة انتشار المعلومات وسهولة تداولها عبر خدمات الإنترنت، مما أدى إلى ظهور العديد من المخاطر(٥٨) والاعتداءات التى تتم في الأنظمة الإلكترونية، الأمر الذى أدى إلى ضرورة نشر الوعي بين المستخدمين لحماية أمن المعلومات، وذلك من خلال قيام الدول والمنظمات إلى وضع التشريعات التى تحمى أمن المعلومات، فضلاً عن العديد من المنظمات التى تقوم بوضع مواصفات دولية لتكون بمثابة الدليل الاسترشادي الأمثل لحماية أمن المعلومات مثل منظمة الأيزو. (٥٩)

(٥٦) متاح على الموقع الإلكتروني : https://alnaswallhayah.com /
(٥٧) أشرف توفيق شمس الدين: مرجع سابق، ص ٨٨.
(58) Ramirez, M, Ariza, L., and Miranda, M., The disclosure of information on rsecurity in listed companies in Latin America- proposal for a cyber security disclosure index), journal of sustainability ,2022,14(3).
(٥٩) عزة فاروق جوهري، طه محمد حسن، أمن المعلومات الرقمية وسبل حمايته في ظل التشريعات الراهنة، مجلة المركز العربي للبحوث والدراسات في علوم المكتبات والمعلومات، مج ٦، العدد ١٢، ٢٠١٩م، ص ٨٥. متاح على الرابط:
http://search.mandumah.com/Record/994947

(ISSN: 2356 - 9492)

ويرتبط الأمن السيبراني ارتباطاً وثيقاً بالتحول والتبادل الرقمي للبيانات، لكن الملف للنظر والمؤسف سهولة اختراق تلك المعلومات والبيانات، والاعتداء عليها والعبث بها، وتقف الدول عاجزة عن منعها أو الوقاية منها، كون التقنية المستخدمة في هذه الجرائم متطورة جداً، مما يتطلب ضرورة العمل والحرص على حماية أمن تلك المعلومات والبيانات المتوفرة على مختلف الأنظمة، لأن فقدان المعلومات والبيانات المنتقلة عبر الشبكات الإلكترونية من الأمور المكلفة الصعب تعويضها، كما أن حماية تلك المعلومات والبيانات فيه حافظة على الأنفس والأعراض والأموال المرتبطة بهذه البيانات والمعلومات(٦٠).

وتعتبر الجرائم الإلكترونية ظاهرة إجرامية جديدة مستحدثة تدق أجراسها لتنبئ المجتمع المعاصر بمدى وحجم المخاطر وهول الخسائر الناجمة عن تلك الجرائم التى تمثل اعتداء صارخ على التقنيات الحديثة بكافة معطياتها من بيانات ومعلومات وبرامج على اختلاف أنواعها.

لذا يتناول الفصل الثاني حماية الأنظمة الإلكترونية من الاختراق والتلف للأشخاص والدول، فيشتمل هذا الفصل على ثلاث مباحث: الأول يتناول الجريمة السيبرانية كتهديد للأمن السيبراني، ثم تأثير الإعلام في الوعي بالأمن السيبراني في مبحث ثانٍ، ثم في مبحث ثالث وسائل حماية الأنظمة الإلكترونية؛ يعقبهما خاتمة، ثم أهم النتائج والتوصيات ثم قائمة بأهم المراجع العربية والأجنبية المستند إليها البحث الحالي وذلك على الترتيب التالي:

(٦٠) عادل موسى عوض جاب الله: وسائل حماية الأمن السيبراني – دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة، جامعة الأزهر، كلية الشريعة والقانون، المجلة العلمية، العدد ٣٤، الإصدار الأول، الجزء الثالث، ٢٠٢٢، ص٢٩.

المبحث الأول: الجريمة السيبرانية كتهديد للأمن السيبراني

المبحث الثاني: تأثير الإعلام في الوعي بالأمن السيبرانى

المبحث الثالث: وسائل حماية الأنظمة الإلكترونية في التشريع الكويتي والتشريعات المقارنة

وذلك على التفصيل التالي:

## المبحث الأول

## الجريمة السيبرانية كتهديد للأمن السيبراني

أدى التقدم العلمي والتقني في مجال الاتصالات(٦١) وظهور شبكة الإنترنت(٦٢) وتضخمها وامتدادها إلى كل أقاليم الدول تقريباً إلى تنوع وتعدد الأنشطة الإجرامية التى ترتكب من خلالها وعبر عدة دول، كما أفرزت المواقع الإلكترونية ثورة إعلامية، أثبتت أهميتها في ساحات التغيير، حتى إنها نافست الإعلام التقليدي، دوراً وحضوراً، كما أثارت إشكالات عديدة على الصعيد القانوني، أهمها التساؤل عن مسئولية المواقع الإلكترونية الإعلامية جنائياً، عن محتواها الضار أو غير المشروع، ومع كثرة الأشخاص القائمين على عمل هذه المواقع يثار التساؤل عن تحديد المسئول جنائياً، وكذلك الحالات التى تقوم فيها المسئولية الجنائية للمواقع الإلكترونية.

كما أدى ظهور الجرائم السيبرانية كنمط جديد من أنماط الجريمة إلى توجه المجتمع الدولي للتعاون من أجل تصدٍ دامغ لتلك الجرائم التي لها بالغ الأثر السلبي، حيث تعتمد أغلب المجتمعات على تقنيات الاتصالات والمعلومات، ومع ذلك الاعتماد المستمر

(٦١) محمد سامي الشوا: الإثبات الجنائي في ظل نظام العولمة والتقنيات الحديثة، دراسة تطبيقية على الاتحاد الأوروبي، التشريع الفرنسي، دار النهضة العربية، ٢٠١٨، ص٥.

(٦٢) نشأت هذه الشبكة في الولايات المتحدة الأمريكية وهي عبارة عن مشروع أنفقت عليه وكالة مشاريع البحوث المتقدمة في وزارة الدفاع الأمريكية خلال ستينات القرن الماضي، وكان هدف الوزارة بناء شبكة متماسكة يمكن أن تصمد في ظل ظروف صعبة كحدوث كارثة نووية وذلك لنقل المعلومات الأمنية والعسكرية في ظل الكارثة، وذلك عبر إعداد سلسلة من الوصلات الحاسوبية تعرف باسم Arpanet لتضمن بذلك بقاء الاتصال فيما بين الأجهزة الأمنية والعسكرية المختلفة، وبعد ذلك في عام ١٩٦٨م أدخلت الوزارة أربع جامعات أمريكية عبر الشبكة لتبادل الأبحاث إلى أن غطت معظم الجامعات الأمريكية عام ١٩٧٢م إلى أن تخلت وزارة الدفاع الأمريكية عن الشبكة نهائياً في ثمانينات القرن الماضي. للمزيد انظر: بيل بول: انطلق مع الإنترنت، ترجمة مركز التعريب والترجمة، الدار الجامعية للعلوم، بيروت، ١٩٩٦م، ص١٢.

(ISSN: 2356 - 9492)

تصاحبه مخاطر ناشئة ومحتملة تهدد تلك الشبكات، وتؤثر بالسلب على البنية التحتية للمعلومات الوطنية الحساسة، وخاصة المعلومات الشخصية والأمن الفكري(٦٣).

وتصف الجريمة المتعلقة بالمعلومات الحاسوبية بأنها فعل إجرامي هدفه المعلومات الحاسوبية، بينما تصف اتفاقية منظمة شنغهاي للتعاون(٦٤) (على نطاق أوسع) "جرائم المعلومات" بأنها استخدام موارد المعلومات والتأثير عليها في الفضاء المعلوماتي لأهداف غير مشروعة(٦٥)، أما اتفاقية مجلس أوروبا(٦٦) على الرغم من تعريفها للمصطلحات فإنها تستخدم عناوين تجريم واسعة، تشتمل على " جرائم ضد سرية وسلامة وتوافر البيانات والمعلومات والأنظمة الإلكترونية.

أما مشروع قانون الاتحاد الأوروبي(٦٧) فيستخدم على نحو مشابه عناوين تجريم تميز بين "جرائم خاصة بتكنولوجيات المعلومات والاتصال وجرائم ذات تكييف قانوني محلها تكنولوجيات المعلومات والاتصال.

وفي الواقع تتبنى بعض الصكوك الدولية والإقليمية المعنية بالجريمة السيبرانية مفهوماً ضيقاً للأنظمة أو البيانات الحاسوبية لتكون محل الجريمة، في حين أن الصكوك الأخرى تتناول نطاقاً عريضاً من الجرائم، تتضمن أفعالاً حيث يكون محل الجريمة شخصاً أو شيئاً ما ذو قيمة، أو بالأحرى نظام حاسوبي أو بيانات حاسوبية، ولكن أينما يعتبر نظام حاسوبي أو نظام معلومات فإنه جزء لا يتجزأ من أسلوب ارتكاب الجريمة(٦٨).

