

Cybercrime in Jordanian Law

Mohammad Taha Ibrahim Al-Flaieh
Faculty of Law
Middle East University
mohd@gedaralaw.com

Received : 28/02/2023

Accepted :23/05/2023

Abstract:

As a result of the vast technological development and the start of the digital era and the transition of societies from the actual physical reality to cyber reality, we are experiencing significant and increasing cybercrimes on the individual, society, and the security system. So, this study came to identify cybercrimes as they are actually crimes of the modern era. The study identifies cyber security and its importance in providing the necessary protection for the information network, information systems, data and critical infrastructures associated with it, and explain the concept of cybercrime and its characteristics. Then clarify elements of cybercrime and the penalties for them according to the Jordanian law, specifically Cyber Security Law No. 16 of 2019 and Cybercrime Law No. 27 of 2015. This study concluded that cybercrime has become a reality because of the technological development, which should be tackled through more accurate and comprehensive legal material to prohibit ill use of the provided modern technology, which is complicated and related to cyber space that recognizes no limits.

Keywords: Cyber Security: Cybercrime, Information Network, Information Systems, Electronic Space.

الجريمة السيبرانية في النظام القانوني الأردني

محمد طه ابراهيم الفليح

كلية الحقوق

جامعة الشرق الأوسط

mohd@gedaralaw.com

القبول : 2023/05/23

الاستلام : 2023/02/28

المخلص:

نتيجة للتطور التكنولوجي الهائل، ودخول العصر الرقمي، وانتقال المجتمعات من الواقع الفعلي المادي إلى الواقع السيبراني، أصبحنا نشاهد ظهور الجرائم السيبرانية، وتعدّيها على الفرد والمجتمع والمنظومة الأمنية في الدولة، بشكل ملحوظ ومتزايد، لذا جاءت هذه الدراسة للتعرف إلى الجرائم السيبرانية؛ كونها هي بالفعل جرائم العصر الحديث، حيث بينت الدراسة ما هو المقصود بالأمن السيبراني، وأهميته في توفير الحماية اللازمة للشبكة المعلوماتية، ونظم المعلومات والبيانات، والبنى التحتية الحرجة المرتبطة بها. وبيان مفهوم الجرائم السيبرانية وخصائصها، ثم بيان أركانها والجزاءات المفروضة على مرتكبيها، وذلك وفقاً للتشريعات الأردنية وخاصة قانون الأمن السيبراني رقم (16) لسنة (2019)، وقانون الجرائم الإلكترونية رقم (27) لسنة (2015)، حيث انتهت هذه الدراسة إلى أن الجريمة السيبرانية أصبحت موجودة بحكم الواقع والتطور التكنولوجي، والتي لا بدّ من مواجهتها ضمن نصوص قانونية أكثر دقة وإحاطة؛ لمواجهة إساءة استخدام التكنولوجيا المتاحة ضمن شكلها الحديث، وطابعها المُعدّد المرتبط بالفضاء الإلكتروني الذي لا يعترف بالحدود.

الكلمات المفتاحية: الأمن السيبراني: الجريمة السيبرانية، الشبكة المعلوماتية، نظم المعلومات، الفضاء الإلكتروني.

المقدمة:

إنّ ظاهرة الإجرام السيبراني المتطورة تحمل جانباً مُظلماً، يتجسّد بعدم قدرة القواعد القانونية أن تتطور بقدر مساوٍ لتلك الظاهرة، حتى تستطيع الحدّ من تلك التعديات والجرائم التي تتمّ باستخدام شبكات الاتصالات الحديثة، مثل: الإنترنت، والحاسوب، والهواتف النقالة، والبريد الإلكتروني، واعتراض المعلومات السرية أو الكشف عنها، وغيرها من الجرائم العابرة للحدود.

ويشمل الأمن السيبراني أمن المعلومات على أجهزة الحاسب الآلي وشبكاته، بما في ذلك العمليات والآليات التي تتمّ من خلالها حماية معدات الحاسب الآلي، والمعلومات والخدمات من أيّ تدخل غير مقصود، أو غير مصرح به، أو تغيير أو إتلاف قد يحدث. ولقد أصبح الأمن السيبراني ركيزة أساسية في كل المنظمات والمؤسسات بل وحتى الدول؛ لمواجهة الحروب الإلكترونية. فالجريمة السيبرانية هي إحدى الجرائم المعاصرة التي أصبحت تشكل خطراً على الفرد والمجتمع، وعلى الأمن في الدولة ككل، وتتميّز بكونها سريعة التنفيذ، وتتمّ بواسطة أحدث الأجهزة الإلكترونية التي يصعب معها إثباتها أو اكتشاف مرتكبيها. لذا، كانت الدولة سبّاقة في تطوير منظومة الأمن السيبراني؛ من أجل حماية الشبكة المعلوماتية، ونظم المعلومات والبيانات، والبنى التحتية الحرجة المرتبطة بها، وذلك بسنّ القوانين والأنظمة التي تختصّ بمكافحة الجرائم السيبرانية، وفرض الجزاءات على مرتكبيها.

أهمية الدراسة:

يكتسب موضوع الدراسة أهمية كبيرة؛ بسبب جسامة الأخطار وحجم الخسائر الناجمة عن الجرائم السيبرانية بأنواعها المختلفة، التي لم تعدّ عواقبها قاصرة فقط على الأفراد فحسب، وإنّما امتدت آثارها لتهدد المجتمع والدول ككل، حيث تقوم الدراسة هنا بالتركيز على التوعية بخطورة الجرائم السيبرانية، وبيان مفهومها وخصائصها، وبيان الإطار القانوني لهذه الجريمة، والجزاءات المفروضة على مرتكبيها، وكذلك مدى كفاية التشريعات القانونية الحديثة لمكافحة الجرائم السيبرانية في حماية التطور التكنولوجي، بعيداً عن القواعد العامة التقليدية التي ذكرت في قانون العقوبات، خاصةً جرائم الحاسوب والإنترنت، والتي تتعرض للكثير من الانتهاكات، على أن تكون تلك النصوص قادرة على مواجهة الظواهر الإجرامية بكل أبعادها وآثارها السلبية، كعمليات النسخ، والحذف، والإتلاف، ونقل المعلومات والبيانات الإلكترونية، أو القرصنة وغيرها من الجرائم السيبرانية بكافة أنواعها المُستحدثة.

مشكلة الدراسة:

إنّ الطبيعة الخاصة للجرائم السيبرانية، وما تتسم به من سمات خاصة تُميزها عن الجرائم التقليدية، تطرح العديد من الإشكالات الجديدة بالنسبة للقانون الجزائي، مثل: الاختصاص التشريعي المكاني والزمني، والذي يتمثل في مدى تطبيق القانون الوطني الجزائي على

الأمن السيبراني هو فرع من فروع التكنولوجيا، يُعنى بحماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقمية؛ التي تهدف عادةً للوصول إلى المعلومات الحساسة، أو تغييرها، أو إتلافها، أو ابتزاز المستخدمين للحصول على الأموال، أو تعطيل العمليات التجارية (Cyber Security report, 2021)، حيث يُعرّف الأمن السيبراني بأنه: "مجموعة من الإجراءات المُتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة"

(Al-Hamamseh & Al-Amarat, 2022) كما يُعرّف بأنه: "أمن الشبكات والأنظمة المعلوماتية، والبيانات والمعلومات والأجهزة المتصلة بالإنترنت، لمواجهة التهديدات ومنعها، أو للحدّ من خطر الهجوم على البرمجيات، أو أجهزة الحاسوب، أو الشبكات. فهو المجال الذي يتعلق بإجراءات الحماية ومقاييسها ومعاييرها المفروضة اتخاذها، أو الالتزام بها؛ لمواجهة التهديدات، ومنع التعديات، أو للحدّ من أثارها في أقصى وأسوأ الأحوال" (Jbour, 2016)، أو "هو النشاط الذي يؤمّن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحدّ من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحوّل الأضرار، إلى خسائر دائمة" (Hassan, 2017).

