

السياسة التشريعية الأردنية لأحكام الأمن السيبراني ما بين الواقع والمأمول

حذيفة محمد أحمد البستنجي ^{ID}

قاضي، المجلس القضائي الأردني - الأردن

Bustanji@yaho.com

ملخص

أصبح الأمن السيبراني قضيةً مهمّةً تثير قلق الدول والشركات والأفراد، ونظرًا إلى تطور أدوات انتهاك أمن الشبكات وأنظمة المعلومات في الفضاء الرقمي؛ تناولت هذه الدراسة التكييف القانوني للأمن السيبراني الذي يُعنى بحماية الأنظمة والشبكات؛ حيث هدفت الدراسة كشف الثغرات التي وقع فيها المشرع الأردني عند تعريف وتنظيم قواعد الأمن السيبراني والجرائم المرتبطة به. اعتمدت الدراسة منهجية تحليلية ومقارنة؛ حيث جرى تحليل الأحكام القانونية المتعلقة بالأمن السيبراني والجرائم المرتبطة به في الأردن من خلال مقارنتها بأحكام وردت في قوانين أخرى؛ لتقييم مدى ملاءمة تلك الأحكام للتطورات التقنية والتحديات الحديثة في هذا المجال. إن اتباع هذه المنهجية التحليلية النقدية المقارنة يهدف إلى تقديم رؤية تشريعية متكاملة، تسهم في تحسين الإطار القانوني الحالي لتعزيز منظومة الأمن السيبراني. وخلصت الدراسة إلى أن الوضع القانوني الحالي يعوق تطوير منظومة الأمن السيبراني، بسبب القصور في تعريفه نفسه، إضافة إلى الخلط بين الواقعة على الأفراد بوسيلة إلكترونية وبين الجرائم الواقعة على الشبكات وأنظمة المعلومات.

الكلمات المفتاحية: الأمن السيبراني، الجريمة السيبرانية، الجريمة الإلكترونية، أنظمة المعلومات، الشبكات المعلوماتية، الأردن

للاقتباس: البستنجي، حذيفة محمد أحمد. «السياسة التشريعية الأردنية لأحكام الأمن السيبراني ما بين الواقع والمأمول»، المجلة الدولية للقانون، المجلد الخامس عشر، العدد المنتظم الأول، 2026، تصدر عن كلية القانون، وتنشرها دار نشر جامعة قطر. <https://doi.org/10.29117/>

ir1.2026.0364

© 2026، البستنجي، الجهة المرخص لها: دار نشر جامعة قطر. تم نشر هذه المقالة البحثية وفقًا لشروط Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0). تسمح هذه الرخصة باستخدام غير التجاري، وينبغي نسبة العمل إلى صاحبه، مع بيان أي تعديلات عليه. كما تتيح حرية نسخ، وتوزيع، ونقل العمل بأي شكل من الأشكال، أو بأية وسيلة، ومزجه وتحويله والبناء عليه، طالما يُنسب العمل الأصلي إلى المؤلف. <https://creativecommons.org/licenses/by-nc/4.0/>

The Jordanian Legislative Policy for Cybersecurity Provisions between Reality and Aspirations

Huthaifa Mohammad Ahmad Albustanji 

Judge, The Judicial Council of Jordan- Jordan

Bustanjii@yahoo.com

Abstract

Cybersecurity has become a significant issue that raises concern among nations, businesses, and individuals alike. Due to the continuous evolution of methods for committing crimes in the digital environment, this study addresses the legal framework of cybersecurity to identify the gaps that the Jordanian legislator has encountered in defining and organizing the relevant provisions and associated crimes. The study concluded that the current legal situation hinders the development of the cybersecurity framework, primarily due to gaps in defining cybersecurity itself and the overlap between electronic crimes against individuals and those targeting networks and information systems. To address this, the study adopted a comprehensive analytical comparative methodology, examining the legal provisions related to cybersecurity and associated crimes in Jordan by comparing them with other legal systems to uncover deficiencies and legislative gaps. This methodology aims to provide a comprehensive perspective that contributes to improving the current legal framework and proposing effective solutions to bridge the gaps and enhance the cybersecurity system.

Keywords: Cybersecurity; Cybercrimes; Electronic Crimes; Information systems; Networks; Jordan

Cite this article as: Albustanji, H. M. A. "The Bill of Exchange Domiciliation Clause, A Comparative Study in the Light Of French Judicial Rulings," *International Review of Law*, Vol. 15, Regular Issue 1, 2026. <https://doi.org/10.29117/irl.2026.0364>

© 2026, Albustanji, H. M. A., licensee, IRL & QU Press. This article is published under the terms of the Creative Commons Attribution Non-Commercial 4.0 International (CC BY-NC 4.0), which permits non-commercial use of the material, appropriate credit, and indication if changes in the material were made. You can copy and redistribute the material in any medium or format as well as remix, transform, and build upon the material, provided the original work is properly cited. <https://creativecommons.org/licenses/by-nc/4.0>

مقدمة

في السنوات الماضية، لم يعد الأمن السيبراني مجرد تقنية سريعة التطور فحسب، بل أصبح ضرورةً أساسيةً تزداد أهميتها لكل فرد وشركة ومؤسسة حكومية. إذ يمكن أن تؤدي اختراقات أنظمة المعلومات والشبكات إلى مخاطر جسيمة واضطرابات كبيرة، مما يتسبب في انتهاكات للخصوصية وعمليات ابتزاز إلكتروني، بالإضافة إلى تهديدات تمس الأمن القومي للدول. من هنا، يتضح أن الشركات والحكومات والأفراد بحاجة إلى تكثيف جهودهم لتعزيز إجراءات الأمن السيبراني. ولا يمكن تحقيق ذلك إلا من خلال وضع تشريعات قوية توفر الأساس القانوني المتين لأي حلول تقنية تهدف إلى مواجهة الهجمات السيبرانية وملاحقة مرتكبي الجرائم المرتكبة بالفضاء الرقمي. وفي هذا السياق، يرتبط تعزيز الأمن السيبراني في المملكة الأردنية الهاشمية بشكل وثيق بالأطر القانونية المعمول بها، مثل قانون الأمن السيبراني الأردني وقانون الجرائم الإلكترونية. وبالتالي، سنتناول هذه الدراسة تحليل بعض الأحكام التنظيمية والتجريبية الواردة في هذه القوانين.

هدف الدراسة

تهدف هذه الدراسة إلى تحليل مجموعة من القواعد القانونية الواردة في قانوني الأمن السيبراني والجرائم الإلكترونية في المملكة الأردنية الهاشمية، من أجل تسليط الضوء على مواطن الخلل والقصور والتداخل في تلك القواعد. يأتي هذا التحليل في ظل التطور السريع للتكنولوجيا، الذي أدى إلى ظهور مفاهيم جديدة مرتبطة بها، بينما في الوقت نفسه تطورت الأساليب والأدوات المستخدمة في ارتكاب الجرائم داخل البيئة الرقمية. لذلك، تسعى هذه الدراسة إلى تقديم تحليل دقيق لماهية الجرائم التي تستهدف الشبكات وأنظمة وتقنيات المعلومات، وتمييزها عن غيرها من الجرائم المرتكبة بالفضاء الرقمي، بما يساهم في فهم أفضل للتحديات التشريعية التجريبية والتنظيمية.

مشكلة الدراسة

تتمثل مشكلة الدراسة في وجود فجوات تشريعية تتعلق بأحكام الأمن السيبراني والجرائم المرتبطة به في المملكة الأردنية الهاشمية. إن هذه الفجوات قد تؤدي إلى زيادة المخاطر الأمنية، مثل الاختراقات الأمنية للشبكات والبيانات، وارتفاع معدلات الجرائم المرتكبة بالفضاء الرقمي. ومن هنا، تتمحور المشكلة الأساسية للدراسة حول الإجابة عن السؤال الرئيس التالي: ما هي الثغرات التشريعية التي تعيق تطوير الأمن السيبراني في الأردن؟ وتنبثق عن هذا السؤال الرئيس عدة تساؤلات فرعية، وهي: ما الفرق بين الجريمة السيبرانية والجريمة الإلكترونية؟ هل ثمة ضرورة تشريعية للتفريق بين الجرائم الواقعة على الشبكات وأنظمة المعلومات عن غيرها من الجرائم المرتكبة في البيئة الرقمية.

أهمية الدراسة

تتمثل أهمية هذه الدراسة في تسليط الضوء على الدور الحيوي للجانب القانوني في تطوير المنظومة الأمنية السيبرانية في الأردن. فعلى الرغم من أن الأردن يُعد من الدول الرائدة في تعزيز تدابير الأمن السيبراني من الناحيتين

التقنية والفنية، خاصة من خلال وضع استراتيجيات متقدمة مقترنة بمدد زمنية محددة¹، إلا أن الثغرات القانونية لا تزال تشكل عائقاً أمام تطوير منظومة الأمن السيبراني بشكل متكامل. لذا تكمن أهمية الدراسة في بيان أثر تداخل الجرائم المرتكبة بالفضاء السيبراني على تطوير منظومة الأمن السيبراني؛ من خلال البحث في مواطن وأسباب هذه التدخلات وتحليلها بشكل منهجي، مما يسهم في إثباتها كمشكلة قانونية قائمة ثم اقتراح حلول وتوصيات لتصحيح هذه الثغرات لتلائم الواقع السيبراني المعاصر.