(٦٣) شيخة حسين الزهراني: التعاون الدولي في مواجهة الهجوم السيبراني، مرجع سابق، ص ٧٥١.
(٦٤) اتفاقية كومنولث الدول المستقلة، فقرة (أ)، المادة الأولى.
(65) Riza Azmi, and Kautsarina, Revisting cyber definition, European Conference on Cyber Warfare and Security, July 2019.
(٦٦) اتفاقية مجلس أوروبا بشأن جرائم الحاسوب، العناوين ١، ٢، ٣.
(٦٧) مشروع اتفاقية الاتحاد الأوروبي، الجزء الثاني، الفصل الأول والثاني، والجزء الثالث، الفصل الخامس.
(٦٨) Adamkolo Mohamed, Umaro Pate, Book Review: Understanding new media 2nd edition by Eugenia Siapera, Journal Komunikasi Indonesia, vol. VIII, no.3, November 2019.

**الأفعال التى تشكل الجريمة السيبرانية:**

تركز الفئة الثانية على الأفعال التى يعتبر فيها النظام الحاسوبي بمثابة الأسلوب الأساسي المستخدم في ارتكاب الجريمة، ويصاحب ذلك اختلاف في محل هذه الأفعال الإجرامية، ففي حالة الاحتيال باستخدام الكمبيوتر تعتبر المقتنيات الاقتصادية محل الجريمة، أما في حالة جرائم حقوق المؤلف والعلامات التجارية المرتكبة بواسطة الحواسيب، فإن محل الجريمة يتمثل في حقوق الملكية الفكرية المحمية.

ومن هذه التهديدات والتسلط ما قامت به العديد من شركات البرمجيات رفيعة المستوى عام ٢٠١٠ من الإبلاغ عن سلسلة من الهجمات عبر الإنترنت، وفي النهاية قد سجلت اختراقات في محرك بحث لشركة كبيرة، وباستخدام نقطة ضعف في أحد متصفحات شبكة الإنترنت، قام المهاجمون بعمل نفق داخل شبكة داخلية عبر حواسيب عمل الموظفين(٦٩) المعرضة للخطر، وتمكنوا من الدخول إلى حسابات البريد الإلكتروني واختراق مركز تخزين شفرة المصدر المؤمنة على نحو غير ملائم(٧٠).

وفي نفس العام تلقى مستخدموا موقع التواصل الاجتماعي رسائل بريد إلكترونية من حساب وهمي مع روابط لنظام تسجيل دخول زائف ليبدو أنه مرسل من الشركة، وبالفعل قام المستخدمون الضحايا بالدخول والتسجيل، وأصبحت وثائق المستخدمين عرضة للخطر، ومن المحتمل أن يصبح المضيف المخترق أحد الأعضاء في شبكة البوت نت ZeuS. (٧١)

وفي أوائل عام ٢٠١٣ اتهمت النيابة العامة في أمريكا الشمالية ثلاثة رجال أوروبيين بإنتاج وتوزيع فيروس حاسوبي ألحق الضرر بأكثر من مليون جهاز حاسوب على مستوى العالم، وتمكنوا من الوصول إلى معلومات بشأن حسابات بنكية شخصية

(٦٩) أمينة ختو: بيئة المؤسسة وأثرها على الأداء الوظيفي، مذكرة مكملة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة عبدالحميد بن باديس، مستغانم، ٢٠١٨-٢٠١٩، ص٤٧.

(70) Riza Azmi, and Kautsarina, Revisting cyber definition, European Conference on Cyber Warfare and Security, July 2019.

(71) Trustwave. 2011. SpiderLabs Global Security Report, Michelle Moore (1/1/2021), "Top Cybersecurity Threats in 2021", University of San Diego, Retrieved 28/11/2021. Edited.

(ISSN: 2356 - 9492)

استولوا من خلالها على مبلغ ٥٠ مليون دولار أمريكي على الأقل في الفترة ما بين ٢٠٠٥ إلى ٢٠١١، وقد تم إنتاج هذا الفيروس في أوروبا ثم انتشر في أمريكا الشمالية، حيث ألحق الضرر بأجهزة الكمبيوتر التى تخص هيئات وطنية، وقد وصفت هذه القضية بأنها " واحدة من أكثر عمليات الدمار المالي التى لم تشهد مثلها حتى الآن "(٧٢).

أما الفئة الأخيرة من أفعال الجريمة السيبرانية فتتمثل في تلك المتعلقة بالمحتوى الحاسوبي، وتتمثل في الكلمات والصور المرسلة أو المخزنة والأصوات، حيث يعتبر الهدف المادي للعمل الإجرامي في الجرائم المتعلقة بالمحتوى في أغلب الأحيان هو شخص ما، أو جماعة محددة من الأشخاص أو شئ ما ذا قيمة كبيرة، أو عقيدة ما، وبنفس النهج كما في الفئة الثانية، يمكن من حيث المبدأ أن ترتكب هذه الأفعال بدون الاتصال بالإنترنت، فضلاً عن استخدام نظم حاسوبية في ذلك، واتخاذ جميع التدابير اللازمة لحماية المستخدمين سواء كانوا أفراداً أو دولاً على حد سواء(٧٣).

**صور جرائم الفضاء الإلكترونى:**

تعود نشأة الحروب السيبرانية إلى مرحلة الحرب الباردة، فإن أول حرب سيبرانية وقعت بين الولايات المتحدة الأمريكية والاتحاد السوفيتي في عام ١٩٨٢، إذ قام جهاز المخابرات السوفيتي بعملية تسمي Line X ، وقد صممت هذه العملية لتساعد الاتحاد السوفيتي على سرقة تكنولوجيا المعلومات لكل أنشطة الغرب، إذ قامت بتدريب جيش من العلماء على التسلل إلى الشركات والوكالات والمؤسسات بمختلف أنواعها وأنشطتها بهدف الاختراق وسرقة المعلومات الأمريكية، وتعمد تسريب المعلومات إلى وكالة

(٧٢) أيمن البوغانمن: بنية سوق المعلومات في عصر الإنترنت: بين الديكارتية المجحفة والداروينية المقلوبة، مجلة ألباب، العدد.١٤، ٢٠١٩، ص ٥٣.

– انظر أيضاً: صالحه، نار الانفكاك والإعلام الرقمي: الهيمنة المعلوماتية والاحتلال الرقمي، مركز أبحاث منظمة التحرير الفلسطينية، عدد ٢٧٩، مجلد ٢٧٨، ٢٠٢٠، ص٥١.

(٧٣) أحمد جلال محمود: أثر التهديدات غير التقليدية للأمن على العلاقات الدولية المعاصرة – الأمن السيبراني في الشرق الأوسط - دراسة حالة من ٢٠٢٠ - ٢٠٣٠، بحث منشور في المؤتمر الدولي مستقبل منطقة الشرق الأوسط – رؤية مصر، جامعة عين شمس، مركز الشرق الأوسط للدراسات المستقبلية، القاهرة، ٢٠٢٠م، ص٥٦.

المخابرات الأمريكية CIA ، وبدلاً من إلقاء القبض عليهم جندتهم لصالحها وبدأت بإعطاء معلومات مغلوطة. وكانت نتيجة تلك لمعلومات المغلوطة لبناء العمود الفقري لخطوط نقل الغاز الطبيعي والنفط القادم من سيبريا، وبعد فترة قصيرة تسبب الخطأ المتعمدة في الشفرة المسربة في حدوث انفجار لخط الأنابيب وكان هذا الانفجار يعادل ثلث حجم انفجار القنبلة النووية التى ألقتها أمريكا على هيروشيما(٧٤).

وفيما يلي بعض من صور جرائم الأنظمة الإلكترونية أو الفضاء الإلكتروني، نذكر منها على سبيل المثال لا الحصر:

**١- جرائم الإتجار بالبشر:**

يعد الإتجار بالبشر أحد أشكال الجريمة المنظمة عابرة الحدود، التى اتسع نطاقها بكل ملحوظ خلال الآونة الآخيرة، باعتبارها جريمة عابرة للحدود، حيث لا توجد أي منطقة جغرافية في العالم بمنأى عن هذه الجريمة كشكل جديد من أشكال العبودية التى جرمها الجديد من الاتفاقيات والمعاهدات الدولية. (٧٥)

**٢- الجماعات الإرهابية واستخدامها الفضاء الإلكتروني (العراق نموذجًا):**

على الرغم من أن التطور التكنولوجى الذى مر به العراق، بالانفتاح على مجال تكنولوجيا المعلومات، والاتصالات، بعد الغزو الأمريكى فى ٢٠٠٣، فإنه حول "بغداد" إلى ساحة مفتوحة يسهل اختراقها، فور سقوط نظام "صدام حسين"، فمارست أشكالاً جديدة، ومبتكرة من الإرهاب، باستخدامها وسائل الاتصال الحديثة، والمتطورة. (٧٦)، قد طالت المؤسسات الإعلامية، مثل قنوات "UTV" وقناة "الفلوجة"، إضافة إلى الهجوم

(٧٤) الحروب السيبرانية: نتائج ملموسة لمعارك غير مرئية، الجندي، بتاريخ ٢٠٢١/٤/١م، الشبكة الدولية للمعلومات https//www.alijudi.com.

(٧٥) الأمم المتحدة، دليل المناقشة لمؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية، كيوتو، اليابان، ٢٠٢٠، ص ٥٤.

(٧٦) ابتهاج إسماعيل يعقوب وآخرون: مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية على وفق المتطلبات الدولية: دراسة اختبارية، العراق، مجلة الدراسات المالية والمحاسبية والإدارية، المجلد ٩، العدد ١، ٢٠٢٢، ص ١٤٠٥.