ويُعرّف الأمن السيبراني أيضًا بأنه "مجموع الوسائل التي من شأنها الحدّ من خطر الهجوم على البرمجيات، أو أجهزة الحاسوب، أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة، وكشف الفيروسات الرقمية ووقفها، وتوفير الاتصالات المشفرة" (Mustafa, 2022).

ثانيًا: التعريف التشريعي للأمن السيبراني:

عرّف الأمن السيبراني في التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام (2011-2010) بأنه: "مجموعة من المهمات، مثل: تجميع وسائل، وسياسات، وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريب، وممارسات فضلى، وتقنيات يمكن استخدامها لحماية البيئة السيبرانية، وموجودات المؤسسات والمستخدمين" (Jbour, 2019) (Fawzy, 2019)، وكذلك قدّمت وزارة الدفاع الأمريكية (البنتاغون) تعريفًا دقيقًا للأمن السيبراني بأنه: "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية من مختلف الجرائم، والهجمات، والتخريب، والتجسس، والحوادث" (Al-Barrak, 2020) (Al-Hamamseh & Al-Amarat, 2022).

أمّا المشرّع الأردني فقد عرّف الأمن السيبراني في المادة الثانية من قانون الأمن السيبراني رقم (16) لسنة (2019)، بأنه: "الإجراءات المُتخذة لحماية الأنظمة، والشبكات المعلوماتية، والبنى التحتية الحرجة من حوادث الأمن السيبراني، والقدرة على استعادة عملها واستمراريتها،

الجرائم السيبرانية التي تُرتكب خارج حدود الوطن، إذا تحقّقت أيّ من عناصرها على إقليم الدولة. وكذلك يثير موضوع البحث مشكلة مدى إمكانية تطبيق نصوص قانون الأمن السيبراني الأردني لسنة (2019)، وقانون الجرائم الإلكترونية رقم (27) لسنة (2015)، في توفير الحماية اللازمة للشبكة المعلوماتية، ونظم المعلومات والبيانات، والبنى التحتية الحرجة المرتبطة بها من التعدي عليها.

وتثير هذه المشكلة بعض التساؤلات الآتية:

ما هو المقصود بالأمن السيبراني وما هي أهميته؟

ما هي الجرائم السيبرانية وما هي خصائصها؟

ماهي أركان الجريمة السيبرانية؟

ماهي الجزاءات القانونية المفروضة على الجرائم السيبرانية؟

خطة الدراسة:

لمعالجة إشكالية الدراسة وجدنا ضرورة تقسيمها إلى مبحثين وفق

الآتي:

المبحث الأول: ماهية جريمة الأمن السيبراني.

المبحث الثاني: أركان جريمة الأمن السيبراني والجزاءات المترتبة عليها.

الخاتمة.

المبحث الأول:

ماهية جريمة الأمن السيبراني:

إنّ الأمن السيبراني أصبح مطلبًا ضروريًا لكل الدول دون استثناء؛ لأنّه يتعلق بالحماية من المخاطر المحتملة عن طريق مصادر خارجية من خلال الإنترنت، بل أصبح الأمن السيبراني ركيزة أساسية في كلّ المنظمات والمؤسسات، وحتى الدول لمواجهة الحروب الإلكترونية. ويشمل الأمن السيبراني أمن المعلومات على أجهزة الحاسب الآلي وشبكاته، بما في ذلك العمليات والآليات التي تتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات، من أيّ تدخل غير مقصود، أو غير مصرح به، أو تغيير أو إتلاف قد يحدث. وعليه، سنبيّن في هذا المبحث مفهوم الأمن السيبراني في مطلب أول، ومن ثمّ نبيّن مفهوم الجرائم السيبرانية في مطلب ثانٍ.

المطلب الأول:

مفهوم الأمن السيبراني:

سنبيّن في هذا المطلب مفهوم الأمن السيبراني، وذلك من خلال بيان تعريفه في الفقه والتشريع في الفرع الأول، ثمّ نبيّن أهمية الأمن السيبراني في الفرع الثاني.

الفرع الأول:

تعريف الأمن السيبراني:

أولاً: التعريف الفقهي للأمن السيبراني:

نظام المعلومات: "مجموعة البرامج والأدوات المُعدّة لإنشاء البيانات أو المعلومات إلكترونياً، أو إرسالها، أو تسلمها، أو معالجتها، أو تخزينها، أو إدارتها، أو عرضها بالوسائل الإلكترونية"، وهو المعنى ذاته الوارد في المادة الثانية من قانون الجرائم الإلكترونية الأردني رقم (27) لسنة (2015).

الشبكات المعلوماتية: "ارتباط بين أكثر من نظام معلومات لإتاحة البيانات والمعلومات والحصول عليها".

البرامج: "مجموعة من الأوامر والتعليمات الفنية المعدة لإنجاز مهمة قابلة للتنفيذ باستخدام أنظمة المعلومات"، وهو المعنى ذاته الوارد في المادة الثانية من قانون الجرائم الإلكترونية الأردني رقم (27) لسنة (2015).

عمليات الأمن السيبراني: "مجموعة من الإجراءات المرتبطة بإدارة ومراقبة واكتشاف حوادث الأمن السيبراني، والتهديدات التي تقع ضمن حيز الفضاء السيبراني، ووضع خطط الاستجابة لها وتنفيذها".

خدمات الأمن السيبراني: "الأنشطة الفنية والإدارية والاستشارية في مجال الأمن السيبراني، بما فيها خدمات التقييم الأمني، والمراقبة، والتدقيق، والخدمات الاستشارية".

المجرم الإلكتروني: هو مستخدم الحاسوب الذي يكون هدفه وهوايته الدخول غير المصرح إلى أنظمة الحاسوب، وكل ما يرتبط بها من معلومات ذات طبيعة خاصة لمالكي هذه المعلومات، وذلك من خلال تحويل لغته إلى لغة رقمية يقوم بتخزينها، ومن ثم استخدامها، واسترجاع معلوماتها باستخدام الحاسوب الإلكتروني الرقمي وملحقاته (Khalili, 2017).

وتجدر الإشارة إلى أن هنالك أصنافاً مختلفة من المجرمين السيبرانيين؛ وذلك نتيجة للتطور الهائل في التكنولوجيا، وأهم هذه الأصناف هي: لص الهوية، وهو من أوائل أصناف المجرم الإلكتروني، والذي يهدف للوصول إلى المعلومات الخاصة بأشخاص آخرين: (أرقام هواتف، وعناوين، وأرقام حسابات)؛ وذلك بنية إجراء معاملات بأسمائهم، مثل: التحويلات المالية والاحتياز، وفي بعض الأحيان يكون هذا الاختراق لحسابات حكومية وشركات. أما النوع الثاني فهو مطارد الإنترنت، وهو من يتتبع الحسابات الشخصية للآخرين، وغالباً ما يتم هذا النوع من الجرائم على وسائل التواصل الاجتماعي، حيث يهدف المجرم للحصول على المعلومات بهدف؛ التهديد والابتزاز والتشهير، والحصول على مبالغ مالية مقابل هذا الأمر. وبالمقابل، نجد أنّ النوع الثالث هو إرهابي الإنترنت، حيث إنّ هذا النوع من أنواع المجرمين يُعدّ من أخطرهم، حيث إنّه مستوحى من السياسة، ويقوم بالدخول إلى المعلومات الحكومية، والشبكات الكبيرة، وذلك بنية إحداث أضرار في الدولة، وزعزعة الأمن الداخلي لها، بالإضافة إلى دوافع سياسية أخرى (Odeibat, 2022).