منهجية الدراسة

اعتمدت الدراسة على المنهج التحليلي والنقدي المقارن بهدف تحليل مفاهيم الأمن السيبراني والجرائم السيبرانية والجرائم الإلكترونية، ودراسة التكيف القانوني لهذه المفاهيم في التشريعات الأردنية مقارنةً بالتشريعات الدولية والإقليمية. وقد وقع الاختيار على قوانين الاتحاد الأوروبي لما فيها من تطور عالمي في مجال الأمن السيبراني، بالإضافة إلى التشريعات العربية كالقانون السعودي والقانون القطري، نظراً لارتباط هذه الدول بالاتفاقية العربية لمكافحة جرائم أنظمة المعلومات. إن الاعتماد على هذا المنهج ساهم في توضيح الفروق بين الجرائم السيبرانية والإلكترونية، واستكشاف أوجه التداخل والتفريق بينهما، إلى جانب تحديد مواطن القصور في التشريعات الوطنية. من خلال ذلك، تسعى الدراسة إلى تقديم توصيات مستندة إلى أفضل الممارسات الدولية والإقليمية لتحسين المنظومة القانونية الأردنية، بما يعزز قدرتها على مواجهة التحديات السيبرانية المستقبلية.

خطة الدراسة

تهدف الدراسة إلى تحليل التكيف القانوني للأمن السيبراني في النظام القانوني الأردني واستكشاف التداخل في الجرائم المرتكبة في الفضاء السيبراني. لتحقيق هذا الهدف. تنقسم الدراسة إلى مبحثين رئيسيين: أولهما يتناول التكيف القانوني للأمن السيبراني في النظام القانوني الأردني. أما الثاني فيتناول مسألة التداخل في الجرائم المرتكبة بالفضاء السيبراني.

المبحث الأول: التكيف القانوني للأمن السيبراني في النظام القانوني الأردني

إن الأمن السيبراني، كمفهوم حديث، نشأ نتيجةً للتطور التكنولوجي السريع وزيادة الاعتماد على الأنظمة المعلوماتية والشبكات في مختلف المجالات. فقد أتاح الاتصال الواسع بهذه الأنظمة والشبكات للمجتمع العالمي إمكانية التواصل من خلال المنتجات الرقمية المرتبطة بها. ومع ذلك، تحتوي هذه الشبكات والأنظمة على نقاط ضعف يمكن استغلالها، مما يزيد من فرص الوصول غير المرغوب فيه من قبل المجرمين. لذا، أصبحت الهجمات السيبرانية على الشبكات والأنظمة والمنتجات المرتبطة من أبرز سمات جرائم العصر². وبالتالي، أصبح الأمن السيبراني محور اهتمام الحكومات والمؤسسات والأفراد في جميع أنحاء العالم.

1 وزارة الاتصالات وتكنولوجيا المعلومات، الإستراتيجية الوطنية للأمن السيبراني (2018-2023)، الأردن، 2018.

2 Gagandeep Singh & Vikrant Sharma. (2021). Cyber-Security and Its Future Challenges. International Journal of Information Security and Cybercrime, 10(1), 38.

إن الأمن السيبراني يتطلب تكييفاً قانونياً خاصاً لمعرفة ماهيته ووسائله إذ يعد التكيف القانوني أمراً بالغ الأهمية؛ لضمان وجود إطار قانوني وتنظيمي متين يمكن من خلاله تنظيم وتعزيز الأمن السيبراني. فالأردن، مثل العديد من الدول، أدركت أهمية الأمن السيبراني وأخذت خطوات ملموسة لتعزيز هذا المجال من خلال سن تشريعات خاصة. فعلى سبيل المثال، تم إعداد قوانين تهدف إلى تنظيم الفضاء السيبراني وتوفير التدابير اللازمة لتعزيز الأمن السيبراني³. إضافة إلى وضع قواعد قانونية خاصة لملاحقة مرتكبي الجرائم السيبرانية⁴. بالإضافة إلى توضيح بعض أوجه القصور التشريعي في الأحكام الواردة في هذا القانون، وعليه سنتعرض أولاً لماهية الأمن السيبراني لنبين لاحقاً في الطبيعة التنظيمية لأحكام قانون الأمن السيبراني

المطلب الأول: ماهية الأمن السيبراني

للهولة الأولى، قد يكون غريباً سماع مصطلح الأمن السيبراني، إذ أن الأمن يعني الحماية والشعور بالطمأنينة ومفهوم سيبراني مرادف لكل ما هو الكتروني⁵. في الأردن، اعتقد الكثيرون أن الأمن السيبراني هو ذاته الأمن الإلكتروني وأن الجريمة السيبرانية هي ذاتها الجريمة الإلكترونية. يعود هذا الاعتقاد إلى كون مفهوم الأمن السيبراني لم يكن رائجاً بالأردن قبل سن قانون الأمن السيبراني في عام 2019⁶، حيث كان هناك قانون الجرائم الإلكترونية رقم 27 لعام 2015⁷. وهو ما أثار اللغط بين المفهومين.

إن كلمة «سيبراني» مشتقة من الكلمة الإنجليزية «Cyber»؛ حيث قيل إن أصل هذه الكلمة يعود إلى المصطلح اليوناني (kybernetike) «κυβερνητική»، الذي يعني «فن القيادة» أو «التحكم»⁸، حيث يعتبر العالم نوربرت وينر هو أول من استخدم المصطلح عام 1948 عند دراسته لموضوع القيادة والسيطرة في عالم الحيوان، أما في قاموس المورد العربي فعرف السيبراني بـ «علم الضبط»⁹. وعلى صعيد قوانين الدول عرف قانون الأمن السيبراني الأوروبي رقم 2019/881 الأمن السيبراني بأنه الأنشطة اللازمة لحماية أنظمة الشبكات والمعلومات ومستخدمي هذه الأنظمة وغيرهم من الأشخاص المتأثرين بالتهديدات السيبرانية¹⁰. بالمقابل، عرفه قانون أمن المعلومات الفيدرالي

3 قانون الأمن السيبراني الأردني، الأردن، رقم 16 لسنة 2019، منشور بالجريدة الرسمية في العدد 5595 على الصفحة 5143 بتاريخ 16-09-2019 والساري بتاريخ 16-09-2019

4 قانون الجرائم الإلكترونية، الأردن، رقم 17 لسنة 2023، منشور بالجريدة الرسمية في العدد 5874 على الصفحة 3579 بتاريخ 13-08-2023 والساري بتاريخ 12-09-2023

5 إسلام مصطفى، «جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري»، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية)، مج 12، ع 2، 2022 ص 722.

6 قانون الأمن السيبراني، مرجع سابق

7 قانون الجرائم الإلكترونية، الأردن، رقم 27، سنة 2015، منشور بالجريدة الرسمية في العدد 5343 على الصفحة 5631 بتاريخ 01-06-2015 والساري بتاريخ 01-06-2015 الملغى ب قانون الجرائم الإلكترونية 2023 رقم 17 لسنة 2023.

8 Norbert Wiener (1961). Cybernetics: Or Control and Communication in the Animal and the Machine , 2nd revised edn, Hermann & Cie and MIT Press, 116.

9 منير البعلبكي، معجم أعلام المورد، دار العلم للملايين، بيروت 2004، ص 243.

10 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (The European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15.

الأمريكي لعام 2014 بأنه عملية حماية المعلومات عن طريق منع الهجمات وكشفها والرد عليها¹¹. أما على صعيد الفقه فوصف الأمن السيبراني بأنه تقنيات دفاعية أو تدابير أمنية متخذة لاكتشاف الدخلاء المحتملين وإحباطهم¹². أما قانون الأمن السيبراني الأردني فقد عرف الأمن السيبراني بأنه «الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني والقدرة على استعادة عملها واستمراريتها سواء أكان الوصول إليها بدون تصريح أو سوء استخدام أو نتيجة الإخفاق في اتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي إلى ذلك»¹³. يتضح من تعريف المشرع الأردني لمفهوم الأمن السيبراني أنه يبنى على ثلاثة عناصر رئيسية وهي أولاً: الأفعال المادية وتتمثل في الإجراءات المتخذة من قبل الشركات أو الحكومات أو الأفراد. ثانياً: الهدف: وهو حماية الأنظمة والشبكات والبنى التحتية الحرجة¹⁴. ثالثاً: الخطر وهو حادث الأمن السيبراني¹⁵، ويمكن تنفيذها على النحو التالي: -

أولاً: الأفعال المادية وهي الإجراءات التي تتخذها الشركات، أو الحكومات، أو الأفراد للحفاظ على أمن المعلومات والبنى التحتية الرقمية. تشمل هذه الإجراءات مجموعة واسعة من التقنيات، العمليات، والممارسات المصممة لمواجهة التهديدات المحتملة التي يشكلها المتسللون، مجرمو الإنترنت، والجهات الفاعلة الخبيثة. قد تتضمن التهديدات البرامج الضارة، التصيد الاحتيالي، برامج الفدية، انتهاكات البيانات، وغيرها من أشكال الهجمات السيبرانية المتعددة¹⁶.