(ISSN: 2356 - 9492)

السيبرانى على موقع مطار بغداد، وفى غالبها هجمات حجب للخدمة تستهدف البنية التحتية للشبكات من نوع ."DDos".[٧٧]

**٣- الجماعات الإرهابية واستخدامها الفضاء الإلكترونى (إيران نموذجًا):**

كانت أول دولة تتبنى هذا المفهوم "الولايات المتحدة الأمريكية"؛ بهدف نشر أفكارها، وسياساتها، والترويج لها حول العالم، فأنشأت "واشنطن" فريق التواصل الرقمى، وفضاء الرأى الذى يتيح إمكان التعبير عن الآراء حول الموضوعات المتعلقة بالسياسة، والاقتصاد، وموقع المجتمع المدنى، الذى وظفت به منظمات المجتمع المدنىفى تحقيق النتائج المرجوة من هذه الدبلوماسية.[٧٨]

المبحث الثاني

تأثير الإعلام في الوعي بالأمن السيبرانى

أخذت ثورة المعلومات والمعرفة طابعاً متسارعاً مع بداية العقد التاسع عشر، ونتيجة لهذه الثورة المعرفية تطورت القطاعات الزراعية والصناعية والخدماتية والأمنية وغيرها من القطاعات، فالمعلومات والمعرفة أصبحت حالياً أساساً للكثير من السلع والخدمات الجديدة، فإنتاج السلعة الرقمية أو المعلوماتية تحتاج إلى خبرة كبيرة، وكما هي الحياة متغيرة ومتقلبة، فالمعلومات تتصف بذات الصفة، فهي تتميز بالتبدل والتغير المستمرين، وهي على ما يبدو تعد بمثابة شريان الحياة للمؤسسات ككل، هذا وقد أصبحت البيئة التى تعيشها المنظمات في ظل العولمة أكثر انفتاحاً ومنافسة كونها معتمدة على قواعد ثابتة أساسها تكنولوجيا المعلومات. [٧٩]

ففى ظل التطورات التكنولوجية المتتالية، والتنوع فى أدوات القوة، وتطور طبيعة الحروب بمختلف أجيالها؛ تتعاظم أهمية تحقيق "الردع السيبرانى"، الذى بات مقياسًا

(٧٧) باسم على خرسان: الأمن السيبراني في العراق: قراءة في مؤشر الأمن السيبراني العالمي ٢٠٢٠، مركز البيان للدراسات والتخطيط، ٢٠٢١م، ص ٥.

(٧٨) كرار عباس متعب فرج: الحرب السيبرانية: دراسة إستراتيجية في الهجمات بين إيران والولايات المتحدة الأمريكية، مجلة حامورابي للدراسات، العدد ٤٠، السنة ١٠، ٢٠٢١م، ص٣٤.

(٧٩) خالد مخلف الجنفاوي، التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت، المجلة العربية للآداب والدراسات الإنسانية، مج ٥، العدد ١٩، ٢٠٢١م، ص ٧٧

لمدى قدرة الدول على حماية نفسها من أى محاولات للاختراق، وبالتالى تأمين البيانات، والمعلومات التى تملكها، وحماية أمنها القومى، خاصَة فى ظل توظيف بعض الدول، أو الفاعلين من غير الدول، سواء شركات متعددة الجنسيات، أو منظمات دولية، أو حتى جماعات إرهابية– للفضاء الإلكترونى كمجال لتحقيق أهدافها بالصراعات المختلفة، وفى ذلك الإطار تطور مفهوم القوة، ومفهوم "الحروب السيبرانية"Cyber Wars ، وتزايدت القدرات المهددة للأمن، والمعوِقة لتحقيق التنمية، حيث تضاعف الخطر الإلكترونى فى المقابل مع تطور الوسائل التكنولوجية، وحدوث طفرة هائلة بها(٨٠).

ويقع على عاتق الإعلام(٨١) مسئولية للقيام بجهود فى تحدى، ومواجهة تهديدات الأمن الفكرى الذى يعني سلامة فكر الإنسان من الانحراف مما يؤدى إلى تحقيق رجاحة فكره الذى ينعكس عليه، وعلى مجتمعه بالأمن والطمأنينة والاستقرار في جميع مجالات الحياة خاصة مجال الأنظمة الإلكترونية، ورفع التوعية بمجال الفضاء الإلكترونى، الذى بات يُستخدم بعدة صور، وأشكال غير سلمية، كأداة لتحقيق ميزة نسبية فى الصراعات الدولية، والأجيال الجديدة من الحروب، بما ينعكس سلبًا على الأمن المعلوماتى العالمى، وهو ما نتج عنه تحولات بمفهوم القوة، واستبدال القوة التقليدية (القوة الصلبة Hard Power )، بأدواته العسكرية، وصولًا إلى مفهوم القوة الإلكترونية، التى لا تخضع لقوانين دولية واضحة، لاختلافها تمامًا عن القوة التقليدية التى شملها القانون الدولى.

لهذا ساد الاعتقاد بأن وسائل الإعلام تستطيع أن تغير اتجاهات الأفراد والسيطرة عليهم، وأن وسائل الإعلام قد حلت محلّ العنف والقهر في السيطرة على الجماهير وسلب عقولهم، انطلاقا من اللعب على نفسيتهم واقناعهم بواقع جديد من خلال طرح قضايا منطقية تؤثر على المتلقين لها، وتجعلهم يؤيدون الطرح التي تتبناه تلك الجهة على حساب الجهة الأخرى؛ حيث تهدف أية عملية اتصالية لإقناع المتلقي والتأثير فيه

(٨٠) نهى مجدى محمد السيد: الأمن السيبرانى وعلاقته بالمضمون الإعلامى فى ظل رؤية مصر ٢٠٣٠، المجلة العلمية لبحوث الإعلام والاتصال، العدد ٣٥، أكتوبر ٢٠٢١، ص ٨٦.
(٨١) خالد محمد غازي: صناعة الكذب، كيف نفهم الإعلام البديل، وكالة الصحافة العربية، الجيزة، ٢٠٢٢م، ص ١٤.

(ISSN: 2356 - 9492)

معرفيا ونفسيا وسلوكيا عبر تزويده بالمعلومات والبيانات سواء كانت صحيحة ضمن سياقاتها الطبيعية أو معلومات ناقصة أو حتى كاذبة ومفبركة، ويتم ذلك بأساليب وبرامج مختلفة عبر مواقع التواصل الاجتماعي. (٨٢)

ومما يزيد من أهمية وتأثير وخصوصية دور المضمون الإعلامي تحدى الأمن السيبراني المتمثل في المخاطر الأمنية والتهديدات المرتبطة بمهاجمة الأمن الفكري، حيث يعجز النهج التقليدي عن مواجهتها ويستلزم وجود إستراتيجية وطنية وعمل مؤسسي استباقي لمعالجة التهديد بالتركيز على مصدر الخطر، حيث أن انتشار استخدام التكنولوجيا الحديثة للإعلام والاتصال قد فرض واقعاً سيبرانياً جديداً أصبح يسمى بالفضاء السيبراني أو الافتراضي، الذى أثر على حياة الأفراد والمجتمعات، وأفرز العديد من الجرائم الإلكترونية، أو ما يعرف بالجرائم المعلوماتية، وذلك بالتزامن مع التطورات المتلاحقة للتقنية والتكنولوجيا(٨٣).

وتعتمد استراتيجية الحرب النفسية للمعلومات على مدّ المتلقي بمجموعة من المعلومات المتناقضة مع بعضها البعض في الآن نفسه تجعله في حيرة من أمره هل يصدق هذا أم يصدق هذا مما يؤدي إلى تشظي الرأي العام الأولي المعارض وتحدث عملية إعادة تشكيل رأي عام يتفق مع هدفها حيث يمكن للمعلومات والإشاعات التي تتولىّ الجهات المستخدمة بثها أن تؤدي إلى تشكيل رأي عام يتبلور بالإتجاه التي تسعى إلى تحقيقه(٨٤).

وبما أن عملية السيطرة على الرأي العام في الوقت الحالي تحتاج إلى التمكن من السيطرة على وسائل الإعلام الاجتماعي الجديد والتكنولوجية لتتمكن من الوصول إلى

(٨٢) محمد الراجي: *صناعة الأخبار الكاذبة ولولب الحصار المعلوماتي للرأي العام*. (٢٧ مايو/ايار, ٢٠١٨)، تم الاسترداد من مركز الجزيرة للدراسات http://studies.aljazeera.net.

(٨٣) نهى مجدي محمد السيد: الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر ٢٠٣٠م، المجلة العربية لبحوث الإعلام والاتصال، العدد ٢٥، أكتوبر ٢٠٢١م، ص ٤٨٤.

(٨٤) غالب كاظم الداعمي: *صناعة الرأي العام من عصر الطباعة إلى فضاء االإنترنت - تقاليد موروثة وسلطة مطلقة*، دار أمجد للنشر والتوزيع، الأردن ٢٠١٩م، ص١٥.

أكبر فئة من الرأي العام المهتم بالقضية التي تخصها، نظراً لقدرة وسائل الإعلام التقليدية أو الجديدة على الوصول إلى إعداد كبيرة من البشر والتأثير عليهم بسهولة(٨٥).