سواء أكان الوصول إليها بدون تصريح، أو سوء استخدام، أو نتيجة الإخفاق في اتباع الإجراءات الأمنية، أو التعرض للخداع الذي يؤدي لذلك"، حيث أوضحت المادة ذاتها معنى حادث الأمن السيبراني بأنه: "الفعل أو الهجوم الذي يشكل خطراً على البيانات، أو المعلومات، أو نظم المعلومات، أو الشبكة المعلوماتية، أو البنى التحتية المرتبطة بها، ويتطلب استجابة لإيقافه، أو للتخفيف من العواقب أو الآثار المترتبة عليه".

ومن خلال هذه التعاريف نجد أنّها تحرص على اتخاذ كافة الإجراءات الدفاعية لصد الهجمات السيبرانية، والتي تشمل قرصنة أجهزة الحواسيب، وشبكات المعلومات، واتخاذ التدابير المطلوبة للحماية من هذه الهجمات والتحديات، أي أنّ الأمن السيبراني يتبع نهجاً محدداً يتكوّن عادةً من عدة طبقات للحماية، تُنَبِّت في أجهزة الكمبيوتر، أو الشبكات، أو البرامج، أو البيانات التي ينوي المستخدم حمايتها.

ثالثاً: بعض المصطلحات المرتبطة بالأمن السيبراني:

من هذه التعاريف السابق ذكرها، نوضح بعض المصطلحات الواردة فيها لارتباطها بالأمن السيبراني، كما وردت في القانون رقم (16) لسنة (2019)، حيث ذكرت المادة الثانية توضيحاً للمفاهيم والمصطلحات الآتية:

الفضاء السيبراني: "بيئة تتكون من تفاعل الأشخاص، والبيانات، والمعلومات، ونظام المعلومات، والبرامج على الشبكات المعلوماتية، وأنظمة الاتصالات، والبنى التحتية المرتبطة بها".

البنى التحتية الحرجة: "مجموعة الأنظمة والشبكات الإلكترونية، والأصول المادية وغير المادية، أو الأصول السيبرانية والأنظمة التي يعد تشغيلها المستمر ضرورة لضمان أمن الدولة، واقتصادها، وسلامة المجتمع".

التصريح: "الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر، أو إلى الجمهور؛ للدخول إلى أو استخدام نظام المعلومات أو الشبكة المعلوماتية؛ بقصد الاطلاع، أو إلغاء، أو حذف، أو إضافة، أو تغيير، أو إعادة نشر بيانات أو معلومات، أو حجب الوصول إليها، أو إيقاف عمل الأجهزة، أو تغيير موقع إلكتروني، أو إلغائه، أو تعديل محتوياته"، وهو التعريف ذاته الوارد في المادة الثانية من قانون الجرائم الإلكترونية الأردني رقم (27) لسنة (2015).

البيانات: "الأرقام، أو الحروف، أو الرموز، أو الأشكال، أو الأصوات، أو الصور، أو الرسومات التي ليست لها دلالة بذاتها"، وهو المعنى ذاته الوارد في المادة الثانية من قانون الجرائم الإلكترونية الأردني رقم (27) لسنة (2015).

المعلومات: "البيانات التي تمت معالجتها وأصبحت لها دلالة"، وهذا ما جاءت عليه المادة الثانية من قانون الجرائم الإلكترونية الأردني رقم (27) لسنة (2015).

الفرع الثاني.

أهمية الأمن السيبراني:

إنَّ الأمن السيبراني مهم على مستوى المجتمع والأفراد في حماية البيانات الشخصية، والصور، والملفات، والفيديوهات، والحسابات الشخصية، وكلمات المرور، والحسابات البنكية، وكذلك على مستوى الشركات والمؤسسات، في حماية الأصول الإلكترونية، والبيانات، والمعلومات، وبيانات الموظفين، والسيرفرات، والمواقع الإلكترونية، وكذلك على مستوى الدولة في حماية أمنها الإلكتروني، وحماية الأنظمة المالية والاقتصادية والعسكرية، والتلفزيون والراديو من الهجمات الإلكترونية والقرصنة والتعطيل (Al-Barrak, 2020). فالهجمات السيبرانية وما ينجم عنها من أضرار تكلف الشركات والدول مليارات الدولارات سنوياً، حيث تتعرض الدول في اليوم الواحد إلى مئات الآلاف من الهجمات الإلكترونية، ومحاولات تعطيل أو سرقة الأنظمة والمعلومات وغيرها من الهجمات الإلكترونية (Al-Amarat & Al-Hamamseh, 2022)، فالأمن السيبراني يساعد على حماية المؤسسات والشركات من هجمات البرامج الضارة، التي تهدف إلى الاحتيال، والنصب، وسرقة البيانات الشخصية والملكية الفكرية، والتي تؤدي إلى إحداث ضرر كبير لا يمكن للشركات إصلاحه.

ومن الأهداف التي يعمل الأمن السيبراني على تحقيقها، هي حماية البنية التحتية الحرجة للمعلومات الوطنية الحيوية، والاستجابة للحوادث والهجمات الإلكترونية، وحلّها والتعافي منها، وتوافر البيانات للأشخاص المصرّح لهم الوصول إلى البيانات والمعلومات وتعديلها في الوقت مناسب، وذلك من خلال عمليات الأمن السيبراني التي تُعنى بإدارة حوادث الأمن السيبراني، والتهديدات التي تقع ضمن حيز الفضاء السيبراني، ومراقبتها، واكتشافها، ووضع خطط الاستجابة لها وتنفيذها (Cyber Security report, 2021)، وهذا ما نصّت عليه المادة الثانية من قانون الأمن السيبراني الأردني لسنة (2019). وبالتالي، فإنَّ هدف الأمن السيبراني هو توفير الحماية اللازمة للوقاية والتصدي لمثل هذه الهجمات والتحديات، ولا شكَّ بأنَّ ذلك لا يقتصر على التهديدات السيبرانية الخارجية دون غيرها، بل يشمل تهديدات أخرى داخلية تؤثر على الدولة والمجتمع كذلك، إذ إنّه لا بدّ من حماية الجهاز الإلكتروني منها، والتي قد ترتكب نتيجة لجهل المستخدم بتفعيله لبرامج مجهولة المصدر، تحمل برمجيات خبيثة تحدث أضراراً بالسيطرة على البيانات من خلال سرقتها؛ بهدف طلب الفدية المالية، والتي قد تكون مرهقة وكبيرة، ولا يملك الضحية إلا الانصياع لطلبها، إضافةً إلى عمليات اعتراض باستخدام مجموع حركات سريعة في آن واحد؛ مما يسبب ضغطاً على الخوادم، ويؤدي إلى تقليل فاعليتها وتعطيلها؛ لتسبب خسائر كبيرة خاصّة عندما تتزامن مع مواسم معينة، حيث إنّ فوات موعدها تتسع معه الخسارة، والذي ينشأ معه دور الأمن السيبراني

المهم والفاعل بالتدخل بالتحذير أو المنع من الدخول (Atieh, 2014).

وبالتالي، فهناك عدة أنواع من التهديدات التي يمكن أن يتعامل معها الأمن السيبراني، ومنها:

الجرائم السيبرانية: تقوم بهذه الجرائم على الأغلب مجموعات الهاكرز، وتهدف إلى تحقيق مكاسب مالية، أو التسبب في حدوث خلل.

الهجوم السيبراني: يهتم بجمع معلومات من أجل تحقيق دوافع سياسية.