ثانياً: الهدف وهو حماية أنظمة المعلومات، الشبكات المعلوماتية، أو البنى التحتية الحرجة. فنظام المعلومات هو مجموعة متكاملة من المكونات التي تتعاون لجمع البيانات إلكترونياً، ومعالجتها، وتخزينها، وإنتاج المعلومات لدعم اتخاذ القرارات بصورة إلكترونية¹⁷. مثال ذلك نظام إدارة الموارد البشرية في الشركات. أما شبكات المعلومات فهي بنية تحتية تتألف من مجموعة من الأجهزة المترابطة، مثل الحواسيب، الخوادم أو أنظمة المعلومات التي تتواصل مع بعضها البعض لتبادل البيانات والمعلومات عبر الوسائط الإلكترونية¹⁸. إن الحفاظ على استمرارية هذه الأنظمة والشبكات يعد أمراً أساسياً لضمان استقرار وأمن الأفراد والمجتمع، خاصة إذا كان تشغيلها ضرورياً لضمان أمن الدولة، التي تُعرف بالبنى التحتية الحرجة.

11 Federal Information Security Modernization Act of 2014, 44 USC § 3551 et seq (2014).

12 مصطفى، ص 723.

13 المادة 2 من قانون الأمن السيبراني، مرجع سابق.

14 البنى التحتية الحرجة هي مجموعة الأنظمة والشبكات الإلكترونية والأصول المادية وغير المادية أو الأصول السيبرانية والأنظمة التي يعد تشغيلها المستمر ضرورة لضمان أمن الدولة واقتصادها وسلامة المجتمع، راجع المادة 2 من قانون الأمن السيبراني، مرجع سابق.

15 حادث أمن سيبراني هو 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، راجع المادة 2 من قانون الأمن السيبراني، مرجع سابق.

16 The European Union Agency for Cybersecurity (ENISA), ENISA threat landscape report 2023, visit date 2/9/2024 file:///C:/Users/Dell/Downloads/ENISA%20Threat%20Landscape%202023.pdf.

17 راجع المادة 2 من قانون الأمن السيبراني، مرجع سابق.

18 المادة 2 من قانون الأمن السيبراني، مرجع سابق.

ثالثاً: الخطر وهو حادث الأمن السيبراني حيث عرفه القانون بأنه الفعل أو الهجوم الذي يشكل خطراً على البيانات أو المعلومات أو نظم المعلومات أو الشبكة المعلوماتية أو البنى التحتية المرتبطة بها ويتطلب استجابةً لإيقافه أو للتخفيف من العواقب أو الآثار المترتبة عليه¹⁹. إن تعريف الحادث السيبراني بهذه الصورة يعتريه قصور، إذ أن الحادث السيبراني لا يُشترط أن يكون هجوماً بالضرورة؛ بل يمكن أن يتضمن أي خلل أو تهديد يؤثر على أمن المعلومات أو الأنظمة، سواء كان ناتجاً عن هجوم متعمد أو خطأ غير مقصود. وبالتالي، يشمل الحادث السيبراني كل محاولة غير مشروعة للوصول إلى الأنظمة، سواء من خلال اختراقات، هجمات إلكترونية، أو حتى نتيجة للإخفاق البشري في تطبيق الإجراءات الأمنية المناسبة²⁰.

إن إدراج الخطأ البشري ضمن الحوادث السيبرانية ليس أمراً عشوائياً، بل يعكس إدراكاً عميقاً لأهمية هذا العنصر في مجال الأمن السيبراني. انطلاقاً من هذا الفهم، قامت التشريعات المتقدمة بأخذ الأخطاء البشرية في الحسبان ضمن تعريفاتها للحوادث السيبراني؛ حيث تعترف بأن تلك الأخطاء يمكن أن تشكل تهديدات جدية للأمن المعلوماتي، مما يتطلب استجابة فعالة لحماية الأنظمة. فعلى سبيل المثال، جاء في التوجيه الأوروبي الأول لأمن الشبكات وأنظمة المعلومات (NIS Directive)²¹، تعريف الحادث السيبراني بأنه أي حدث يؤثر سلباً على أمن الشبكة وأنظمة المعلومات. أما التوجيه الأوروبي الثاني (NIS2 Directive)²²، فقد عرفه بأي حدث يهدد توافر أو سلامة أو صحة أو سرية المعلومات المخزنة أو المنقولة أو المعالجة، أو يهدد الخدمات المقدمة عبر الشبكة وأنظمة المعلومات أو التي يمكن الوصول إليها عبرها.

في المقابل، يتضح أن المشرع الأردني، على عكس التشريعات المتقدمة، ضيق نطاق تعريف الحادث السيبراني، مما أدى إلى استثناء العديد من الحالات المرتبطة بالإهمال أو الأخطاء غير المقصودة. فحصر صور الاختراق الواردة في التعريف في السلوكيات المادية، يعني أنه لا انتهاك لتدابير الأمن السيبراني بصورة سلوكيات سلبية مثل الأخطاء البشرية. فرغم أن هذه الحالات قد تشكل تهديداً فعلياً للأنظمة والشبكات والبنى التحتية الحرجة، إلا أنها لا تُدرج ضمن الحوادث السيبرانية وفقاً للتعريف الحالي، مما قد يؤدي إلى إغفال فهم شامل لمخاطر الأمن السيبراني التي تتغير وتتغير من يوم إلى آخر، سيما وأن المجرم السيبراني شخص ذكي ويطور باستمرار تقنيات الانتهاك مثل استخدام برامج الفدية المتطورة والبرمجيات الخبيثة كالفايروسات وأحصنة طروادة وبرامج التجسس وغيرها من البرمجيات التي تعيق أو توقف الشبكات وأنظمة المعلومات²³.

19 المادة 2 من قانون الأمن السيبراني، مرجع سابق.

20 David Opderbeck (2016). Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry, 75 Maryland Law Review, 935.

21 European Parliament and Council of the European Union, Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, (NIS Directive) Official Journal of the European Union, L 194 (2016), 1–30.

22 European Parliament and Council of the European Union, Directive (EU) 2022/2555 of 14 December 2022 on the Security of Network and Information Systems (NIS2 Directive), Official Journal of the European Union L 334/1 (2022) 80–152.

23 Burak Clinar, "A Study on Cyber Threat Intelligence Based on Current Trends and Future Perspectives" in Advances and Challenges in Science and Technology Vol 5 (P B International 2023) 40.

في النهاية، يتبين من تعريف القانون للأمن السيبراني أنه قد أوضح عناصره الرئيسية كما ذكرت سابقاً، لكنه لم يقتصر على تلك العناصر فقط، بل أضاف تفاصيل غير ملائمة حول كيفية اختراق الشبكات أو الأنظمة وصورها. إن ذكر النص القانوني لأساليب اختراق الأنظمة والشبكات أخرج التعريف عن سياقه؛ إذ أن تعريف الشيء لغوياً يعني تقديم وصف مختصر أو شرح موجز لتوضيح معناه، وأما التفصيل فهو التوسع في الشرح وذكر الجزئيات المتعلقة بطرق انتهاك تدابير الأمن السيبراني. فذكر أشكال وحالات اختراق تدابير الأمن السيبراني تدخل في نطاق التوسع والشرح التفصيلي، وهو أمر يفترض أن يرد في موضع آخر من القانون وليس ضمن التعريف ذاته، فالأنظمة القانونية المتطورة، مثل توجيهات الأمن السيبراني الأوروبي وقانون أمن المعلومات الفيدرالي الأمريكي²⁴، قدمت تعريفات مختصرة وواضحة لمفهوم الأمن السيبراني وأجمعت هذه التعريفات على أن الأمن السيبراني كمصطلح قانوني مستحدث، يشمل الإجراءات المتخذة لحماية أنظمة المعلومات، والشبكات، والبرامج، والبيانات من الوصول غير المشروع أو التهديدات المحتملة. أما أساليب وطرق الاختراق، فمحلها نص قانوني منفصل عن التعريف ذاته. بناءً على ما تقدم من بيان ماهية الأمن السيبراني كمصطلح قانوني مستحدث، يتوجب البحث في طبيعة الأحكام القانونية التي تضمنت الأحكام السيبرانية وهو ما سنتناوله فيما يلي.

المطلب الثاني: الطبيعة التنظيمية لأحكام قانون الأمن السيبراني

ركز قانون الأمن السيبراني الأردني بشكل أساسي على الجوانب الإجرائية والتنظيمية، دون التوسع في التفاصيل التقنية أو العقوبات الجنائية. يظهر من ذلك أن أهداف القانون تكمن في وضع إطار تنظيمي يحدد مهام وأدوار المركز الوطني للأمن السيبراني في الأردن، بالإضافة إلى وضع ضوابط لتنظيم عمليات الأمن السيبراني. كما نص القانون على بعض العقوبات الإدارية التي يمكن فرضها في حال مخالفة أحكامه²⁵، مما يشير إلى أن الغرض الرئيسي هو تعزيز الامتثال والتنظيم داخل المؤسسات المعنية بالأمن السيبراني بدلاً من التركيز على العقوبات الصارمة.

يتضح من الأسباب الموجبة لسن القانون أن إرادة المشرع كانت واضحة في جعله قانوناً تنظيمياً وليس تشريعياً بحتاً، فقد أشارت تلك الأسباب إلى أن الهدف الأساسي من القانون هو حماية المملكة من تهديدات حوادث الأمن السيبراني، وتأسيس أمن سيبراني وطني يُدار من قبل مركز مختص لضمان التصدي لهذه التهديدات التي تستهدف أنظمة المعلومات والبنى التحتية، مع تعزيز مستوى الأمن الوطني الشامل للمؤسسات والأفراد. كما يهدف القانون إلى تطوير قدرات الرصد، الإنذار، والاستجابة لحوادث الأمن السيبراني، وتقليل الأضرار الناجمة عنها، بالإضافة إلى خلق بيئة آمنة وجاذبة للاستثمار، مما يساهم في تعزيز الاقتصاد الوطني، خصوصاً في ظل التطور السريع في أنظمة المعلومات والبنى التحتية، وتزايد حجم الخدمات الحكومية الإلكترونية²⁶.