وبفضل النقلة التكنولوجية الرقمية مثل الإعلام منصة واسعة الاستخدام وفقاً للنوايا الاجتماعية والأيديولوجية، الأمر الذى فتح المجال لاستخدامات غير مشروعة وضعت المجتمعات والدول في موقف لا يحسد عليه، حيث ظهرت أشكالاً جديدة من الجرائم التى اتخذت صفة إلكترونية شملت القدرة على التسلل والاختراق للمواقع وتدمير البيانات الحساسة أو سرقتها واستغلالها أو حتى سرقة الأموال وانتهاك الأمن والخصوصية(٨٦).

لذا يلعب الإعلام دوراً جوهرياً وأساسياً في مختلف نواحي الحياة الإنسانية والثقافية والاجتماعية والأمنية وأيضاً السياسية، فالإعلام وسيلة لنمو وتنمية واستقرار كافة المجتمعات، ليمثل الإعلام الدور الضابط الناعم لنشر وتفعيل الوعي الأمني، ويؤدى كذلك دوره في دعم عمل الجهات الأمني ومساندته على مواجهة الاختراقات التى انتشرت مؤخراً بشكل يهدد استقرار المجتمعات وأمنها(٨٧).

فكثيرة هي الجهات المؤثرة التي تريد دوما توجيه الرأي العام لخدمة أغراضها الشخصية، وكسب رأي عام موالي لوجهة نظرها، وبما أن عملية السيطرة على الرأي العام في الوقت الحالي تحتاج إلى التمكن من السيطرة على وسائل الإعلام الاجتماعي الجديد والتكنولوجية حتى تتمكن من الوصول إلى أكبر فئة من الرأي العام المهتم بالقضية التي تخصها، نظراً لقدرة وسائل الإعلام سواء كانت التقليدية أو الجديدة على الوصول إلى إعداد كبيرة من البشر والتأثير عليهم بسهولة(٨٨).

---

(٨٥) إيناس إبراهيم الشيتي: تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية بالمملكة العربية السعودية، دراسة تطبيقية على جامعة القصيم، ماجستير غير منشورة، جامعة القسيم، ٢٠١٩م.

(٨٦) سلام لامية، طالة وكهينة: الجريمة الإلكترونية بُعد جديد لمفهوم الإجرام عبر منصات التواصل الاجتماعي، مجلة الرواق للدراسات الاجتماعية والإنسانية، المجلد ٦، العدد ٢، ٢٠٢٠م، ص ٤٨٥.

(٨٧) إسماعيل جابوربي: دور الأمن السيبراني في مواجهة التهديدات الإلكترونية، دراسة حالة الجزائر، مجلة تحولات، المجلد الثالث، العدد الثاني، الجزائر ٢٠٢٠م، ص ٤٨٥.

(٨٨) إيناس إبراهيم الشيتي: تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية بالمملكة العربية السعودية، دراسة تطبيقية على جامعة القصيم، ماجستير غير منشورة، جامعة القسيم، ٢٠١٩م.

(ISSN: 2356 - 9492)

يطلق على هذا النوع من الإعلام مسميات عدة تستخدم بالترادف مع الإعلام السيبرانى، منها الإعلام الجديد أو الإلكترونى أو الرقمى، وكلها مسميات يستخدمها الباحثون للإشارة إلى معنى واحد وهو ذلك الإعلام بوسائله المختلفة الموجود على شبكة الإنترنت والفضاء الإفتراضى، لتصبح هذه الأدوات الجديدة هى وسائل نقل الأخبار والمعلومات بشكل مستمر حاملة معها الكثير من الأفكار العابرة لحدود مجتمعاتها [٨٩].

ويقع على عاتق الإعلام[٩٠] مسئولية للقيام بجهود فى تحدى، ومواجهة تهديدات الأمن الفكرى، وتزايدت القدرات المهددة للأمن، والمعوِّقة لتحقيق التنمية، حيث تضاعف الخطر الإلكترونى فى المقابل مع تطور الوسائل التكنولوجية، وحدوث طفرة هائلة بها[٩١]. فكان دور الأمن الفكري والعمل به كمبدأ لتمكين الشباب من مواجهة الانحرافات، ونبذ ثقافة العنف والتطرف والجريمة والعدوان من خلال العمل على توعية الأفراد والمؤسسات عن طريق الإعلام للتغلب على معوقات تعزيز الأمن الفكري[٩٢].

كما تتهدد البنية الكونية للمعلومات بشكل حاد نتيجة تعاظم الارتباط بالفضاء الإلكترونى، كما استغل ذلك العديد من الجماعات الإرهابية[٩٣]، التى تسعى للإضرار بالأمن القومى للدول، وقد رصدت العديد من الدراسات[٩٤] الأطر القانونية والضوابط المهنية والأخلاقية لضبط عملية النشر عبر الإنترنت، وتنطلق من نظرية المسئولية الاجتماعية وحقوق النشر والتأليف وحقوق الملكية الفكرية، وقد حددت الآليات التى

(٨٩) أسماء عاصم: الإعلام الجديد: الإشكاليات وأنماط التغير، المركز العربى للبحوث والدراسات، مارس ٢٠٢٠م، ص ٥٤.

(٩٠) خالد محمد غازي: صناعة الكذب، كيف نفهم الإعلام البديل، وكالة الصحافة العربية، الجيزة، ٢٠٢٢م، ص ١٤.

(٩١) نهى مجدى محمد السيد: الأمن السيبرانى وعلاقته بالمضمون الإعلامى فى ظل رؤية مصر ٢٠٣٠، المجلة العلمية لبحوث الإعلام والاتصال، العدد ٣٥، أكتوبر ٢٠٢١، ص ٨٦.

(٩٢) عواطف بنت يحيى القحطاني: متطلبات تعزيز الأمن الفكري لدى الطالبة الجامعية من منظور طريقة العمل مع الجماعات، المجلة العربية للدراسات الأمنية، جامعة نايف للعلوم الأمنية، مجلد ٣٥، العدد ٢، ٢٠١٩م، ص ٤٩٦

(٩٣) ماجد بن خلاف حمود العنزي: الإرهاب السيبراني وانعكاساته على الأمن الوطني، جامعة نايف العربية للعلوم الأمنية، ٢٠٢١: https://www.repository.nauss.edu.sa/handle/123456789/66752

(٩٤) أبو بكر شحرة: بناء القدرات في الأمن السيبراني، المجلة العربية، الأمن السيبراني حروب الأرقام الصماء، ع ٤٩٨، الرياض، السعودية، ٢٠١٨م، ص ٩.

يمكن الاستناد إليها في صياغة أسس المسئولية الاجتماعية لوسائل التواصل الاجتماعي، لما أحدثته من تغيرات في بيئة الإعلام وأبرزها الضبط الذاتي للمهنة ووضع لقواعد الممكنة للتطبيق وصياغة وتعديل التشريعات بما يتلائم مع تطورات تكنولوجيا الاتصال والمعلومات وتطوير مستوى الوعي بمخاطر تلك الوسائل، ومدى التزامها بأخلاقيات التواصل وما تقوم به من نشر الثقافات، وتكوين الصداقات ومشاركة الرأي، حيث لابد من وجود آلية لمنع نشر الأفكار المتطرفة وسلبيات السعي وراء الشهرة من خلال التجاوز وممارسة الاتصالات الكاذبة وتزييف الصوروالمضامين[٩٥].

## المبحث الثالث

## حماية الأنظمة الإلكترونية في التشريع الكويتي والتشريعات المقارنة

تظهر الجريمة المعلوماتية (السيبرانية)، لتضع حدوداً للرفاهية التى نتجت عن استخدام الشبكة الإلكترونية، وتدفع بالمجتمعات والدول إلى التسابق في سن القوانين العقابية التى تسعى لحماية المعاملات الإلكترونية، حيث تؤدى الهجمات الإلكترونية إلى تداعيات سلبية على التنمية الشاملة (الاقتصادية، والاجتماعية، والسياسية.. وغيرها).[٩٦]

وحتى وقت قريب كانت للحكومات مقاربات مختلفة بشأن التشريعات الخاصة بالإنترنت، فمعظم دول العالم تنظّم الإنترنت ضمن حدود قيمها السياسية والقانونية والأخلاقية والثقافية، فإن اعتماد تشريعات فعالة وتنفيذها لمكافحة جرائم الإنترنت يشكل تحديًا كبيرًا للحكومات، وبالتالي فإن جرائم الإنترنت تمثل تحديًا كبيرًا للأجهزة القانونية، في كلّ من البلدان المتقدمة والنامية، ذلك أن عملية التشريع تستغرق وقتًا طويلاً لمواجهة تلك المخاطر[٩٧].

(95) Zhang ,Yuan , et al. (2017). Solution of Media Risk and Social Responsibility Governance of Social Media. ITM Web of Conferences,1 November, available at: https//:www.researchgate.net/.

(٩٦) طارق عبد العظيم والسيد عباس الرشيدي: إثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية على مصادر الأسهم وأحجام التداول: دراسة مقارنة في قطاع تكنولوجيا المعلومات، مجلسة المحاسبة والمراجعة، العدد الثاني، ٢٠١٩م، ص ٤٣-٤٨٧.