الإرهاب الإلكتروني: ويشمل العبث بالنظم الإلكترونية لمجرد إثارة الذعر أو الخوف.

وهذا ما سوف نبينه في المطلب الآتي:

المطلب الثاني.

مفهوم جريمة الأمن السيبراني:

إنَّ للأمن السيبراني -كما أوضحنا سابقاً- دوراً كبيراً في التقليل من أنشطة الجرائم الإلكترونية، والتي ستزداد بشكل كبير وسريع مع مرور الوقت؛ نظراً للتطور التكنولوجي الهائل، والذي يستلزم الربط بين عدد كبير من الأجهزة المتصلة مع شبكة العالم. وعليه، سنتناول هذا المطلب من خلال فرعين، نخصّص الأول في تعريف الجريمة السيبرانية، ونبيّن في الفرع الثاني خصائص الجريمة السيبرانية، وعلى النحو الآتي:

الفرع الأول.

تعريف جريمة الأمن السيبراني:

إنَّ الجرائم السيبرانية من الجرائم التي تباينت تسمياتها، وتطورت بتطور التقنية المرتبطة بها، فقد أطلق عليها بالبدائية اسم إساءة استخدام الكمبيوتر، ثمّ احتيال الكمبيوتر، ثمّ جرائم الهاكرز، وبعدها جرائم الإنترنت، إلى الجرائم السيبرانية (Abdel Hamid, & Molook, 2020). وتتوقف تعريف الجريمة السيبرانية في المقام الأول على الغرض من استخدام المصطلح، فالجريمة السيبرانية الأساسية تتمثل في عدد محدود من الأعمال التي تمسّ بسرية البيانات، أو النظم الحاسوبية وسلامتها وتوافرها. أمّا الأعمال المنفّذة بواسطة الحواسيب، والرامية إلى تحقيق مكاسب شخصية أو مالية أو إحداث أضرار، بما في ذلك الجريمة المتصلة بالهوية ومحتوى الحواسيب: (والتي تندرج كلّها ضمن نطاق أوسع من معنى مصطلح الجريمة السيبرانية)، فلا يمكن تطويعها بسهولة لتتطوّل ضمن تعريف قانونية لمصطلح جامع. ويلزم تعريف الأعمال الأساسية التي تشكل جريمة سيبرانية، وإن كان تعريف الجريمة السيبرانية لا يتّسم بالقرن نفسه من الأهمية فيما يخص الأغراض الأخرى، كتحديد نطاق صلاحيات الهيئات المختصة بالتحريات والتعاون الدولي، حيث يفضل التركيز على الأدلة الإلكترونية فيما يخصّ أيّ جريمة، بدلاً من التركيز على

السيبرانية تتميز بعدة خصائص تميزها عن غيرها من الجرائم التقليدية، بكونها تحتاج لقيامها أجهزة كمبيوتر، أو أجهزة موبايل، وشبكة إنترنت، فهي لا تحدّد بحدود معينة؛ نظراً لاتساع استخدام شبكة الإنترنت، وهي من الجرائم التي يصعب إثباتها؛ كونها ترتكب عن بُعد بواسطة أجهزة تكنولوجية متطورة.

وعليه، سنبين أهم الخصائص التي تتميز بها الجرائم السيبرانية وفق التفصيل الآتي:

أولاً: تتميز الجرائم السيبرانية بأنها من الجرائم التي ترتكب عن بُعد بواسطة أجهزة إلكترونية متطورة:

نظراً لكون الجريمة السيبرانية ترتكب عن بُعد بواسطة أجهزة إلكترونية متطورة، والتي تُعدّ الوسيلة الأوضح لقيام هذه الجريمة، فيمكن اعتبارها من أهم الخصائص التي تميز هذه الجريمة عن غيرها من الجرائم الأخرى. وبالتالي، يُعدّ الجهاز الإلكتروني هو الذي يميز الجريمة الإلكترونية، وبدونه كوسيلة لا يمكن وصفها بأنها جريمة إلكترونية، فهي من الجرائم التي تحتاج إلى دقة وخبرة عالية من الجاني بأجهزة الحاسب الآلي والإنترنت للقيام بها (Ladadoh, 2021).

ثانياً: تتميز الجرائم السيبرانية بأنها من الجرائم العابرة للحدود:

نتيجة الانتشار الواسع والسريع لشبكة الإنترنت، وسهولة الوصول والولوج إليها في أيّ مكان بالعالم، نتج ارتباط بين أجهزة الحاسب الآلي التي ترتبط بشبكة الإنترنت دون أن يحدها مكان أو حدود، فهي لا تعرف الحدود الجغرافية للدول لارتباط العالم بشبكة واحدة (AlSahafi, 2020)، فأصبح من السهل على المجرمين أن يكونوا في بلد غير البلد التي يوجد فيها موقع الهجوم، أو الاعتداء على الأفراد، أو أمن الدولة، فكان لا بدّ من وجود آلية دولية وإقليمية للحدّ من هذه الهجمات، ومكافحتها، والتصدي لفاعليها ومحاسبتهم (Ladadoh, 2021).

ثالثاً: تتميز الجرائم السيبرانية بأنها من الجرائم صعبة الإثبات والاكتشاف:

إنّ الجريمة السيبرانية أو الجريمة الإلكترونية على خلاف الجرائم التقليدية الأخرى، لا تترك أثراً مادياً ملموساً؛ مما يصعب معه اكتشافها وإثباتها، إضافة إلى كون الجاني بعيداً جداً، وربما يكون في دولة أخرى عن المجني عليه، وذلك عبر استخدامه أجهزة إلكترونية متطورة وحديثة لارتكاب جريمته، بالإضافة إلى سرعة ارتكاب هذه الجريمة والتي ربما تستغرق بضعة ثوانٍ، ممّا يجعل منها جريمة عابرة للقارات، والذي معه تكون صعبة الاكتشاف والإثبات؛ لسهولة محو الآثار المترتبة عليها (Al-Zoubi & Al-Manasah, 2010).

المبحث الثاني.

أركان جريمة الأمن السيبراني والجزاء المقررة لها:

كما بيّنا سابقاً، إنّ أيّ فعل أو هجوم يشكل خطراً على البيانات،

تركيبة واسعة واصطناعية للجريمة السيبرانية (United Nations Office on Drugs & Crime, 2013).

ونتيجة حداثة الجرائم السيبرانية وتطورها، فإنّ فقهاء القانون لم يستقروا على تعريف واحد لهذه الجريمة، فمنهم من عرّفها بأنها: "الجريمة التي تتم بواسطة الكمبيوتر، أو أحد وسائل التقنية الحديثة على كمبيوتر آخر، أو أحد وسائل التقنية الحديثة، مع ضرورة توفر شبكة اتصال فيما بينها" (AlSahafi, 2020). وعرّفها جانب آخر بأنها: "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة، كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود" (Al-Quraan, 2017). كما عرفت الجريمة السيبرانية بأنها: "السلوك غير المشروع أو المنافي للأخلاق أو غير المسموح به المرتبط بالشبكات المعلوماتية العالمية، فهي جرائم العصر الرقمي التي تطلّ المال، والمعرفة، والثقة، والسمعة، وهي كلّها تنفذ عن طريق التقنية" (AlSahafi, 2020). وقد اتّجه جانب كبير من الفقهاء إلى اعتماد التعريف الذي تبنته منظمة التعاون الاقتصادي والتنمية (OCDE)، المنعقد في باريس سنة (1983)، حيث عرفت الجريمة المعلوماتية بأنها "كلّ سلوك غير مشروع، أو غير أخلاقي، أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو نقلها" (Abdel Hamid & Molook, 2020).