تتسم الأحكام التنظيمية للأمن السيبراني بالمرونة؛ حيث يمكن إصدارها عبر قرارات أو أنظمة أو تعليمات تنظيمية، تبعاً لحاجة الدول لضمان الأمن السيبراني وحماية بنيتها التحتية الرقمية. ولا يشترط أن تصدر هذه الأحكام

24 NIS Directive, NIS2 directive and Federal Information Security Modernization act, op. cit.

25 راجع المادة 37 من قانون الجرائم الإلكترونية، مرجع سابق.

26 الأسباب الموجبة لسن قانون الأمن السيبراني، مجلس الأعيان، تاريخ الزيارة 15 / 8 / 2024 / ar <https://senate.jo/ar>

بموجب قانون، كما هو الحال في قطر؛ حيث صدر القرار الأميري رقم (1) لسنة 2021 بإنشاء الوكالة الوطنية القطرية للأمن السيبراني²⁷، الذي يمثل خطوة تنظيمية مهمة لتعزيز الأمن السيبراني في الدولة من خلال وضع السياسات المناسبة والإشراف على تنفيذها. هذه المرونة التشريعية تمكن الجهات المختصة من الاستجابة السريعة للتحديات السيبرانية المتجددة.

على ضوء إرادة المشرع الأردني، باعتبار الأحكام التنظيمية للأمن السيبراني، فالسؤال الذي ينبغي طرحه: هل كان من الملائم أن يقتصر المشرع على اعتبار قانون الأمن السيبراني قانوناً تنظيمياً فقط، أم أن التجريم كان ينبغي أن يكون جزءاً من أحكام القانون؟ للإجابة على هذا السؤال، يجب أولاً النظر إلى ما إذا كان ذلك ممكناً من منظور قانوني؛ حيث تنقسم القواعد القانونية إلى قواعد موضوعية وقواعد إجرائية. فالقانون الموضوعي هو الذي ينظم الحقوق والواجبات أو القيود التي تُفرض على الأفراد، مثل قانون العقوبات²⁸. أما القانون الإجرائي، فهو الذي ينظم الإجراءات أو الأشكال التي يجب اتباعها لحماية الحقوق أو الامتثال للقيود المفروضة، مثل قانون أصول المحاكمات الجزائية²⁹.

هذه التقسيمات الشائعة للقواعد القانونية معترف بها في القوانين الأردنية. وعند العودة إلى التشريعات الوطنية الأردنية، نجد أنه لا يوجد ما يمنع، من منظور تشريعي، أن يجمع القانون بين القواعد الموضوعية والإجرائية في نص واحد. على سبيل المثال، قانون الجرائم الإلكترونية الأردني هو في جوهره قانون موضوعي، ومع ذلك يحتوي على بعض القواعد الإجرائية، مثل المادة 37 التي تفرض إجراءات معينة يجب على منصات التواصل الاجتماعي اتباعها³⁰. لذا، فإن الدمج بين الجوانب التنظيمية والتجريبية كان ممكناً في قانون الأمن السيبراني، وكان يمكن أن يعزز القانون من خلال إضافة أحكام تتعلق بالتجريم إلى جانب الجوانب التنظيمية والإجرائية.

قد يجادل البعض بأن العديد من الأنظمة القانونية في العالم قد فرّقت بين التجريم والتنظيم في مجال الأمن السيبراني. على سبيل المثال، لم يتضمن قانون الأمن السيبراني الأوروبي رقم 881/2019 أحكاماً موضوعية تجريبية³¹، بل اقتصر على قواعد إجرائية خاصة. في المقابل، فإن التوجيه الأوروبي رقم 40/2013 بشأن الجرائم الواقعة على أنظمة المعلومات هو الذي تناول تجريم الأنشطة التي تشكل اعتداءً على أنظمة المعلومات أو الشبكات³². بالتالي قد يرى متبنو هذه النظرية أن تضمين قانون الأمن السيبراني أحكاماً تجريبية ليس واقعياً وليس له أساس قانوني.

27 القرار الأميري رقم (1) لسنة 2021 بإنشاء الوكالة الوطنية القطرية للأمن السيبراني، الجريدة الرسمية لدولة قطر، العدد (3)، تاريخ الإصدار: 2021/2/7.

28 عمار الحسيني وعبد الرازق جاسم، «تكامل القاعدة الجنائية الإجرائية»، مجلة العلوم القانونية والسياسية، مج 7، ع 1، 2018، ص 3.

29 المرجع نفسه.

30 راجع المادة 37 من قانون الجرائم الإلكترونية، مرجع سابق.

31 op. cit. EU Cybersecurity Act 2019.

32 European Parliament and Council, Directive 2013/40/EU of 12 August 2013 on attacks against information systems [2013] OJ L 218/8.

على الرغم من أن دمج الأحكام السيبرانية الجرمية بالتنظيمية ليس مفضلاً لدى العديد من الأنظمة القانونية، إلا أن له أساساً تشريعياً في القانون الأردني، إذ تُعتبر الاتفاقية العربية لمكافحة جرائم المعلومات اللبنة الأولى لسن قواعد قانونية تحكم أنظمة المعلومات وتجرم الأفعال الواقعة عليها داخل الأردن³³. وقد تضمنت هذه الاتفاقية أحكاماً موضوعية وإجرائية؛ حيث احتوت على فصل خاص بالقواعد التجريبية وآخر بالقواعد الإجرائية. لذا، فإن الأساس التشريعي لقواعد الأمن السيبراني التي تشمل الشبكات وأنظمة المعلومات جاء بناءً على قواعد إجرائية وموضوعية. وعليه، فإن تضمين قانون الأمن السيبراني الأردني لكلا النوعين من القواعد يعد أمراً مشروعاً ويعكس الأساس التشريعي الذي يستند إليه.

أما فيما يتعلق بالتوجيه الأوروبي رقم 40 / 2013 بشأن الجرائم المتعلقة بأنظمة المعلومات وسنه كقانون مستقل ينظم تلك الجرائم³⁴، بدلاً من دمجها في قوانين جرمية أو تنظيمية أخرى، فنجد أن إصدار قانون خاص يعالج الجرائم التي تستهدف الشبكات وأنظمة المعلومات يُعد خياراً مثالياً في حال عدم الرغبة في دمج الأحكام التنظيمية والجرمية المتعلقة بالأمن السيبراني داخل إطار قانون واحد. فالأهمية لا تكمن في كيفية تنظيم الأحكام الجرمية، سواء كانت في قانون مستقل أو ضمن قانون الأمن السيبراني، بل في تخصيص أحكام جرمية منظمة في إطار موحد منعاً لإفلات المجرم السيبراني من الملاحقة.

غياب أحكام جرمية منظمة في إطار موحد للتعامل مع الاعتداءات على شبكات وأنظمة المعلومات في الأردن، سواء كان ذلك من خلال قانون تجريمي مستقل أو ضمن أحكام قانون الأمن السيبراني، قد أسفر عن حدوث التباس في فهم الأحكام الجرمية المتعلقة بانتهاكات الأمن السيبراني. بناءً على ذلك، سيتناول المبحث القادم مسألة التداخل بين الجرائم المرتكبة ضد الشبكات وأنظمة المعلومات والجرائم الإلكترونية، بهدف تسليط الضوء على أهمية فصل الجرائم المتعلقة بالشبكات وأنظمة المعلومات عن غيرها من الجرائم، خصوصاً تلك التي تستهدف الأفراد بوسائل إلكترونية.

المبحث الثاني: التداخل في الجرائم

إن النص القانوني الواضح يمثل الدرع الأول في مواجهة التحديات المرتبطة بالتكنولوجيا؛ حيث يساهم في ملاحقة مرتكبي الجرائم الواقعة بالفضاء السيبراني ويعزز الأمن السيبراني من خلال تقديم إطار قانوني يمكن الجهات التنفيذية والقضائية من القيام بواجبها بفعالية³⁵. وفي هذا السياق، تجدر الإشارة إلى أن مصطلحي «الجرائم الإلكترونية» و«الجرائم السيبرانية» غالباً ما يُستخدمان بالتزامن، ورغم التداخل بينهما إلى حد ما، إلا أنهما يعالجان موضوعين مختلفين تماماً، فكل انتهاك أو اعتداء باستخدام التكنولوجيا الرقمية يُعد جريمة، سواء كان الانتهاك أو الاعتداء موجّهاً ضد الأفراد أو أنظمة المعلومات أو الشبكات، لكن ليست كل جريمة ترتكب بالفضاء الإلكتروني

33 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية، رقم 214، سنة 2010.

34 Directive 2013/40/EU of 12 August 2013, op. cit

35 الفضاء السيبراني هو بيئة تتكون من تفاعل الأشخاص والبيانات والمعلومات ونظام المعلومات والبرامج على الشبكات المعلوماتية وأنظمة الاتصالات والبنى التحتية المرتبطة بها. راجع المادة 2 من قانون الأمن السيبراني، مرجع سابق.

ترتبط بالضرورة بانتهاك للأمن السيبراني وبالتالي لا تعتبر جريمة سيبرانية. لذلك، يتناول هذا المبحث أولاً اختلاف الجريمة الإلكترونية عن الجريمة السيبرانية، ليتناول بعد ذلك مواطن التداخل التشريعي بين الجرائم الإلكترونية والسيبرانية في التشريع الأردني.