(٩٧) أميرة عبد العظيم محمد: المخاطر السيبرانية وسبل مواجهتها في القانون الدولي، مجلة البحوث الفقهية والقانونية بدمنهور، العدد الخامس والثلاثون، الجزء الثالث، ٢٠٢٠م، ص٣٨٨.

(ISSN: 2356 - 9492)

وكان من بين هذه الجهود ما قامت به الدول الأوروبية والعربية لمواجهة وحماية الأنظمة الإلكترونية، فأصدرت دولة السويد عام ١٩٧٣م أول قانون لها في مجال مكافحة تقنية المعلومات ثم الدنمارك من حيث إصدار التشريعات التى تكافح جرائم الحاسب الآلي والإنترنت عام ١٩٨٥، وجاءت بريطانيا عام ١٩٨٦ بإصدار تعريف التزوير، ثم توالت القوانين والتشريعات الدولية.

وعلى الجانب التشريعي العربي فهناك العديد من الدول العربية التي واكبت التطور التقني الحاصل في مجال تكنولوجيا المعلومات وعملت على محاولة التصدي وكان لابد لها من وجود إطار تشريعي قانوني لمواجهة هذه الجرائم في الوطن العربي، بإصدارها عدد من التشريعات الخاصة، ومن بين هذه الدول سلطنة عمان: أصدرت عام ٢٠٠١ جملة من التشريعات لمكافحة الجريمة المعلوماتية تحت مسمى قانون مكافحة جرائم الحاسب الآلي (قانون مكافحة الجرائم الالكترونية)، وكان من أهمها الأتي: المرسوم السلطاني رقم ٧٢ لسنة٢٠٠١م الصادر بشأن تعديل بعض أحكام قانون الجزاء العماني ليشمل معالجة جرائم الحاسب الآلي (الكمبيوتر)، ثم المغرب: سعي المشرع المغربي لوضع نصوص تشريعية تعمل على تنظيم المعالجة القانونية للجريمة المعلوماتية وذلك بموجب القانون رقم ٧٠٠٣ الصادر بتاريخ ١٦ رمضان الموافق ١٤٢٤ الموافق ١١ نوفمبر ٢٠٠٣م.

**التدابير الأمنية لحماية أمن المعلومات:**

يهدف الأمن السيبراني بشكل مباشر إلى الانتقال من العمل التقليدي إلى استخدام التقنيات الحديثة بعمليات الإطلاع على الوثائق وكذلك الاتصالات اللازمة لممارسة العمل الرقابي، تقوم على ربط الوحدات التنظيمية التنفيذية مع الأجهزة الرقابية في التشكيلات التى تعتمد على رقابتها لتسهيل الحصول على البيانات والمعلومات بسرعة

ودقة مرتفعة[٩٨]، والتى تهدف إلى حماية الفضاء السيبراني المحلي من خلال توافر تمكين الخصوصية وحماية سرية المعلومات. ومن هذه التدابير[٩٩]:

- التدابير التنظيمية والمادية: هدفها بناء بيئة آمنة للمعلومات ومنع الوصول إلى المعلومات وقواعدها.[١٠٠].

- التدابير التقنية: التشفير وينقسم إلى تشفير المتماثل / تشفير المفتاح الخاص[١٠١].

- التدابير في التشريع الكويتي:

لا يمكننا إنكار الجهود المبذولة من قبل الجهات القانونية المختصة في دولة الكويت لمكافحة الجرائم التقنية في عالم المعلوماتية والتطور، وتنفيذ وتطبيق هذه الأحكام، وما يتضمنه من قوانين ونصوص لمكافحة جميع جرائم تقنية المعلومات، الأمر الذي يوجب علينا تناول هذه الأحكام والقوانين، لما تحتويه من أحكام موضوعية وأحكاماً إجرائية، وتناولا لما اتجهت إليه القوانين في الكويت للإحجام والتقليل من الجرائم الإلكترونية وانعكاساتها وتأثيراتها السلبية على مجتمعنا الكويتي.[١٠٢]

- فلم ينص المشرع الكويتي على الجانب الإجرائي للجرائم المعلوماتية بالشكل اللازم، فهذه الجرائم تتطلب وجود إجراءات خاصة لكونها تقع في عالم افتراضي، وهو ما

(١) مصباح أحمد حامد الصحفي وآخرين: مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي لمرحلة الثانوية بمدينة جدة، مجلة البحث العلمي في التربية، العدد ١٠، الجزء ١٠، ٢٠١٩م، ص ٤٩٣-٥٣٤.

(99)Shailendra Rathore, Pradip Kumar Sharma. Social network security: Issues, challenges, threats, and solutions, Information Sciences, Vol 421, Italy: Elsevier Ltd, 2018, P. 51.

(١٠٠) عزة فاروق عبدالمعبود وطه محمد حسن: أمن المعلومات الرقمية وسبل حمايتها في ظل التشريعات الراهنة، المجلة المصرية لعلوم المعلومات، مج٧، ع١، بنى سويف ٢٠٢٠م، ص ١٩١.

(101) Qiuyan Tian, Hao Kang, Ting Ai. Analysis and Comparison of Network Information Security Encryption Technology, Advanced in Engineering, Vol. 166, China: Atlantis Press, 2018, P. 679, Available At:

(١٠٢) بوقرين عبد الحليم، قانون مكافحة جرائم تقنية المعلومات الكويتي: دراسة مقارنة، الكويت، مجلة كلية القانون الكويتية العالمية، العدد ٤، ٢٠١٧م، ص ٣١٥.

(ISSN: 2356 - 9492)

يخلق العديد من الصعوبات من الناحية التطبيقية، ويجعل الإجراءات العادية عاجزة عن إثبات هذه الجرائم والوصول إلى المجرمين.

– صدرت حزمة من التشريعات كان من بينها القانون رقم ٦٤ لسنة ١٩٩٩ في شأن حقوق الملكية الفكرية، والقانون رقم ٩ لسنة ٢٠٠١ بشأن استعمال أجهزة الاتصالات الهاتفية وأجهزة التصنت والقوانين المعدلة له، وصدر القانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية الذى اشتمل على ٣٠ مادة منظمة للمعاملات الإلكترونية، وصدر القانون رقم ٦٣ لسنة ٢٠١٥[١٠٣] بشأن مكافحة جرائم تقنية المعلومات، وقد استغل المشرع الكويتي وجود العديد من التشريعات المقارنة والاتفاقيات الدولية المناسب[١٠٤].

ولقد أسهب المشرع الكويتي في ذكر المفاهيم المتعلقة بالجرائم الإلكترونية أكثر من أي قانون آخر، وبإجراء مقارنة بسيطة بين هذه المفاهيم وتلك الواردة في القانون الجزائري أو السعودي أو الاتفاقية العربية نلحظ الدقة في التعبير عن المفاهيم وشرحها، ومع ذلك نلحظ وجود بعض النقائص نوردها فيما يلي: [١٠٥]

١– إن المشرع الكويتي ربط مفهوم الاحتيال الإلكتروني بقصد الحصول على منفعة دون وجه حق أو الإضرار بالغير[١٠٦]، وهو جانب الصواب قليلاً، حيث أنه من المعلوم أن الكثير من عمليات الاحتيال الإلكتروني ترتكب بدفاع المتعة والتحدى، ولم يعرف المشرع الكويتي (التداخل) وهو فعل يختلف عن الدخول غير المشروع، ويختلف عن

(١٠٣) صدر بقصر السيف في ٢٠ رمضان ١٤٣٦- الموافق ٧ يوليو ٢٠١٥م، ليعمل به بعد ستة أشهر من تاريخ نشره في الجريدة الرسمية.

(١٠٤) المادة الأولى من قانون مكافحة جرائم تقنية المعلومات الكويتي.

(١٠٥) بسمة يونس محمد: الحروب السيبرانية وأثرها في التنظيم الدولي"، كلية الآداب والعلوم بالمرج، ليبيا، مجلة العلوم والدراسات الإنسانية، بنغازي، ٢٠١٨م، ص ١٠٨.

(١٠٦) عرف المشرع الكويتي الاحتيال الإلكتروني بأنه" التأثير في نظام إلكتروني أو نظام معلوماتي أو شبكة معلوماتية أو مستند أو سجل إلكتروني أو وسيلة تقنية معلوماتية أو نظام أو جهاز حاسب آلي أو توقيع إلكتروني، وذلك عن طريق البرمجة أو الإفصاح أو النقل أو النشر لرقم أو كلمة أو رمز سري أو بيانات سرية أو خاصة، بقصد الحصول على منفعة دون وجه حق أو الإضرار بالغير".

الالتقاط، وهو يتعلق بمحالة الجاني اعتراض الموجات والإشارات بقصد الإطلاع على محتواها، أو بقصد التشويش وهو ما يحدث في البث التليفزيوني المشفر.

٢- لم يعرف المشرع الكويتي (الوسيط في خدمة الإنترنت) والوسيط له دور كبير في إيصال المعلومات أو توريدها وحفظها، وهو يتحمل جزءاً من المسئولية الجنائية عن بعض هذه الجرائم.