أما المشرّع الأردني فلم يعرف الجريمة السيبرانية أو الجريمة الإلكترونية، لا في قانون الجرائم الإلكترونية رقم (27) لسنة (2015)، ولا في قانون الأمن السيبراني رقم (16) لسنة (2019)، إلّا أنّه أورد في المادة الثانية من قانون الأمن السيبراني، معنى حادث الأمن السيبراني بأنه: "الفعل أو الهجوم الذي يشكل خطراً على البيانات، أو المعلومات، أو نظم المعلومات، أو الشبكة المعلوماتية، أو البنى التحتية المرتبطة بها، ويتطلب استجابة لإيقافه، أو للتخفيف من العواقب أو الآثار المترتبة عليه"، أي أنّ المشرّع الأردني عدّ كلّ فعل أو هجوم يشكل خطراً على البيانات، أو المعلومات، أو نظم المعلومات، أو الشبكة المعلوماتية، أو البنى التحتية المرتبطة بها، جريمة سيبرانية. وبالتالي، يمكننا تعريف الجريمة السيبرانية بأنها جريمة إلكترونية تقع ضمن جرائم الحاسوب وتقنيات المعلومات، وأنها فعل ينطوي على استخدام وسيلة تقنية معلومات، أو نظام معلوماتي، بما يخالف أحكام القانون، وهو ما لم يجزّه قانون الجرائم الإلكترونية، وإنّما جرّم بعض الأفعال التي تقع ضمن أنظمة المعلومات.

الفرع الثاني.

خصائص جريمة الأمن السيبراني:

إنّ خصائص هذه الجريمة تتمثل في كونها عابرة للحدود، وتقع في بيئة رقمية تتسم بالخطورة البالغة، في حين يتسم مرتكبوها بالتخصصية والمهارة التكنولوجية العالية؛ بهدف تحقيق مكاسب مالية، أو الانتقام، أو الترفيه، إضافة إلى أنّ الدوافع على ارتكاب الجريمة قد تتطور إلى الإرهاب والاعتداء على الخصوصية، أي أنّ الجرائم

الفرع الثاني.

الركن المادي للجريمة السيبرانية:

يقصد بالركن المادي للجريمة هو فعل خارجي له طبيعة مادية محسوسة تُدركه الحواس، ولذلك فلا جريمة بلا ركن مادي، فهو الفعل أو السلوك الذي يقوم به الشخص، ويُجرّمه القانون الجزائي، ويرتّب على القيام به عقوبة، ويتكوّن الركن المادي من عناصر ثلاثة، وهي: السلوك الإجرامي، والنتيجة الإجرامية، وعلاقة السببية بين السلوك والنتيجة الإجرامية (Jbour, 2012). ويتمثل الركن المادي للجريمة السيبرانية في سلوك إجرامي إرادي، يستعمل فيه الجاني وسائل أو أساليب غير مشروعة، تُشكّل اعتداءً على الأمن السيبراني، وتُشكّل خطراً على الشبكة المعلوماتية، أو البيانات، أو نظم المعلومات، أو البنى التحتية المرتبطة بها. والسلوك الإجرامي في الجريمة السيبرانية يتطلب قيام الجاني بفعل إيجابي يتمثل في قيامه بأفعال وأساليب غير مشروعة، من أجل الحصول بأيّ وسيلة كانت على البيانات، أو نظم المعلومات، أو قيامه بفعل سلبي، يتمثل بقيام الجاني بمخالفة نص القانون، والدخول على المواقع أو الشبكة المعلوماتية، أو نظم المعلومات بدون تصريح، إضافةً إلى تحديد بداية السلوك الإجرامي والشروع فيه (Al-Zaraa, 2014). وحتى يتحقّق السلوك الإجرامي لا بدّ من أن تتوفر الوسائل التكنولوجية التي تؤدي لقيام هذه الجريمة من أجهزة حاسب آلي، أو هواتف ذكية، بالإضافة إلى شبكة الإنترنت، فبغير ذلك لا يتحقّق الفعل أو السلوك الجرمي، وبالتالي لا نكون أمام جريمة اعتداء يشكّل خطراً على الأمن السيبراني (Hijazi, 2004)، وهو ما أكّده المشرّع الأردني في قانون الجرائم الإلكترونية لسنة (2015) ضمن المادة الرابعة منه، عندما جرّم بعض الأفعال التحضيرية التي تُعتبر بحدّ ذاتها جريمة.

الفرع الثالث.

الركن المعنوي للجريمة السيبرانية:

لا تقوم الجريمة قانونياً بمجرد ارتكاب الفاعل للفعل الجرمي المكوّن للركن المادي، بل يجب أن يصدر هذا الفعل عن شخص طبيعي متمتعاً بالأهلية القانونية يسند إليه هذا الفعل معنوياً. فالقاعدة العامة أنّه لا جريمة بغير ركن معنوي، فيه يتم تحديد مسؤولية الفاعل عن الجريمة، بحيث لا يُسأل الفاعل عن الجريمة ما لم تكن هناك صلة بين مادياتها ونفسيته (Al-Baraiseh, 2021).

ويقصد بالركن المعنوي العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني مرتكبها، وهذه العلاقة هي محلّ الإذئاب في معنى استحقاق العقاب، ومن ثم يوجّه إليها لوم القانون وعقابه (Al-Baraiseh, 2021). ولذلك فإنّ الركن المعنوي للجريمة السيبرانية قد يتخذ صورة القصد، ولكنّه قصد عام يُضاف إليه في بعض الحالات قصد خاص، وبعبارة أخرى قد يتخذ القصد الجرمي صورة الخطأ،

أو المعلومات، أو نظم المعلومات، أو الشبكة المعلوماتية، أو البنى التحتية المرتبطة بها يُعدّ جريمة سيبرانية، وتقوم هذه الجريمة على عدة أركان بالإضافة إلى الجزاء المترتب على ارتكاب هذه الجريمة، وهذا ما سنبيّنه من خلال مطلبين، نُخصّص الأول لبحث أركان جريمة الأمن السيبراني، ونتناول في الثاني الجزاءات المقررة لجريمة الأمن السيبراني وفق الآتي:

المطلب الأول.

أركان جريمة الأمن السيبراني:

إنّ الجريمة السيبرانية لا تختلف عن أيّ جريمة أخرى، فهي تقوم على عدة أركان تتمثل بالركن الشرعي، والركن المادي، والركن المعنوي. وهذا ما سنبيّنه من خلال ثلاثة فروع، نبين بالأول الركن الشرعي للجريمة السيبرانية، ونُخصّص الثاني للركن المادي للجريمة السيبرانية، أمّا الثالث سنلقي الضوء من خلاله على الركن المعنوي للجريمة السيبرانية، وعلى النحو الآتي:

الفرع الأول.