المطلب الأول: اختلاف الجريمة الإلكترونية عن الجريمة السيبرانية

بشكل عام يمكن وصف الجريمة من منظور قانوني، بأنها كل فعل أو امتناع عن فعل شيء ينص عليه القانون ويعاقب مرتكبه بعقوبة جنائية³⁶. استنتج هذا الوصف من المبدأ القانوني الذي ينص على أن «لا جريمة ولا عقوبة إلا بنص»³⁷. فقيام الجريمة بشكل عام، يجب توفر ثلاثة أركان رئيسية وهي: الركن الشرعي؛ ويتمثل في وجود نص قانوني يجرم الفعل أو الامتناع عن الفعل. وهذا يعني أن القانون هو المصدر الذي يحدد ما يُعتبر جريمة وما لا يُعتبر كذلك. ثانياً: الركن المادي؛ ويتمثل في السلوك الفعلي للجاني، سواء كان فعلاً إيجابياً (مثل السرقة) أو سلبياً (مثل الامتناع عن تقديم مساعدة لشخص في حالة خطر عندما يكون ذلك ملزماً قانوناً). ثالثاً: الركن المعنوي؛ ويتضمن القصد الجرمي أو النية الإجرامية للجاني، بحيث يجب أن يكون هناك وعي وإرادة لارتكاب الفعل الذي يعتبره القانون جريمة³⁸.

تقليدياً، يمكن أن تحدث الجريمة ضد الأفراد، كما هو الحال في جرائم الإيذاء التي تتضمن الأفعال التي تؤذي صحة أو سلامة الأشخاص. كما يمكن أن تستهدف الجريمة الأموال، كما في حالات السرقة التي تتضمن الاستيلاء على أموال الآخرين بغير حق بنية التملك. ومع التقدم التكنولوجي، أصبحت الجرائم تُمارَس إما ضد البيانات أو أنظمة المعلومات أو الشبكات، أو ضد الأفراد باستخدام وسائل إلكترونية. ومع ظهور هذا النوع من الجرائم، نشأت مفاهيم وأحكام جديدة، تُعرف باسم الجرائم الإلكترونية والجرائم السيبرانية. فما هي هذه الجرائم؟

أولاً: الجرائم الإلكترونية؛ لم يتوصل الفقه إلى تعريف شامل ومانع للجريمة الإلكترونية؛ حيث أطلق بعضهم عليها مسمى جرائم الإنترنت، في حين أشار آخرون إليها كجرائم مرتبطة بالكمبيوتر أو الجرائم المعلوماتية³⁹. عرّف بعض الفقهاء الجريمة الإلكترونية بأنها مجموعة من الأفعال الإجرامية التي تتضمن استخدام الإنترنت أو أجهزة الكمبيوتر أو غيرها من الأجهزة الإلكترونية. وبمعنى أوسع، يمكن اعتبارها نشاطاً إجرامياً يكون فيه الكمبيوتر أو الشبكة هو المصدر أو الوسيلة أو الهدف أو الفضاء المرتبط بالجريمة⁴⁰. فمن جهة أخرى، عرّف جانب آخر من الفقه الجريمة الإلكترونية بأنها المخالفات التي تُرتكب ضد الأفراد أو المجموعات بهدف إيذاء سمعتهم

36 عبد الفتاح حجازي، الجرائم الإلكترونية: دراسة مقارنة، دار الفكر والقانون، المنصورة، ط1، 2008، ص33.

37 المادة 3 من قانون العقوبات وتعديلاته رقم 16 لسنة 1960، الأردن، منشور بالجريدة الرسمية في العدد 1487 على الصفحة 374 بتاريخ 1960/05/01 والساري بتاريخ 1960/06/01.

38 عبد الرحمن محمود، الجرائم والعقوبات، ج1، دار الكتب القانونية، عمان، ط2، 2019، ص45.

39 وفاء لطفي، «الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني»، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، مج23، ع1، 2022، ص154.

40 Iris Bjelica Vlajić, Branko Nikolić, and Nadežda Gudelj (2023). 'Legal Aspects of Fighting Cyber Crime in the European Union', ODITOR, 31.

أو التسبب في أذى مادي أو نفسي، سواء بشكل مباشر أو غير مباشر، من خلال استخدام شبكات الاتصال مثل الإنترنت⁴¹.

تبين مما سبق أن الفقهاء اختلفوا في تعريف الجريمة الإلكترونية؛ حيث وسَّع البعض مفهومها ليشمل أي جريمة تُعتبر إلكترونية سواء كان نظام المعلومات أو الشبكة المعلوماتية محل الجريمة أو الوسيلة المستخدمة لارتكابها. في المقابل، اعتبر آخرون أن الجريمة الإلكترونية هي تلك التي تُرتكب ضد الأفراد باستخدام وسائل إلكترونية، مثل تقنية المعلومات أو أنظمتها أو الشبكات المعلوماتية. ويرى مؤيدو هذا الرأي أنه إذا لم يكن الهدف هو الأشخاص، فإن الجريمة تُصنف ضمن نوع آخر من جرائم المعلومات⁴².

أما بالنسبة للاتفاقيات الدولية المتعلقة بالجرائم الإلكترونية، فقد وقعت اتفاقية بودابست للجرائم الإلكترونية في عام 2001، وتُعتبر أول اتفاقية دولية تهدف إلى مكافحة الجرائم المرتكبة في الفضاء السيبراني⁴³. حيث عرّفت الجريمة الإلكترونية بأنها أي فعل غير قانوني يرتكب عن طريق أو ضد الأنظمة المعلوماتية أو الشبكات. ويشمل ذلك الجرائم التي تُرتكب باستخدام أجهزة الكمبيوتر والإنترنت، مثل الجرائم ضد السرية وسلامة وتوافر البيانات والنظم المعلوماتية، بالإضافة إلى الجرائم المتعلقة بالاحتيال والجرائم الاقتصادية. من جهة أخرى، لم تُعرّف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الجريمة الإلكترونية أو جرائم تقنية المعلومات⁴⁴، لكن أحكام الاتفاقية شملت كل الجرائم المرتكبة ضد أو بواسطة وسائل تقنية المعلومات وهي التقنيات التي تُستعمل لتخزين المعلومات، وترتيبها، وتنظيمها، واسترجاعها، ومعالجتها، وتطويرها، وتبادلها.

تناولت القوانين والتشريعات العربية تعريف الجريمة الإلكترونية بوضوح؛ حيث عرّف المشرع القطري الجريمة الإلكترونية بأنها أي فعل يتم باستخدام تقنية المعلومات أو نظام معلوماتي أو شبكة معلوماتية، بشكل غير قانوني، وبما يخالف أحكام القانون⁴⁵. يتضح من ذلك أن القانون القطري يعتبر الجريمة الإلكترونية بناءً على معيار الوسيلة المستخدمة، بحيث تُصنف الجريمة الإلكترونية إذا استُخدمت تلك الوسائل في ارتكابها، بغض النظر عن موضوع الجريمة، سواء كانت موجهة ضد أشخاص أو أنظمة أو تقنيات إلكترونية.

على خلاف القانون القطري، لم يعرف قانون الجرائم الإلكترونية الأردني الجريمة الإلكترونية بل تركها للقضاء. وعليه، جاء في قرار إحدى المحاكم الأردنية تعريف الجريمة الإلكترونية ووصفها بأنها مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو ثبت عبر محتوياتها أن جهاز الحاسب الآلي هو هدف الجريمة وقد يكون محلها أو أدواتها⁴⁶. يُسهم وجود تعريف واضح للجريمة الإلكترونية في النصوص

41 Debarati Halder and karuppannan Jaishankar (2011), Cyber Crime and the Victimization of Women: Law Rights, and Regulations IGI Global 2011, 17.

42 Ibid, 17

43 Budapest Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) ETS No 185.

44 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مرجع سابق.

45 قانون رقم (14) لسنة 2014 بشأن إصدار قانون مكافحة الجرائم الإلكترونية، دولة قطر، الجريدة الرسمية، ع15، ص7، 2/10/2014.

46 محكمة بداية جزاء عمان بصفتها الاستئنافية، الحكم الجزائي رقم 2021/1050 صدر بتاريخ 2021/5/9.

القانونية في تقليل احتمالات تضارب الأحكام القضائية المتعلقة بتفسير هذا النوع من الجرائم. فالقضاء معني بتطبيق الأحكام القانونية على الوقائع الجرمية، وليس بوضع تعريفات لمفاهيم لم ينص عليها القانون. ومع ذلك، في ظل غياب نصوص قانونية تُحدد ماهية الجرائم الإلكترونية بوضوح، كان لا بد من تدخل القضاء الأردني لتقديم إطار قانوني عام يُحدد ما يندرج تحت مظلة الجرائم الإلكترونية.