**- في التشريع المصري:**

نصت المادة الثانية من قانون جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨م على التزامات وواجبات مقدم الخدمة بنصها على:

أولاً: مع عدم الإخلال بالأحكام الواردة بهذا القانون وقانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣م، يلتزم مقدموا الخدمة بما يأتي: (١) حفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات لمدة مائة وثمانين يوماً متصلة. (٢) المحافظة على سرية البيانات التى تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضلائية المختصة. (٣) تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها أو تلفها.

رابعاً: يلتزم مقدموا خدمات تقنية المعلومات ووكلائهم وموزعيهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين، دون سواهم(١٠٧).

وكفلت المادة ٧٣ من قانون تنظيم الاتصالات المصري حماية الحق في خصوصية البيانات والمعلومات لمستخدمي الاتصالات في مواجهة القائمين على تقديم تلك الخدمات " يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز خمسن ألف جنيه أو بإحدى هاتين العقوبتين كل من قام أثناء تادية وظيفته في مجال الاتصالات أو بسببها بإذاعة أو تسجيل أو نشر تسجيل لمضمون رسالة أو جزء منها دون سند قانوني، أيضاً إخفاء أو تغيير أو إعاقة أو تحوير أية رسالة

(١٠٧) يقصد بشبكة الاتصالات في هذا القانون النظام أو مجموعة النظم المتكاملة للاتصالات شاملة ما يلزمها من البنية الأساسية (المادة ٥/١)، ويقصد بالمستخدم أي شخص طبيعي أو اعتباري يستعمل خدمات الاتصالات أو يستفيد منها (المادة ٦/١) من القانون المصري.

(ISSN: 2356 - 9492)

اتصالات أو لجزء منها تكون قد وصلت إليه، أو إفشاء أية معلومات خاصة بمستخدمي الشبكة أو عما يجرونه أو ما يتلقونه من اتصالات دون وجه حق(١٠٨).

**خاتمة البحث**

الشبكة الإلكترونية المتصلة أصبحت جزءاً لا يتجزأ من حياتنا اليومية، خير دليل على ذلك استخدام كافة المؤسسات والحكومات هذه الشبكة الإلكترونية بفعالية، عن طريق جمع كميات مهولة من المعلومات الرقمية ومعالجتها وتخزينها ومشاركتها، لذلك أصبحت حماية هذه المعلومات أكثر حيوية لأمننا القومي واستقرارنا الاقتصادي.

ويعد موضوع بحثنا عن الأمن السيبراني وحماية الأنظمة الإلكترونية واحد من مستحدثات التطور التكنولوجي والرقمي الذي نعايشه في العالم مؤخراً، والقاعدة المهمة التي يجب علينا معرفتها هي أنه لا شيء آمن على شبكة الإنترنت.

والأمن السيبراني يحارب تلك المشكلات القانونية والعملية التى تثيرها الجريمة الإلكترونية، فأصبح الأمن السيبراني أصبح حاجة ملحة للقائمين بالمؤسسات الوطنية والدولية على حد سواء، فلا يمكن لأي دولة مهما بلغت من قوة التطور التكنولوجي والصرامة في قوانينها أن تواجه هذا النوع من هذه الجرائم وحدها، ومن ثم وجب على كل الدول النص وتذليل إجراءات التعاون فيما بينها.

وقد أسفر هذا البحث عن بعض من النتائج والتوصيات على النحو التالي:

**أولاً: النتائج:**

١- الجريمة الإلكترونية جريمة متطورة بتطور الوسائل المستخدمة في هذا المجال الإجرامي التقني الجديد، فهي مرتبطة بالتطور الهائل المصاحب للثورة التكنولوجية المعلوماتية في العصر الحديث.

(١٠٨) هذه الخصوصية مقيدة بالمادة ٦٧ من ذات القانون التى تنص على" للسلطات المختصة في الدولة أن تخضع لإداراتها جميع خدمات وشبكات اتصالات مشغل أو مقدم خدمة، وأن تستدعي العاملين لديه القائمين على تشغيل وصيانة تلك الخدمات في حالة حدوث كارثة كبيعية أو بيئية، أو في الحالات التى تعلن فيها التعبئة العامة طبقاً لأحكام القانون ٨٧ لسنة ١٩٦٠، وأي حالات تتعلق بالأمن القومي".

٢- مرتكبي هذا السلوك الإجرامي الإلكتروني هم أشخاص يعيشون بيننا، ويتميزون بالذكاء المعلوماتي، وقدرتهم الفائقة على استخدام هذه التقنيات ووسائلها المختلفة، والقدرة على الاختراق أو التخريب أو التدمير أو الاستيلاء على البرامج والنظم والمعلومات المختلفة المخزنة على المواقع الإلكترونية على أجهزة الحاسبات الإلكترونية أو على شبكات الإنترنت أو على الأجهزة الإلكترونية الحديثة الأخرى.

٣- القصور التشريعي في معظم القوانين الوضعية سواء على المستوي الوطني أو العربي أو الأجنبي، حيث أن القوانين الحالية شبه عاجزة عن كفالة الحماية الجنائية للنظم والمعلومات والبيانات وسائر المستندات المخزنة على الأجهزة الإلكترونية.

٤- عجز الأجهزة والأدوات والوسائل المستخدمة حالياً في مكافحة السلوك الإجرامي الإلكتروني، على الرغم من الجهود المبذولة من الأجهزة التشريعية والأمنية في البحث والتحري والمعاينة والتفتيش والضبط.

٥- ظهر على سطح السلوك الإجرامي الجديد عدة مسميات لأنواع مستحدثة منه وهي الحرب الإلكترونية – الإرهاب الإلكتروني – سوء استخدام نظام التوتير والفيس بوك في التشهير والسب والقذف والإساءة إلى الآخرين.

٧- يوجد اهتمام متزايد بموضوع الجرائم الإلكترونية (المعلوماتية)، ومحاولة تنظيم وكفالة الحماية الجنائية وذلك بتنظيم الجوانب الإجرائية الموضوعية، على المستوي الإقليمي والدولي، إذ تلاحظ اهتمام عدة اتفاقيات دولية وأوروبية، ومن أهمها الاتفاقية الأوروبية للجرائم المعلوماتية لسنة ٢٠٠١، حيث قبلت جميع الاقتراحات المقدمة إليها الخاصة بجميع أنواع أدلة الإثبات الجنائي للحاسب الآلي (الكمبيوتر) دون استثناء.

٨- يوجد اهتمام كبير وملحوظ في معظم الدول العربية والأجنبية وجهود على أعلى مستوى لمكافحة الجرائم الإلكترونية أو الخصوصية المعلوماتية، وعلى رأسها في الدول العربية مصر والكويت وقطر وسلطنة عمان والمملكة العربية السعودية، وفي الغرب الولايات المتحدة الأمريكية وفرنسا وألمانيا وإنجلترا، وفي آسيا اليابان والهند وماليزيا، وفي أفريقيا جنوب أفريقيا وجيبوتي ونيجيريا.

(ISSN: 2356 - 9492)

١١- تدعيم الرقابة المجتمعية والأسرية، وتدعيم دور وسائل الإعلام للتصدي والحديث عن الجرائم الالكترونية والتوعية اللازمة عنها.

١٢- هناك مزيد من التعاون الدولي لمكافحة واجهة الجرائم الإلكترونية والسيطرة عليها.

**ثانيًا: التوصيات**

١- مراجعة المناهج التربوية والأمنية وتطويرها بالوعي الكامل بالجرائم الإلكترونية، وقواعد الأمن السيبراني، وتدعيم وتعزيز الجهة المختصة بمكافحة الجرائم الالكترونية، والمؤسسات الأخرى المدنية المعنية بالتوعية المجتمعية ضد الجرائم الالكترونية.

٢- تجريم صور الجريمة الإلكترونية وكذا الأفعال المتعلقة بحيازة أو نشر أو استعمال المعطيات المتحصل عليها من الجرائم الإلكترونية.

٣- التنسيق والتعاون على المستوى الإقليمي والدولي يتعلق بتدابير حماية أسرار البيانات والمعلومات الاقتصادية والتجارية، وإدراج الجرائم الإلكترونية في إطار معاهدات تسليم المجرمين، ويجب أن تباشر الدعاوي الخاصة بتلك الجرائم في العديد من الدول، وأن تراعي أحكام الإدانة الصادرة عن إحداها، وبخاصة في مجال تشديد العقوبة المنطوق بها في دول أخرى بالنسبة لمعتادي مثل هذا النوع من الأجرام (كتهريب الأموال إلى الخارج عن طريق بطاقات الائتمان والدفع الإلكتروني).

٤- ضرورة تدخل المشرع لمعالجة أوجه القصور والخلل التشريعي، بوضع النصوص التشريعية اللازمة لتجريم الأفعال الإلكترونية غير المشروعة، وكفالة وحماية الحق في حفظ المعلومات والبيانات وخصوصيتها بالنسبة لجمع الأفراد والجماعات.

٥- زيادة الوعي بين الأفراد بصفة عامة، وبين رجال القانون والقضاء والأمن بصفة خاصة بالمستجدات ووسائل الحماية الحديثة لأجهزة الحاسب الآلي وأنظمته وشبكات الإنترنت.

٦- بث التوعية وحس الأفراد بالمجتمع، للإبلاغ والإخبار عن الجرائم الإلكترونية (المعلوماتية) والإفصاح عن شخصية مرتكبيها، وذلك عن طريق عقد ندوات خاصة بالتوعية لضمان عدم إفلات أي مجرم من مرتكبي تلك الجرائم من العقاب.