الركن الشرعي للجريمة السيبرانية:

يقصد بالركن الشرعي ضرورة وجود نصّ في القانون يجرم الفعل الذي ارتكبه الشخص حتى تقوم مسؤوليته، وبالتالي إيقاع العقوبة المناسبة عليه، ويُعتبر هذا الركن مقترضاً في الجرائم كافة على اختلافها. فالركن الشرعي يعني السند القانوني لتجريم الفعل، وذلك تطبيقاً لمبدأ الشرعية، بأن "لا جريمة ولا عقوبة إلا بنص". وإعمالاً لذلك، فإنّه من غير الممكن بحال الاجتهاد من القاضي الجزائي، فلا يجوز القياس في التجريم (Jbour, 2012)، خاصةً وأنّ الجرائم الإلكترونية حديثة وذات تقنية عالية، ووضع نصوص خاصة بها ليس بالأمر السهل (Al-Mudhahki, 2014). فالهدف الذي يقصده المشرع من وراء تجريم الأفعال التي تشكل خطراً على البيانات، أو المعلومات، أو نظم المعلومات، أو الشبكة المعلوماتية، أو البنى التحتية المرتبطة بها، هو حمايتها من هذه الاعتداءات، وتعزيز الأمن السيبراني. فكلّ دخول غير مشروع إلى الشبكة المعلوماتية، أو نظام معلومات، سواء أكانت شخصية أم حكومية، تشكل جريمة يعاقب عليها القانون. وهذا ما أوضحه المشرّع الأردني في المادة الثانية من قانون الأمن السيبراني رقم (16) لسنة (2019)، عندما بيّن معنى حادث الأمن السيبراني بأنّه: "الفعل أو الهجوم الذي يشكّل خطراً على البيانات، أو المعلومات، أو نظم المعلومات، أو الشبكة المعلوماتية، أو البنى التحتية المرتبطة بها، ويتطلب استجابة لإيقافه، أو للتخفيف من العواقب أو الآثار المترتبة عليه"، والمتوافق كذلك مع ما جاء في المواد من (3-17) من قانون الجرائم الإلكترونية رقم (27) لسنة (2015)، والذي من خلاله يتبيّن أنّ الركن الشرعي للجريمة السيبرانية، هو نصّ التجريم المشار إليه في تلك النصوص.

المعلوماتية، أو نظام معلومات بأي وسيلة دون تصريح، أو بما يخالف أو يجاوز التصريح، بالحبس مدة لا تقل عن أسبوع، ولا تزيد على ثلاثة أشهر، أو بغرامة لا تقل عن (100) مائة دينار، ولا تزيد على (200) مائتي دينار، أو بكلا هاتين العقوبتين المادتين، (3/أ) من قانون الجرائم الإلكترونية الأردني رقم (27) لسنة (2015).

كما عاقب في الفقرة (ب) من المادة ذاته بأنه: "إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء، أو حذف، أو إضافة، أو تدمير، أو إفشاء، أو إتلاف، أو حجب، أو تعديل، أو تغيير، أو نقل، أو نسخ بيانات، أو معلومات، أو توقيف، أو تعطيل عمل الشبكة المعلوماتية، أو نظام معلومات الشبكة المعلوماتية، فيُعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، ولا تزيد على سنة، وبغرامة لا تقل عن (200) مائتي دينار، ولا تزيد على (1000) ألف دينار". وفي الفقرة (ج) من المادة ذاتها عاقب كل من دخل قصداً إلى موقع إلكتروني؛ لتغييره، أو إلغائه، أو إتلافه، أو تعديل محتوياته، أو إشغاله، أو انتحال صفته، أو انتحال شخصية مالكة، بالحبس مدة لا تقل عن ثلاثة أشهر، ولا تزيد عن سنة، وبغرامة لا تقل عن (200) مائتي دينار، ولا تزيد على (1000) ألف دينار.

واعتبر المشرع الأردني في المادة (12) من قانون الأمن السيبراني لسنة (2019)، المعلومات والبيانات والوثائق ونسخها التي ترد للمركز الوطني للأمن السيبراني، أو تتعلق بأعماله، أو يطلع عليها العاملون فيه ووثائق محمية تسري عليها أحكام قانون حماية أسرار ووثائق الدولة، وهذا ما أكدته قانون حماية أسرار ووثائق الدولة رقم (50) لسنة (1971)، المنشور في عدد الجريدة الرسمية رقم (2315) بتاريخ (1971/8/1)، مع الإشارة إلى أن المشرع الأردني تشدد بالعقوبة؛ إذا نتج عن الدخول دون تصريح نسخ لبيانات حكومية، أو حذفها، أو تعديلها، أو نشرها، والعلة من ذلك خطورة هذه الجرائم على الأمن العام في الدولة، وعلى النظام العام داخل المجتمع.

وتجدر الإشارة إلى أن المشرع الأردني في قانون الجرائم الإلكترونية رقم (27) لسنة (2015)، تناول بعض الجرائم الواقعة على الأمن الوطني، أو العلاقات الخارجية للمملكة، أو السلامة العامة، أو الاقتصاد الوطني في المادة (12) منه، فإذا كان الدخول دون تصريح بصورته البسيطة، تكون العقوبة جُنحة بما لا تقل عن أربعة أشهر، وبغرامة لا تقل عن (500) خمسمائة دينار، ولا تزيد على (5000) خمسة آلاف دينار، أما إذا كان الدخول من أجل إلغاء، أو حذف، أو إفشاء بيانات تتعلق بالأمن الوطني، أو العلاقات الخارجية للمملكة، أو السلامة العامة، أو الاقتصاد الوطني بطريقة غير مشروعة، فتكون العقوبة الأشغال الشاقة المؤقتة، وبغرامة لا تقل عن (1000) ألف دينار، ولا تزيد على (5000) خمسة آلاف دينار، بمعنى أن هذا الفعل يصبح جنائية. وبالتالي تشدد المشرع الأردني في هذا الجانب، لكن ما يؤخذ عليه أنه حصر الظروف المشددة فقط في موضوع الأمن

والقصد الجرمي يتكوّن من عنصرين هما: العلم، والإرادة (Jbour, 2012)، حيث إن إرادة السلوك عنصرٌ جوهريٌ لتكوين الركن المعنوي، سواء أكانت الجريمة عمدية أم غير عمدية (Sorour, 2015). وبالتالي، إذا تمّ الدخول إلى الشبكة المعلوماتية، أو نظم المعلومات دون توفر العلم في البداية لدى المستخدم بأنّ دخوله غير مشروع، ولكن بعد فترة زمنية علم المستخدم أنّ دخوله غير مشروع إلى الشبكة المعلوماتية، أو نظم المعلومات، ولكنّه استمر بالدخول غير المشروع رغم معرفته بذلك، فما هو التوصيف القانوني في هذه الحالة؟

أجاب المشرع الأردني على ذلك، حيث اعتبر أنّ هذه الجريمة لا تقوم إلا بتوفر العلم لدى المستخدم بأن دخوله غير مشروع، فإذا علم بعد دخوله واستمرّ بالدخول، فنقوم الجريمة من لحظة علمه بأنّ الدخول غير مشروع، بشرط أن يكون استمرّ بالبقاء على النظام أو الشبكة المعلوماتية، أما إذا قام بفعله، واخترق النظام الإلكتروني دون علمه بأن دخوله غير مشروع، وانتهى عمله على النظام أو على الشبكة، وبعد انتهاء النشاط علم أن دخوله كان غير مشروع فلا تقوم الجريمة؛ لأنّ الفعل أو النشاط قد انتهت (Ladadoh, 2021)، وذلك وفقاً لنصّ المادة (3/أ) من قانون الجرائم الإلكترونية لسنة (2015)، والتي عاقبت على الدخول قصداً دون وجه حقّ بأية وسيلة موقعاً إلكترونياً، أو نظاماً، أو شبكة إلكترونية، أو تجاوز الدخول المصرح به، أو استمرّ في التواجد بها بعد علمه بذلك.

ويلاحظ أنّ المشرع الأردني نصّ على ضرورة توفر قصد جنائي خاص في قانون الجرائم الإلكترونية الأردني رقم (27) لسنة (2015)، وذلك في المادة الثالثة وحتى المادة السادسة، على أنّ الركن المعنوي في جريمة الدخول بدون تصريح، يقوم على القصد العام والخاص، بمعنى أنّ القصد الجنائي العام يتلخّص في نيّة الدخول غير المشروع إلى النظام الإلكتروني، بينما القصد الجنائي الخاص يتصوّر في نيّة الجاني للوصول إلى حذف المعلومات، أو نسخها، أو تدمير النظام، أو غير ذلك من الأنشطة المُجرّمة.