يتضح من التعريفات القانونية للجريمة الإلكترونية في الاتفاقيات الدولية واجتهادات المحاكم الأردنية أن معظمها جاء موسعاً؛ حيث اعتُبرت الجريمة الإلكترونية قائمةً في حال كان محل الجريمة أو وسيلتها إلكترونيًا. فالوسيلة قد تكون الأنظمة والشبكات أو تقنيات المعلومات، أما المحل فقد يكون الأفراد أو الأنظمة أو الشبكات. إلا أن الباحث يرى أن هذا التوسع في التعريف قد يكون مبرراً في وقت سابق، عند توقيع اتفاقية بودابست للجرائم الإلكترونية في عام 2001⁴⁷، أو عند توقيع الاتفاقية العربية لمكافحة جرائم أنظمة المعلومات في عام 2010⁴⁸، أي عندما كانت الجرائم المرتكبة في الفضاء السيبراني محدودةً أو ضيقةً إلى حد ما. لكن في الوقت الذي أصبحت فيه الجرائم المرتكبة في الفضاء السيبراني هي الطابع الغالب في هذا العصر، أصبح من الضروري التفريق بين الجرائم الإلكترونية وغيرها من الجرائم، بحيث يتم تمييزها وتضييق نطاقها وحصرها في الجرائم التي تقع على الأفراد بواسطة الوسائل الإلكترونية. لذا، يمكن تعريف الجريمة الإلكترونية بأنها الجريمة التي تُرتكب بواسطة نظام معلومات أو شبكة معلوماتية أو أي وسيلة تقنية أخرى ضد أشخاص طبيعيين أو معنويين.

ثانيًا: الجرائم السيبرانية، كحال الجرائم الإلكترونية، تُعتبر الجرائم السيبرانية من الظواهر القانونية الحديثة التي لا تزال تفتقر إلى تعريف موحد في الفقه القانوني. تعود هذه الصعوبة إلى عدم التفريق بينها وبين الجرائم الإلكترونية من حيث التسمية والنطاق الذي تشملانه. حيث اعتبر العديد من الفقهاء والتشريعات الجرائم السيبرانية متماثلةً مع الجرائم الإلكترونية، رغم اختلاف المسميات. فعلى سبيل المثال، عرّف التشريع السعودي الجرائم السيبرانية في نظام مكافحة جرائم المعلومات بأنها أي فعل يُرتكب باستخدام الحاسب الآلي أو الشبكة المعلوماتية بما يتعارض مع أحكام هذا النظام⁴⁹.

بالمقابل، عرف الفقيه غازي الرشيد الجريمة السيبرانية بأنها الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها أو يمثل إغراءً بذلك أو جريمة يكون الحاسب الآلي نفسه ضحيتها⁵⁰. من جهة أخرى، جدير بالذكر أن مصطلح (سيبراني) هو مصطلح غير عربي، بل هو ترجمة لكلمة (Cyber) من اللغة الإنجليزية. لذا، توجد ترجمتان للمصطلح في الأنظمة القانونية العربية؛ الأولى هي: (إلكتروني) والثانية: (سيبراني). ونتيجة لذلك، يستخدم وصف (Cybercrimes) للإشارة إلى كل من الجرائم السيبرانية والجرائم الإلكترونية، مما أدى إلى حدوث خلط بين المفهومين.

47 Budapest Convention on Cybercrime 2011, op. Cit.

48 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مرجع سابق

49 نظام مكافحة جرائم المعلوماتية، السعودية، الصادر بالمرسوم الملكي رقم م/ 17 تاريخ 8 ربيع الأول 1428هـ.

50 غازي الرشيد، الحماية القانونية من جرائم المعلوماتية (الحاسب والإنترنت)، [أطروحة دكتوراه]، الجامعة الإسلامية في لبنان، لبنان، 2004، ص 108.

أما على صعيد القانون الأردني، فلم يرد مصطلح الجريمة السيبرانية بالقوانين الأردنية بل تم سن قانون جرائم أنظمة المعلومات المؤقت لسنة 2010⁵¹، حيث هدف إلى تجريم الأفعال الواقعة على أنظمة المعلومات والشبكات، إذ جاء فور التوقيع على الاتفاقية العربية لمكافحة جرائم المعلومات. للوهلة الأولى يتبادر إلى الذهن أن قانون جرائم أنظمة المعلومات قد جرم الأفعال الواقعة على أنظمة المعلومات والشبكات المعلوماتية فقط على غرار ما ورد في التوجيه الأوروبي رقم 40/2013 بشأن الجرائم المتعلقة بأنظمة المعلومات⁵²، إلا أنه تضمن الجرائم الواقعة على أنظمة المعلومات أو الشبكات إضافة إلى الجرائم الواقعة على الأشخاص باستخدام الأنظمة أو الشبكات، مما سبب تضارباً بين تسمية القانون ومضمونه.

أما في مجال الفقه، فيرى بعض الفقهاء أن الجريمة السيبرانية تُستخدم للتعبير عن الجرائم التي تُرتكب بواسطة أو ضد أنظمة المعلومات والشبكات؛ حيث عرّفوها بأنها الهجوم عبر الفضاء الإلكتروني بهدف السيطرة على مواقع إلكترونية أو بنى تحتية حساسة محمية بأنظمة إلكترونية لتعطيلها، أو تدميرها، أو الإضرار بها⁵³. بالرغم من أن تعريف الفقه الأخير للجريمة السيبرانية قد اقتصر على الجرائم الواقعة على الشبكات وأنظمة المعلومات، إلا أن الهدف من الهجوم الإلكتروني ليس بالضرورة أن يكون عبر السيطرة على الأنظمة والشبكات، فمجرد إعاقة هذه الأنظمة كافٍ لاعتبار الجريمة إلكترونية.

وعليه، يرى الباحث أن الجريمة السيبرانية تتمثل في الاعتداء على الشبكات وأنظمة المعلومات، بصرف النظر عن الوسيلة التي تُرتكب بها الجريمة. فيمكن أن تقع بواسطة سلوك إيجابي يتمثل في اختراقها باستخدام وسيلة إلكترونية، كما يمكن أن تقع عن طريق سلوك سلبي يتمثل في الإهمال أو الترك، مثل عدم اتخاذ التدابير الأمنية الواجبة. لذا، وإن كانت الجريمة السيبرانية تتشابه أحياناً مع الجريمة الإلكترونية من حيث وسيلة ارتكاب الجرم في حال اتخاذ سلوك إيجابي، إلا أنها لا تتداخل معها في حال ارتكاب الجريمة السيبرانية عن طريق الإهمال أو الترك. إن هذا التفريق بين صور الجريمة يعود إلى مبررات موضوعية تكّرس أهمية فصل الجريمة السيبرانية عن الجريمة الإلكترونية.

إن اختلاف الجريمة الإلكترونية والجريمة السيبرانية من حيث المفهوم يربط أثراً مهماً يتمثل في إعادة تكييف النظام القانوني الذي ينظم كل نوع من هذه الجرائم بشكل منفصل. فتصنيف الجريمة السيبرانية باعتبارها الجريمة التي تستهدف الشبكات وأنظمة المعلومات فقط لا يستدعي فقط فصلها عن الجرائم الإلكترونية، بل يقتضي أيضاً إنشاء جهات مختصة تتولى متابعة وملاحقة كل نوع من هذه الجرائم بصورة مستقلة. ومع ذلك، ينبغي التحقق من وجود أسباب كافية تستدعي إجراء هذا التصنيف الجديد، إذ أن اختلاف المفهوم وحده لا يكفي لتبرير إنشاء نظام قانوني مستقل لكل نوع، خاصة أن البيئة الرقمية تشكل العامل المشترك بين جميع هذه الجرائم، وعليه يمكن البحث

51 قانون جرائم أنظمة المعلومات المؤقت، الأردن، رقم 30، سنة 2010، منشور بالجريدة الرسمية في العدد 5056 على الصفحة 5334 بتاريخ 2010-09-16 والساري بتاريخ 2010-10-16.

52 Directive 2013/40/EU of 12 August 2013, op. cit.

53 عبد العزيز الغامدي، جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية 1428 هـ دراسة مقارنة، دار الكتاب الجامعي للطباعة والنشر والتوزيع، السعودية، 2017 ص 32.

بالمبررات والأسباب على النحو التالي.

أولاً: ارتباط الجريمة السيبرانية بالأمن السيبراني من جانب تشريعي

لم يكن مصطلح سيبراني شائعاً في التشريعات الوطنية الأردنية قبل سن قانون الأمن السيبراني رقم 16 لعام 2019، إلا أنه قد ورد ذلك المصطلح في تعليمات التكيف مع المخاطر السيبرانية لسنة 2018⁵⁴. الصادرة بموجب قانون المعاملات الإلكترونية الأردني⁵⁵. مع صدور قانون الأمن السيبراني، تبين أن الهدف منه هو تنظيم التدابير التي تعزز الأمن السيبراني، وليس تجريم الأفعال التي تمثل انتهاكاً لهذه التدابير. لذلك، من الضروري البحث في التشريعات التي تناولت الجرائم التي تنطوي على انتهاكات لتلك التدابير. وبالعودة إلى التشريعات الأردنية، يتضح أن الجرائم التي تستهدف الشبكات وأنظمة المعلومات والتقنيات المعلوماتية جرى تجريمها بموجب أحكام قانون الجرائم الإلكترونية.

إن تجريم الاعتداءات الواقعة على الأنظمة والشبكات بموجب قانون الجرائم الإلكترونية لم يكن تحت مسمى الجريمة الإلكترونية قبل سن قانون الجرائم الإلكترونية لعام 2015⁵⁶؛ بل كانت تلك الأفعال الجرمية تنظم تحت قانون سمي بقانون جرائم أنظمة المعلومات؛ حيث سن القانون الأخير تنفيذاً لأحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، إذ اشتملت أحكام القانون المذكور على العديد من الجرائم الواقعة على شبكات وأنظمة المعلومات مثل جريمة الدخول غير المشروع إلى نظام معلومات أو شبكة معلوماتية وجريمة تعطيل شبكة معلوماتية أو نظام معلومات وغيرها من الجرائم السيبرانية.