٧- وضع استراتيجية إعلامية هادفة لنشر الوعي الجماهيري لمخاطر الجريمة الإلكترونية وأساليب وسائل أمن المعلومات، من خلال التنسيق بين الوزارات والهيئات ومؤسسات المجتمع المدني ذات الصلة بذلك الأمر.

٨- على غرار إنشاء محاكم اقتصادية متخصصة، فنرى أنه من الضروري إحالة مثل هذه النوعية من الجرائم (الإلكترونية) إلى قضاء متخصص في الجرائم الإلكترونية، نظراً لصعوبة القضايا المتعلقة بها، وحاجتها إلى المزيد من المعطيات الخاصة قد لا تتوافر للقضاء العادي، وبخاصة في مجال الأمن السيبراني.

قائمة المراجع

**أولاً: المراجع باللغة العربية:**

**الكتب المتخصصة:**

١. الرؤية العربية للأمن السيبراني: الواقع – التحديات – الفرص، تونس، المنظمة العربية لتكنولوجيا الاتصال والمعلومات، ٢٠٢١م.
٢. ابتهاج إسماعيل يعقوب وآخرون: مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية على وفق المتطلبات الدولية: دراسة اختبارية، مجلة الدراسات المالية والمحاسبية والإدارية، المجلد ٩، العدد ١، ٢٠٢٢.
٣. أبو بكر شحرة: بناء القدرات في الأمن السيبراني، المجلة العربية، الأمن السيبراني حروب الأرقام الصماء، ع ٤٩٨، الرياض، السعودية، ٢٠١٨م، ص ٩.
٤. أحمد جلال محمود: أثر التهديدات غير التقليدية للأمن على العلاقات الدولية المعاصرة، الأمن السيبراني في الشرق الأوسط، دراسة حالة من ٢٠٢٠ – ٢٠٣٠، بحث منشور في المؤتمر الدولي مستقبل منطقة الشرق الأوسط – رؤية مصر، جامعة عين شمس، مركز الشرق الأوسط للدراسات المستقبلية، القاهرة، ٢٠٢٠م.

(ISSN: 2356 - 9492)

٥. أكرم محمد رضا الطويل، هضبمة عبد الواحد سلطان الجنابي، التوزيع المادي وعناصر خدمة العميل، الطبعة الأولى، دار الحامد للنشر، عمان – الأردن،
٦. الأمن السيبراني: هيئة الإعلام، الكويت، قسم الدراسات والاتصال والعلاقات العامة، ٢٠٢١.
٧. أميرة عبد العظيم محمد: المخاطر السيبرانية وسبل مواجهتها في القانون الدولي، مجلة البحوث الفقهية والقانونية بدمنهور، العدد الخامس والثلاثون، الجزء الثالث، ٢٠٢٠م، ص٣٨٨.
٨. أمينة ختو: بيئة المؤسسة وأثرها على الأداء الوظيفي، مذكرة مكملة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة عبدالحميد بن باديس، مستغانم، ٢٠١٨-٢٠١٩.
٩. أيمن البوغانمن: بنية سوق المعلومات في عصر الإنترنت: بين الديكارتية المجحفة والداروينية المقلوبة، مجلة ألباب، العدد.١٤، ٢٠١٩، ص ٥٣.
١٠. باسم على خرسان: الأمن السيبراني في العراق: قراءة في مؤشر الأمن السيبراني العالمي ٢٠٢٠، بغداد، مركز البيان للدراسات والتخطيط، ٢٠٢١م.
١١. بسمة يونس محمد: الحروب السيبرانية وأثرها في التنظيم الدولي"، كلية الآداب والعلوم بالمرج، مجلة العلوم والدراسات الإنسانية، بنغازي، ليبيا، ٢٠١٨م.
١٢. تغريد صفاء، لبنى خميس مهدي: أثر السيبرانية في تطور القوة، مجلة حامورابي للدراسات، مركز حمورابي للبحوث والدراسات الإستراتيجية، ع٣٣-٣٤، السنة ٨، بغداد ٢٠٢٠م.
١٣. جمعي فريحة: المسئولية المدنية والجنائية لمقدمي خدمة الإنترنت- التخصص قانوني اجتماعي، كلية الحقوق والعلوم السياسية، جامعة د. مولاي الطاهر، الجزائر، ٢٠١٧-٢٠١٨م.
١٤. خالد محمد غازي: صناعة الكذب، كيف نفهم الإعلام البديل، وكالة الصحافة العربية، الجيزة، ٢٠٢٢م.

١٥. راشد محمد المري، الجرائم الالكترونية، في ظل الفكر الجنائي المعاصر "دراسة مقارنة "، القاهرة ، دار النهضة العربية، ٢٠١٨.
١٦. صاح مهدي هادي الشمري، زيد محمد علي إسماعيل، الأمن السيبراني كمرتكز جديد في الإستراتيجية العراقية، مجلة قضايا سياسية، السنة ١٢، العدد ٦٢، جامعة النهرين، كلية العلوم السياسية، ٢٠٢٠م.
١٧. طارق عبد العظيم والسيد عباس الرشيدي: إثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية على مصادر الأسهم وأحجام التداول: دراسة مقارنة في قطاع تكنولوجيا المعلومات، مجلة المحاسبة والمراجعة، العدد الثاني، ٢٠١٩م.
١٨. عبدالفتاح بيومي حجازي: مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي: دراسة قانونية متعمقة في القانون المعلوماتي، الإسكندرية، دار الفكر الجامعي، ٢٠٢٠.
١٩. عزة فاروق عبدالمعبود وطه محمد حسن: أمن المعلومات الرقمية وسبل حمايتها في ظل التشريعات الراهنة، المجلة المصرية لعلوم المعلومات، مج٧، ع١، بنى سويف ٢٠٢٠م
٢٠. على النقروز، جرائم نظم المعلومات، الأردن، دار السناء للنشر، ٢٠١٧م، ص ١١٤.
٢١. عواطف بنت يحيى القحطاني: متطلبات تعزيز الأمن الفكري لدى الطالبة الجامعية من منظور طريقة العمل مع الجماعات، ، جامعة نايف للعلوم ، ٢٠١٩م.
٢٢. –غالب كاظم الداعمي: صناعة الرأي العام من عصر الطباعة إلى فضاء الإنترنت – تقاليد موروثة وسلطة مطلقة، دار أمجد للنشر والتوزيع، الأردن ٢٠١٩م.
٢٣. كرار عباس متعب فرج: الحرب السيبرانية: دراسة إستراتيجية في الهجمات بين إيران والولايات المتحدة الأمريكية، مجلة حامورابي للدراسات، ٢٠٢١م.

(ISSN: 2356 - 9492)

٢٤. محمد سامي الشوا: الإثبات الجنائي في ظل نظام العولمة والتقنيات الحديثة، دراسة تطبيقية على الاتحاد الأوروبي، التشريع الفرنسي، القاهرة، دار النهضة العربية، ٢٠١٨.
٢٥. المجلات والدوريات:
٢٦. إبراهيم رمضان إبراهيم عطايا، الجريمة الإلكترونية وسبل مواجهتها في التشريع الإسلامي والأنظمة الدولية، دراسة تحليلية تطبيقية، طنطا، مجلة كلية الشريعة والقانون، المجلد ٣٠، العدد ٢، ٢٠١٥م، ص٣٧٣.
٢٧. بوقرين عبد الحليم، قانون مكافحة جرائم تقنية المعلومات الكويتي: دراسة مقارنة، الكويت، مجلة كلية القانون الكويتية العالمية، العدد ٤، ٢٠١٧م.
٢٨. حسين بن سليمان بن راشد الطيار، الأمن السيبراني في منظور مقاصد الشارع: دراسة تأصيلية، المملكة العربية السعودية، جامعة الطائف، مجلة جامعة الطائف للعلوم الإنسانية، المجلد ٦، العدد ٢١، ٢٠٢٠م.
٢٩. حسين بن سليمان بن راشد الطيار، الأمن السيبراني في منظور مقاصد الشارع: دراسة تأصيلية، المملكة العربية السعودية، جامعة الطائف، مجلة جامعة الطائف للعلوم الإنسانية، المجلد ٦، العدد ٢١، ٢٠٢٠م.
٣٠. حمدي محمد محمود حسين، المسئولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعي، برلين، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي، المجلد ٢، العدد ٨، ٢٠١٨م.
٣١. خالد مخلف الجنفاوي، التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت، المجلة العربية للآداب والدراسات الإنسانية، مج ٥، العدد ١٩، ٢٠٢١م.
٣٢. راشد محمد المري، أثر تكنولوجيا المعلومات في النظام الأمني والرقابة الداخلية، مجلة الشريعة والقانون بدمنهور، العدد ٤٠، ٢٠٢٣م.
٣٣. زينب طرفي العنزي، الجريمة الإلكترونية في ميزان الفقه والقانون، العراق، مجلة الدراسات الإسلامية والبحوث الأكاديمية، العدد ٩٩، ٢٠٢٢م.