المطلب الثاني.

الجزاءات المقررة لجريمة الأمن السيبراني:

جرّم المشرع الأردني الجرائم السيبرانية التي تهدّد الأمن السيبراني، وفرض جزاءات أصلية وأخرى تكميلية على مرتكب هذه الجريمة. وعليه، سنبيّن الجزاءات المقررة للجريمة السيبرانية؛ من خلال فرعين: نتناول في الأول العقوبات الأصلية، ونُخصّص الثاني للعقوبات التكميلية، وعلى النحو الآتي:

الفرع الأول.

العقوبات الأصلية:

عاقب المشرع الأردني في المادة الثالثة من قانون الجرائم الإلكترونية رقم (27) لسنة (2015)، كل من دخل قصداً إلى الشبكة

العقوبة الغاية المتوخاة من إيقاعها، وهو تحقق الردع الخاص للمهني أو المزود، وعند حدوث ذلك، ومن منطلق حرص المشرع على المستهلك من المخالفات التي قد يرتكبها المهني مستقبلاً، لجأ المشرع للعقوبات الاحترازية والمتمثلة بمنع المخالف المكرر عن مزاولته نشاطه المهني بشكل دائم أو مؤقت، حيث فرض المشرع الأردني في قانون الامن السيبراني رقم (16) لسنة (2019) عقوبات تكميلية على كل من يخالف أحكام هذا القانون، وأوكل المهمة للمركز الوطني للأمن السيبراني، حيث نصّت المادة (16) منه على أنه:

أ- للمركز اتخاذ إجراء أو أكثر من الإجراءات التالية، بحق من يخالف أحكام هذا القانون، والأنظمة والتعليمات والقرارات الصادرة بمقتضاه، وبما يتناسب مع طبيعة المخالفة، والجهة التي ارتكبتها:

- 1- التنبيه الخطي لتصويب المخالفة خلال المدة التي يحددها.
- 2- تصويب المخالفة والرجوع على المخالف بالنفقات التي تكبدها المركز نتيجة لذلك.
- 3- حجب أو إلغاء أو مصادرة أو تعطيل شبكة الاتصالات، ونظام المعلومات، والشبكة المعلوماتية، وأجهزة الاتصالات، والرسائل الإلكترونية الخاصة مع الجهات ذات العلاقة عن كل من يُشتبه في ارتكابه، أو اشتراكه في أي عمل يشكل حادث أمن سيبراني.
- 4- إلزام الجهة المخالفة باتخاذ الاجراءات القانونية بحق من يثبت تسببه بالمخالفة من العاملين لديها.
- 5- إلغاء أو إيقاف ترخيص المرخص له بتقديم أي من خدمات الأمن السيبراني للمدة التي يراها المركز مناسبة.
- 6- فرض غرامة مالية لا تقل عن (500) دينار، ولا تزيد على (100000) دينار، وتضاعف الغرامة في حال تكرار المخالفة.
- ب- لغايات تطبيق أحكام الفقرة (أ) من هذه المادة، يصدر المجلس تعليمات تحدد معايير المخالفات، وضوابطها، والإجراءات المستحقة عليها.

الخاتمة:

إزاء ما تم تناوله في متن هذا البحث من أهمية عملية للأمن السيبراني، ودوره في تعزيز أمن المعلومات وحمايتها من الهجمات السيبرانية، والذي يقصد به بأنه عبارة عن مجموع الوسائل التقنية والإدارية التي يتم استخدامها؛ لمنع الاستخدام غير المصرح به، وسوء استغلال المعلومات الإلكترونية واستعادتها، ونظم الاتصالات والمعلومات التي تحتويها؛ بهدف ضمان توافر عمل نظم المعلومات واستمراريتها، وتأمين حماية البيانات الشخصية وسريتها وخصوصيتها؛ لحماية المواطنين، فقد تبين من خلال دراسة مفهوم الأمن السيبراني، ومفهوم الجرائم السيبرانية وخصائصها، ثم الأركان التي تقوم عليها جريمة الأمن السيبراني والجزاءات المفروضة على مرتكبيها، العديد

الوطني، أو العلاقات الخارجية للمملكة، أو السلامة العامة، أو الاقتصاد الوطني، وكان من الأفضل أن يتحدث عن المواقع، والبيانات الحكومية بشكل عام.

ويلاحظ أنّ الطبيعة القانونية للأفعال الواردة في النصوص التشريعية المتعلقة بالبيانات الشخصية، تتشكل في جوهرها جناحاً تشدد المشرع في بعضها، لكنّها لم تخرج عن الحبس، حيث كان الحد الأعلى هو الحبس لمدة ثلاث سنوات على أبعد تقدير، وهو ما يشكل مشكلة تشريعية، بحيث كان أولى على المشرع الأردني أن يتشدد في حماية البيانات الشخصية، والمعلومات الإلكترونية في حال الحذف والإلغاء، أسوة بالبيانات الحكومية التي تشدد في حمايتها، وفرض عقوبات رادعة قد تصل إلى السجن لمدة خمس سنوات.

لكن قد يثير التساؤل الآتي: ماذا لو كان الجاني من الأشخاص المصرح لهم بالدخول إلى النظام الإلكتروني، وقام بحذف بيانات ومعلومات إلكترونية، أو إتلافها، أو تعديلها؟ أجاب المشرع الأردني عن هذا التساؤل في المادة (8) من قانون الجرائم الإلكترونية الأردني رقم (27) لسنة (2015) حيث نصّ على أنه: "تضاعف العقوبة على الجرائم المنصوص عليها في المواد من (3) إلى (6) من هذا القانون، بحق كل من قام بارتكاب أي منها بسبب تأديته وظيفته أو عمله، أو باستغلال أي منهما"، كما نصّ في المادة (16) من القانون ذاته على مضاعفة العقوبة في حالة تكرار أي من الجرائم المنصوص عليها فيه، حيث جاء النص على أنه: "تضاعف العقوبة المنصوص عليها في هذا القانون في حالة تكرار أي من الجرائم المنصوص عليها فيه". أمّا قانون الأمن السيبراني رقم (16) لسنة (2019)، فقد خلا من أي جزاء يُفرض على مرتكب الجرائم السيبرانية. وأنشأ المركز الوطني للأمن السيبراني، وذلك في المادة الخامسة منه، وحدّد مهام وصلاحيات المركز، وأوكله مهمة التحقق من الحوادث السيبرانية، وفرض الجزاءات على كل من يخالف أحكام هذا القانون، حيث جاء نص المادة (16) فقرة (أ/6) أنه: "أ- للمركز اتخاذ إجراء أو أكثر من الإجراءات التالية بحق من يخالف أحكام هذا القانون والأنظمة والتعليمات والقرارات الصادرة بمقتضاه، وبما يتناسب مع طبيعة المخالفة، والجهة التي ارتكبتها: ... فرض غرامة مالية لا تقل عن (500) دينار، ولا تزيد على (100000) دينار، وتضاعف الغرامة في حال تكرار المخالفة"، وفقاً لما جاء عليه النص في المادة (16) من قانون الأمن السيبراني الأردني المعمول به. كما عاقب المشرع الأردني في المادة (14) من قانون الجرائم الإلكترونية رقم (27) لسنة (2015) كلاً من المشترك، أو المتدخل، أو المحرض بالعقوبة نفسها لمرتكب الجريمة المنصوص عليها في هذا القانون.

الفرع الثاني.