في عام 2015 أدرك المشرع الأردني أن هناك تطوراً سريعاً في مجال تقنية المعلومات لذا اتجه إلى توسيع الجرائم المرتكبة بواسطة أو ضد أنظمة المعلومات عن طريق تعديل تسمية قانون جرائم أنظمة المعلومات إلى قانون الجرائم الإلكترونية؛ حيث أضيفت أحكام قانونية جديدة تهدف إلى توفير حماية أكبر للحقوق والحريات العامة والخاصة من الاعتداء عليها كالابتزاز والاحتيال الإلكتروني وحماية أنظمة المعلومات والشبكات المعلوماتية والأصول المادية وغير المادية أو الأصول السيبرانية⁵⁷. على الرغم أنه كان من الأفضل إعادة ترتيب أحكام القانون عند تعديله بفصل الجرائم السيبرانية عن الجرائم الإلكترونية، إلا أن المشرع كان موفقاً في توسيع نطاق أحكام الجرائم التي تستهدف أنظمة المعلومات. بالإضافة إلى ذلك، جاء تغيير اسم القانون ليصبح أكثر شمولية، بحيث لا يقتصر على الجرائم المرتكبة بواسطة أو ضد أنظمة المعلومات فقط، بل يشمل جميع الجرائم التي تُرتكب باستخدام أي وسيلة إلكترونية، سواء كان الهدف منها نظام معلومات، أو شبكة معلوماتية، أو أشخاصاً طبيعيين أو معنويين.

بالمقابل، عند صدور قانون الأمن السيبراني في عام 2019، نصّ القانون على أن ما يتعلق بالأمن السيبراني

54 تعليمات التكيف مع المخاطر السيبرانية، البنك المركزي الأردني، الأردن، 2018.

55 قانون المعاملات الإلكترونية، الأردن، رقم 30، سنة 2015، منشور في العدد 5341 على الصفحة 5292 بتاريخ 2015/05/17 والساري بتاريخ 2015/05/17.

56 قانون الجرائم الإلكترونية لعام 2015، مرجع سابق.

57 حكومة المملكة الأردنية الهاشمية، الأسباب الموجبة لمشروع قانون الجرائم الإلكترونية الأردني، الأردن، 2015، منشورات مركز قسطاس.

يشمل أنظمة المعلومات والشبكات والبنى التحتية الحرجة، دون أن يتطرق إلى أي حكم يتعلق بالاعتداءات أو الجرائم المرتكبة على الأفراد عبر الفضاء السيبراني. إن إصدار قانون الأمن السيبراني بهدف تحديد الأفعال التي تعد اعتداءات على الشبكات أو أنظمة المعلومات يفيد أن المشرع ارتأى تمييز هذا النوع من الاعتداءات عن غيره، إذ لو لم يكن يرغب في وضع أحكام خاصة لهذا النوع من الاعتداءات لما أفرد لها تشريعاً مستقلاً؛ بل لأدخل أحكامها ضمن قانون الجرائم الإلكترونية أو قانون حماية البيانات أو غيرها من القوانين ذات العلاقة. وبالتالي، فبمجرد سن قانون الأمن السيبراني الأردني لم يعد هناك مبرر لدمج الجرائم التي تتعلق بالاعتداءات على الشبكات وأنظمة المعلومات ضمن مظلة قانون الجرائم الإلكترونية.

ثانياً: الفرق في الوسيلة والمحل بين الجريمة الإلكترونية والجريمة السيبرانية

تعتبر الوسيلة أداة مادية أو معنوية تُستخدم لتنفيذ الجريمة أو تحقيق الهدف الإجرامي، إذ أن الأصل في القانون الجنائي أن الوسيلة التي يتم بها ارتكاب الجرم ليست ذات أثر في بنيانه القانوني ما لم يتدخل المشرع صراحةً ويجعل منها محل اعتبار في الركن المادي للجرم. فعلى صعيد قانون العقوبات الأردني تدخل المشرع استثناءً واعتبر الوسيلة ركناً لقيام جرم الاحتيال الوارد في المادة 417 فعدم توفر إحدى وسائل الاحتيال المذكورة ينفي قيام الركن المادي للجرم، بالمقابل اعتبر المشرع الوسيلة ظرفاً مشدداً بجرائم أخرى كارتكاب جريمة السرقة بواسطة الكسر والخلع كما ورد بالمادة 404 من ذات القانون. على صعيد آخر، لم يرتب القانون أي أثر للوسيلة كأداة لارتكاب الجريمة كما هو الحال في جرم خرق حرمة الحياة الخاصة الوارد في المادة 348 مكرر من قانون العقوبات⁵⁸.

إن قانون الجرائم الإلكترونية ببعض أحكامه اعتبر الوسيلة ظرفاً مشدداً لأوصاف جرمية موجودة مسبقاً كجرائم الذم والقدح والتحقير المرتكبة بوسائل إلكترونية أو جاء ليضيف وسيلة جديدة لارتكاب جرائم معينة لم تكن القواعد التقليدية تستوعبها حتى أنه اعتبر الوسيلة بهذه الجرائم ركناً لقيامها كجرم الدخول غير المصرح به إلى الأنظمة أو الشبكات⁵⁹. وجرم اختراق الأنظمة أو الشبكات بهدف تعطيلها بواسطة برنامج أو أمر برمجي⁶⁰.

إن الوسيلة المستخدمة في الجريمة السيبرانية والتي تستهدف أنظمة المعلومات والشبكات ليست بالضرورة دائماً إلكترونية حيث إن الجريمة السيبرانية ممكن أن تقع عن طريق الإهمال أو الترك كما سبق بيانه، على خلاف الجريمة الإلكترونية. فالركن المادي في الجريمة السيبرانية قد يتمثل في سلوك إيجابي باستخدام وسيلة إلكترونية كالدخول غير المصرح به للشبكات لتعطيلها. بالمقابل قد يقع الركن المادي في صورة سلوك سلبي يتمثل في الفشل في اتخاذ الإجراءات المناسبة أو الامتناع عن اتخاذ التدابير الواجب اتباعها في السياق الرقمي. فإهمال حماية البيانات الشخصية، والامتناع عن واجبات معينة تتعلق بالحفاظ على الخصوصية أو منع الأنشطة غير القانونية عبر الإنترنت أو عدم اتخاذ الإجراءات الأمنية الواجبة الاتباع يندرج تحت مفهوم الجريمة السيبرانية حيث يمكن أن تقع هذه الجرائم دون استخدام وسيلة إلكترونية؛ على خلاف الجريمة الإلكترونية التي لا ترتكب كأصل عام إلا بسلوك

58 راجع المواد 417 و404 و348 مكرر من قانون العقوبات، مرجع سابق.

59 راجع المواد 3 و4 من قانون الجرائم الإلكترونية لسنة 2023، مرجع سابق.

60 راجع المادة 6 من قانون الجرائم الإلكترونية لسنة 2023، مرجع سابق.

إيجابي، والاستثناء أن ترتكب في صورة سلوك سلبي كالحالة التي وردت في المادة 33/ب من قانون الجرائم الإلكترونية التي يتصور فيها أن تقع الجريمة الإلكترونية في صورة سلوك سلبي يتمثل في امتناع أو رفض القائمين على نظام المعلومات أو منصة التواصل الاجتماعي أو الموقع الإلكتروني أو مزود الخدمة لأوامر المحكمة أو الجهات المختصة⁶¹.

أما فيما يتعلق بمحل الجريمة فهو موضوع الجريمة أو الحق المعتدى عليه الذي تستهدفه الجريمة⁶². أي أنه العنصر أو الشيء الذي تركز عليه الجريمة، سواء كان متعلقاً بشخص أو مال أو حق معنوي أو أجهزة أو شبكات أو تقنيات إلكترونية. وهنا يتبين أن محل الجريمة الإلكترونية يختلف عن محل الجريمة السيبرانية، فمحل الجريمة الإلكترونية هو الشخص أو ماله أو اعتباره أما محل الجريمة السيبرانية فهو أنظمة المعلومات أو الشبكات على النحو الذي عرفه القانون.

أكد التطبيق القضائي الأردني وجود فرق بين الجريمة السيبرانية والإلكترونية؛ حيث قضت محكمة بداية عمان بصفقتها الاستثنائية في أحد قراراتها أن هناك فارقاً بين الجريمة التي ترتكب بوسيلة إلكترونية وبين الجريمة التي يكون محلها إلكترونياً أو أجهزة وأنظمة الحاسوب والإنترنت، فمن المؤكد أن كليهما له مفهوم وكيان ووسيلة إثبات تختلف عن الأخرى⁶³، إن ما توصلت إليه المحكمة يناقض ما عرفه القضاء في الكثير من أحكامه التي خلطت بين الوسيلة والمحل كمعيارين يتطلب توفر أحدهما لاعتبار الجريمة إلكترونية إذ عرفت محكمة صلح جزاء عمان في قراراتها ذات الأرقام 16707/2023 و 688/2022 الجريمة الإلكترونية بأنها الجريمة التي يكون نظام المعلومات، الحاسب الآلي، أو الشبكة المعلوماتية، محلها، أو وسيلة ارتكابها⁶⁴.