٣٤. عزة فاروق جوهري، طه محمد حسن، أمن المعلومات الرقمية وسبل حمايته في ظل التشريعات الراهنة، مجلة المركز العربي للبحوث والدراسات في علوم المكتبات والمعلومات، مج ٦، العدد ١٢، ٢٠١٩م، ص ٨٥. متاح على الرابط: http://search.mandumah.com/Record/994947

٣٥. علاء الدين فرحان، من الردعه النووي إلى الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في القضاء السيبراني، الجزائر، جامعة بسكرة، مجلة الفكر، المجلد ١٦، العدد ١، ٢٠٢١م.

٣٦. كامل فتحي كامل خضر، وسمر المداح، العلاقة بين الاقتصاد الرقمي وأمن المعلومات، دراسة تطبيقية على عينة من عملاء البنك الأهلي المصري، المجلة العلمية للاقتصاد والتجارة، المجلد ٥٠، العدد ٣، ٢٠٢٠م.

٣٧. لطيفة نايف سالم الريدين، أثر أمن المعلومات على الاقتصاد الرقمي مع التطبيق على عينة من عملاء بنك الكويتي الوطني، الكويت، مجلة البحوث الإدارية، المجلد ٣٩، العدد ١، ٢٠٢١م.

٣٨. مهدي رضا، الجرائم السيبرانية وآليات مكافتها في التشريع الجزائري، الجزائر، مجلة إليزا للبحوث والدراسات، المجلد ٦، العدد ٢، ٢٠٢١م.

٣٩. نهى مجدي محمد السيد: الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر ٢٠٣٠م، المجلة العربية لبحوث الإعلام والاتصال، العدد ٢٥، أكتوبر ٢٠٢١م.

٤٠. الرسائل العلمية المتخصصة ( ماجستير ودكتوراة ):

٤١. مزيان عبدالقادر، أثر محددات جودة العملاء على رضا العملاء، مذكرة الماجستير، الجزائر، جامعة تلمسان، ٢٠١٢م.

٤٢. شرمالي فتيحة: الجهود الدولية لمكافحة الجريمة المنظمة العابرة للحدود، مذكرة لنيل شهادة الماستر في القانون الخاص، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، ٢٠١٨م.

(ISSN: 2356 - 9492)

٤٣. عيسى سليم داود: جرائم القرصنة الإلكترونية، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، ٢٠١٧م.
٤٤. على زايد محمد الجبيري الشهري: الإطار القانوني للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، رسالة دكتوراه غير منشورة، جامعة نايف للعلوم الأمنية، كلية العلوم الإستراتيجية، قسم الدراسات الإستراتيجية، تخصص دراسات إستراتيجية، ٢٠١٩م.

**النشرات والتقارير:**

٤٥. الضوابط الأساسية للأمن السيبراني، الهيئة الوطنية للأمن السيبراني، ECC-1 : 2018
٤٦. الأمم المتحدة، دليل المناقشة لمؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية، كيوتو، اليابان، ٢٠٢٠م.
٤٧. اتفاقية كومنولث الدول المستقلة، فقرة (أ)، المادة الأولى.
٤٨. اتفاقية مجلس أوروبا بشأن جرائم الحاسوب، العناوين ١، ٢، ٣.
٤٩. الجريدة الرسمية: العدد ٣٢ مكرر (ج) الصادر في ١٤ أغسطس عام ٢٠١٨م.
٥٠. الجريدة الرسمية، ملحق العدد ٤١، بتاريخ ٢٠٠٢/٧/٢٣م.
٥١. المادة الأولى من قانون مكافحة جرائم تقنية المعلومات الكويتي.
٥٢. تقرير ITU، المؤتمر العالمي لتنمية الاتصالات (17-WTDC)، بوينس أيرس، الأرجنتين، ٩–٢٠ أكتوبر ٢٠١٧، مكتب تنمية الاتصالات، الاتحاد الدولي للاتصالات، جنيف، سويسرا، ٢٠١٨، ص٣٠.
٥٣. مشروع اتفاقية الاتحاد الأوروبي، الجزء الثاني، الفصل الأول والثاني، والجزء الثالث، الفصل الخامس.

**المواقع الإلكترونية:**

- المعهد العربي للتخطيط: مخاطر الهجمات الإلكترونية "السيبرانية" وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي على:

ttps://www.researchgate.net/institution/Arab_Planning_Institute2

- ماجد بن خلاف حمود العنزي: الإرهاب السيبراني وانعكاساته على الأمن الوطني، جامعة نايف العربية للعلوم الأمنية، تم الاسترجاع بتاريخ ٢٠٢١/١/٣ على الموقع: https://www.repository.nauss.edu.sa/handle/123456789/66752
- محمد الراجي: *صناعة الأخبار الكاذبة ولولب الحصار المعلوماتي للرأي العام.* (٢٧ مايو/ايار, ٢٠١٨)، تم الاسترداد من مركز الجزيرة للدراسات .http://studies.aljazeera.net

- https://www.cybersecurity-review.com/news-may-2018/phishing-spy-campaign-targets-top-mideast-officials/
- https://infowatch.com/sites/default/files/report/analytics/a_study_of_data_leaks_in_the_middle_east_in_2017-2018_.pdf
- الحروب السيبرانية: نتائج ملموسة لمعارك غير مرئية، الجندي، بتاريخ ٢٠٢١/٤/١م، الشبكة الدولية للمعلومات https//www.alijudi.com.
- المبادئ التوجيهية المتعلقة بأمن البنية التحتية للإنترنت في الدول العربية، مارس ٢٠٢٠م، ص ١١، ولمزيد من الإطلاع: https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc/
- متاح على الموقع الإلكتروني : https://alnaswallhayah.com /
- محمد الراجي: *صناعة الأخبار الكاذبة ولولب الحصار المعلوماتي للرأي العام.* (٢٧ مايو/ايار, ٢٠١٨)، تم الاسترداد من مركز الجزيرة للدراسات .http://studies.aljazeera.net

(ISSN: 2356 - 9492)

**ثانياً: المراجع باللغة الاجنبية:**


1. Adamkolo Mohamed, Umaro Pate, Book Review: Understanding new media 2nd edition by Eugenia Siapera, Journal Komunikasi Indonesia, vol. VIII, no.3, November 2019.
2. BOUDER Hadjira: Quel cadre juridique pour la lutte contre la criminalité liée aux TIC en Algérie, séminaire national sur le cadre juridique des TIC en Algérie; entre opportunité et contraintes, CERIST, Alger, du 16 au 17 mai 2012, p. 4.
3. Csonka P., ( 2020): Internet Crime, the Draft Council of Europe Convention on Cyber- Crime: A Response to the Challenge of Crime in the Age of the internet, Computer Law & Security Report, Vol.28, No.15.
4. Emily Harmer and Karen Lumsden, Online Othering: Introduction, In: Online Othering: Exploring Violence and Discrimination on the Web, 2019.
5. EVELYNE, JACQUES. (2020) Regulating Cybersecurity What civil liability in case of cyber-attacks, p. 231.
6. Fortin, Anne and Heroux, S., (2020), (Cybersecurity disclosure by the companies on the SPP/TSX60, index, vol:19, issue:2, June, pp:73-100.
7. Jérôme Bossan: Le droit pénal confronté à la diversité des intermédiaires de l'internet, RSC, N° 02 du 16/08/2013, p. 295.Rights and Liabilities Involving Online Speech,

available at:http:// www.knox.edu/offices-and-services/information-technology services/computer-use-policies/online-speech.html.

8. National institute of standards and technology (NIST) (2018), a Glossary of key information security terms National institute of standards and technology interagency or internal report. available at http://csrc.nist.gov/publications
9. On June 21, (2018) over 130 participants attended the Geneva Cybersecurity Law & Policy.
10. Qiuyan Tian, Hao Kang, Ting Ai. Analysis and Comparison of Network Information Security Encryption Technology, Advanced in Engineering, Vol. 166, China: Atlantis Press, 2018, P. 679, Available At:
11. Ramirez, M, Ariza, L., and Miranda, M., The disclosure of information on rsecurity in listed companies in Latin America- proposal for a cyber security disclosure index), journal of sustainability ,2022,14(3).
12. Ramirez, M, Ariza, L., and Miranda, M., The disclosure of information on rsecurity in listed companies in Latin America- proposal for a cyber security disclosure index), journal of sustainability ,2022, 14(3).

(ISSN: 2356 - 9492)

13. Reddt, M., & Reddy, G. (2020). A Study of Cyber Security Challenges and Its Emerging Trends On Latest Technologies, Peridot Technologies, 26 (9), 202-2020.
14. Riza Azmi, and Kautsarina, Revisting cyber definition, European Conference on Cyber Warfare and Security, July 2019.
15. Riza Azmi, and Kautsarina, Revisting cyber definition, European Conference on Cyber Warfare and Security, July 2019.
16. Shailendra Rathore, Pradip Kumar Sharma. Social network security: Issues, challenges, threats, and solutions, Information Sciences, Vol 421, Italy: Elsevier Ltd, 2018, P. 51.
17. Trustwave. 2011. SpiderLabs Global Security Report, Michelle Moore (1/1/2021), "Top Cybersecurity Threats in 2021", University of San Diego, Retrieved 28/11/2021. Edited.
18. Zhang ,Yuan , et al. (2017). Solution of Media Risk and Social Responsibility Governance of Social Media. ITM Web of Conferences,1 November, available at: https//:www.researchgate.net/.