العقوبات التكميلية:

لم يكتف المشرع بالعقوبة الأصلية، ففي حالات كثيرة لا تحقق

على مرتكبي جرائم الأمن السيبراني، وتخصيص فصل يشمل على الجرائم المفروضة على مرتكبي هذه الجرائم، بالإضافة إلى الجزاءات المفروضة عليه في قانون الجرائم الإلكترونية رقم (27) لسنة (2017)، بما يتوافق ونوع الجريمة، وما يمرّ به العالم من تطور سريع يرافقه تطور أسلوب ارتكاب الجريمة السيبرانية وانتشارها، وتخصيص مساحة في الإعلام لنشر الأحكام القضائية ذات العلاقة؛ لغايات التوعية بما يترتب من عقاب على مرتكبي الجريمة السيبرانية.

References:

- Abdel Hamid, A., and Molook, N. (2020), "Cybercrime and Its Impact on the Threat to Cultural Security in Algeria", Al-Mufaker Journal for Legal and Political Studies, Volume Three, Issue Two, Algeria.
- Al-Amarat and Al-Hamamseh (2022). Cybersecurity, Concept and Challenges of the Era, Dar Al-Khaleej for Publishing and Distribution, Jordan.
- Al-Baraish, H. (2021). "The Moral Pillar of Cybercrime According to the Jordanian Penal Code", Master's Thesis, Faculty of Law, Middle East University, Jordan.
- Al-Barrak, H (2020). "The Legal Role of Cybersecurity in Anti-Crime", King Khalid University Journal for Human Sciences, Volume VII, Issue Two, Saudi Arabia.
- Al-Jbour, M. (2012). Mediator in the Penal Code, General Section, Dar Wael for Publishing and Distribution, Amman.
- Al-Mudhahki, H. (2014). Information Crimes, a Comparative Study, Al-Halabi Rights Publications, 1st edition.
- Al-Quraan, M. (2017). Electronic Crimes, First Edition, Dar Wael for Publishing and Distribution, Jordan.
- AlSahafi, R (2020). "Cybercrime", research published in the Comprehensive Multidisciplinary Electronic Journal, twenty-fourth issue, fifth month; available at the following URL: <https://www.eimj.org/uplode/images/photo..pdf>.
- Al-Zaraa, M (2014). "The Material Pillar of Information Crimes in the Saudi System, a Fundamental and Analytical Study", a master's thesis in criminal justice, College of Graduate Studies, Naif University of Security Sciences, Riyadh.
- Al-Zoubi, J., and Al-Manasah, O. (2010). Technological Crimes of Electronic Information

من النتائج التي تُعدّ أساسًا ومنطلقًا للعديد من التوصيات، التي يؤمل من المشرّع الأردني الأخذ بها، وذلك على النحو الآتي:

أولاً: النتائج:

- إنّ هدف الأمن السيبراني هو توفير الحماية اللازمة للوقاية من حوادث الأمن السيبراني، والتهديدات التي تقع ضمن حيز الفضاء السيبراني، والتصدّي لها.
- اعتبر المشرّع الأردني أنّ كلّ فعل أو هجوم يشكّل خطرًا على البيانات، أو المعلومات، أو نظم المعلومات، أو الشبكة المعلوماتية، أو البنى التحتية المرتبطة بها جريمة سيبرانية.
- يتحقّق الفعل الإجرامي في الجرائم السيبرانية بتوافر الوسائل التكنولوجية التي تؤدي لقيام هذه الجريمة، من أجهزة حاسب آلي، أو هواتف ذكية، بالإضافة إلى شبكة الإنترنت، فبغير ذلك لا يتحقّق الفعل أو السلوك الجرمي.
- يتطلب لقيام الركن المعنوي في الجرائم السيبرانية توافر القصد الجنائي الخاص، بالإضافة إلى القصد الجنائي العام.
- إنّ المشرّع الأردني تشدّد بالعقوبة إذا نتج عن الدخول دون تصريح نسخ لبيانات حكومية، أو حذفها، أو تعديلها، أو نشرها، والعلّة من ذلك خطورة هذه الجرائم على الأمن العام في الدولة، وعلى النظام العام داخل المجتمع.
- قانون الأمن السيبراني رقم (16) لسنة (2019) قد خلا من أيّ جزاء يُفرض على مرتكب الجرائم السيبرانية، سواء بعض الإجراءات التي يفرضها المركز الوطني للأمن السيبراني، بحقّ من يُخالف أحكام هذا القانون، والأنظمة والتعليمات والقرارات الصادرة بمقتضاه، وبما يتناسب مع طبيعة المخالفة والجهة التي ارتكبتها.

ثانياً: التوصيات:

- على المشرّع الأردني أن يراعي أسس التصنيف للطبيعة الفنية والتقنية للحدث السيبراني، وربطه بالقطاع المتأثر به، ومدى أثر هذا التهديد أو الخطر على تقديم الخدمات اقتصاديًا واجتماعيًا.
- ضرورة التعاون الدولي والإقليمي لوضع قيود يتم من خلالها ملاحقة مرتكبي الهجمات السيبرانية.
- العمل على تقديم الدعم المادي للجهات المتخصصة بمكافحة الجريمة السيبرانية، بإيجاد مخصصات مالية، والاهتمام بالأنظمة والأجهزة الإلكترونية التي تساعد على الحماية من الجريمة، والكشف عن الجاني في حال وقوع الجريمة.
- الاهتمام بتأهيل القضاة انسجامًا مع نوع الجريمة السيبرانية وتطورها؛ للوصول إلى أحكام قضائية رادعة قائمة على أساس سليم لتحقيق الردع.
- على المشرّع الأردني تعديل قانون الأمن السيبراني رقم (16) لسنة (2019)، ومعالجة جميع حوادث الأمن السيبراني، وتشديد العقوبات

- Odeibat, A. (2022). "Who is the Cyber Criminal", E3arabi website.
- Sorour, A. (2015). Mediator in the Penal Code, General Section, Sixth Edition, Dar Al-Nahda Al-Arabiya, Cairo.
- Systems, Dar Al-Thaqafa for Publishing and Distribution, Jordan.
- Atieh, A. (2014). "The Role of the New Tools in Preventing Innovative Crimes: Electronic Terrorism and Ways of Facing it", a Paper Presented at the Scientific Seminar: Innovative Crimes According to International and Regional Changes and Transformations, Amman.
- Comprehensive Study on Cybercrime (2013). United Nations Office on Drugs and Crime; Available at: https://www.unodc.org/documents/organized,crime/cybercrime/Cybercrime_Study_Arabic.pdf
- Cyber Security Report (2021). Jordan Media Authority, Studies, Communication and Relations Department.
- Fawzy, I (2019). "Cybersecurity, Social and Legal Dimensions, Sociological Analysis", Social and National Journal, National Center for Social and Criminological Research, Volume 56, Issue 2, Egypt, available at the following link: <https://jns.journals.ekb.eg>
- Hassan, S (2017). Proving Computer's Crimes and Crimes Committed via the Internet, Dar Al-Nahda Al-Arabiya, Cairo.
- Hijazi, A. (2004). Computer and Internet Crimes, House of Legal Books, Cairo.
- Jarallah, A. (2017). Internet Crimes and their Punishment According to the Saudi System for Anti-Information Crimes, a Comparative study, University Book House, first edition, Riyadh.
- Jbour, M (2016). "Cyber is the Obsession of the Era", Arab Center for Legal Research, League of Arab States.
- Khalili, S (2017). "Particularity of Cyber Criminal", Al-Fiker Journal, Volume 12, Algeria.
- Ladadoh, A. (2021). "The Compatibility of the Provisions of the Jordanian Cybercrime Law with the General Provisions of the Penal Code", Master Thesis, Faculty of Law, Middle East University, Jordan.
- Mustafa, I (2022). "Cybersecurity Hacking Crime, Data and Information Use Protection in Egyptian Law", Journal of the Faculty of Law, Cairo University, Khartoum Branch, Third Issue, Volume 12.