أما على الصعيد الدولي، فقد تبني مؤتمر الأمم المتحدة الثالث لمنع الجريمة والعدالة الجنائية تقسيماً للجرائم المرتكبة في الفضاء السيبراني، بحيث تضم الفئات التالية أولاً: الأفعال التي تكون فيها البيانات أو النظم الحاسوبية هي الشيء المستهدف بالجرم، ومنها ما يرتكب من جرائم بحق سرية البيانات أو النظم الحاسوبية وسلامتها وتوافرها، مثل أفعال الاقتحام غير المشروع للبيانات والحاسوبية. ثانياً: الأفعال التي تشكل فيها النظم أو المعلومات الحاسوبية جزءاً أساسياً من وسائل لارتكاب هذه الجرائم، ومنها استخدام البيانات أو النظم الحاسوبية لأغراض الاحتيال أو السرقة أو إلحاق الأذى بالآخرين⁶⁵. بناءً على هذا التوجه الدولي بادر العديد من الفقهاء إلى تصنيف الجرائم الإلكترونية إلى فئتين رئيسيتين؛ الأولى: جرائم القرصنة التي تكون أنظمة المعلومات أو الشبكات فيها هدفاً للنشاط الإجرامي، وفئة جرائم الإنترنت التي يكون فيها استخدام الأنظمة أو الشبكات أداة فقط حتى يمكن تنفيذ النشاط الإجرامي، وهي الحالة التي يكون فيها استخدام الأنظمة بالحاسب الآلي عرضياً لارتكاب الجريمة⁶⁶.

61 راجع المادة 33/ب من قانون الجرائم الإلكترونية لسنة 2023، مرجع سابق

62 أحمد فتحي سرور، القانون الجنائي: المبادئ العامة للجريمة، مج 1، دار النهضة العربية، القاهرة، ط 3، 2006، ص 142.

63 محكمة بداية جزاء عمان بصفقتها الاستثنائية، الحكم الجزائي رقم 1200/2024، 2024.

64 محكمة صلح جزاء عمان، الحكم الجزائي رقم 16707/2023، 2023؛ محكمة صلح جزاء عمان، الحكم الجزائي رقم، 688/2022، 2023.

65 الأمم المتحدة، تقرير مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، قطر نيسان 2015، ص 8.

66 Raghavan and Latha Parthiban (2014). L. The growing case of cybercrime & types of cybercrime on global scale. A

إن التفريق بين الجرائم بناءً على طبيعة الحق المعتدى عليه هو مبدأ سارت عليه أغلب التشريعات الجزائية الحديثة، إذ تم تنظيم الجرائم المتشابهة بناءً على هذا المعيار، فمثلاً نظم المشرع الأردني في قانون العقوبات الجرائم ضمن فصول ووضعها تحت عناوين مستقلة تحت بنود جرائم واقعة على الأشخاص وجرائم واقعة على الأموال، فتصنيف الجرائم يتم على أسس علمية استناداً إلى العناصر التي يجمعها بها إطار التشابه الحاصل بينها؛ بأخذ معيار خصوصية الحق المعتدى عليه بعين الاعتبار.

فمن هذا المنطلق، يمكن القول إن لتصنيف الجرائم الإلكترونية بناءً على معيار محل الجريمة أهمية عملية وعلمية، فمن الناحية العملية، سيساهم التفريق بين الجريمة السيبرانية والإلكترونية في تعزيز دور مأمور الضبط العدلي في تقصي وتبعية الجرائم بناءً على محل الجريمة. كذلك الحال بالنسبة للاختصاص القضائي؛ حيث يمكن تخصيص غرف قضائية متخصصة تعنى بالجرائم الواقعة على الأنظمة والشبكات وتقنيات المعلومات، وغرف أخرى متخصصة بالجرائم الواقعة على الأشخاص التي تُرتكب بالوسائل الإلكترونية. أما من الناحية العلمية، فإن تصنيف الجرائم يمكن الفقه الجنائي من إجراء البحوث والشروحات والتفسيرات لمجموعة أو فئة معينة من الجرائم الإلكترونية أو السيبرانية، باعتبارهما مجموعتين ترتبطان بأحكام عامة معينة ولكنهما يختلفان في أركانها الخاصة⁶⁷.

ثالثاً: تطور وتعقيد الجرائم السيبرانية

إن التهديدات السيبرانية أصبحت مصدر قلق لكافة الدول بما فيها الأردن؛ حيث تضاعفت وتنوعت أشكال الهجمات السيبرانية فبحسب المركز الوطني للأمن السيبراني تم التعامل مع 1362 حادث أمن سيبراني على مستوى المملكة في عام 2022 في حين تم التعامل مع 2455 حادث أمن سيبراني في عام 2023⁶⁸. من جانب آخر، تتوقع شركات إحصاء البيانات أن تصل قيمة سوق الأمن السيبراني حول العالم إلى 538.3 مليار دولار بحلول عام 2030⁶⁹. كما يتوقع أن ترتفع التكلفة العالمية للجرائم الإلكترونية إلى 23.84 تريليون دولار بحلول عام 2027. ارتفاعاً من 8.44 تريليون دولار في عام 2022، وفقاً لتقديرات شركة Statista⁷⁰، فإن هذه النسب المتوقعة لزيادة كلفة الجرائم الإلكترونية بما فيها الهجمات السيبرانية لم تأت من فراغ فعام 2023 شهد زيادة في الانتهاكات الأمنية السيبرانية بنسبة 72 بالمائة مقارنة بعام 2021، الذي حمل الرقم القياسي السابق على الإطلاق⁷¹.

Journal of Computer Science Engineering and Information Technology Research, 4(2), 2.

67 محمد بدوسي، «تصنيف الجرائم الإلكترونية وفقاً لطبيعة الحق المعتدى عليه: دراسة مقارنة بين التشريع الفلسطيني والإماراتي»، مجلة جامعة العين للأعمال والقانون، ع1، 2023، ص129.

68 المركز الوطني للأمن السيبراني، التقرير السنوي لعام 2023، الأردن، 2023، آخر زيارة 20/9/2024. <https://ncsc.jo/Ar/List/> ReportPublic

69 Demandsage company, Shocking Cybersecurity Statistics for 2024, visit date 20/9/2024. <https://www.demandsage.com/cybersecurity-statistics/>.

70 World Economic forum, 2023 was a big year for cybercrime – here's how we can make our systems safer, visit date 20/9/2024 <https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety>.

71 Varonis, 157 Cybersecurity Statistics and Trends [updated 2024], visit date 20/9/2024 <https://www.varonis.com/blog/cybersecurity-statistics>.

إن الزيادة المطردة في أعداد الهجمات السيبرانية يستدعي بالضرورة تطوير المنظومة التشريعية التي يجب أن تواكب التطورات السريعة في مجال التكنولوجيا، وخاصة في مجال الأمن السيبراني. وعليه إن التطوير المنشود يمكن أن يتم على المستويين التقني والقانوني. ففي الجانب التقني يجب أن تتطور آليات تدابير الأمن السيبراني حتى تصبح أكثر ذكاءً ومرونةً وقدرةً على التكيف مع التهديدات المتجددة والمتزايدة. فعلى سبيل المثال، استخدام تقنيات الذكاء الاصطناعي يمكن أن يلعب دورًا حاسمًا في تعزيز استراتيجيات الكشف عن الهجمات السيبرانية والوقاية منها. بفضل قدرته على التعلم والتحليل الذكي للبيانات الكبيرة، يمكن للذكاء الاصطناعي التنبؤ بسلوكيات غير طبيعية في الشبكات، وتحديد الهجمات السيبرانية المحتملة حتى قبل وقوعها. إضافةً إلى ذلك، يمكنه تعزيز سرعة ودقة الاستجابة لهذه التهديدات⁷².

أما في الجانب القانوني، فيجب أن تكون التشريعات مرنةً وقابلةً للتكيف مع الابتكارات التقنية الحديثة، مثل الذكاء الاصطناعي. فالأحكام التي تنظم آليات اكتشاف الجرائم السيبرانية يجب أن تكون شاملةً حتى تأخذ في الاعتبار التطورات المستمرة للتكنولوجيا وتضع إطارًا قانونيًا يمكنه استيعاب هذه التطورات. كما ينبغي أن تكون التشريعات متناسقةً عالميًا؛ حيث إن الهجمات السيبرانية لا تعرف حدودًا إقليميةً فضلًا عن أنها متطورة باستمرار، فالمجرم السيبراني يتبع أساليب مبتكرةً وغير تقليدية لتنفيذ نشاطه الجرمي، مما يجعل اكتشافه أكثر صعوبةً مقارنةً بالجرائم التقليدية.

إن الجرائم السيبرانية تقوم باستخدام المجرم لتقنيات متقدمة للتخفي والتشفير، مما يصعب من مهمة تتبعه وجمع الأدلة ضده. وبالتالي، يتطلب الأمر خبرات متخصصةً وأدوات تقنيةً متقدمةً للكشف عن هذه الجرائم وتقديم مرتكبيها إلى العدالة. في المقابل، فإن الجرائم الإلكترونية تعتبر امتدادًا للجرائم التقليدية ولكن باستخدام التكنولوجيا كوسيلة لارتكابها. وبالتالي يكون تتبع وإثبات هذه الجرائم أكثر سهولة مقارنةً بالجرائم السيبرانية. ربما يعود ذلك إلى أن وسائل ارتكابها غالبًا ما تكون واضحةً وأكثر ارتباطًا بأنشطة ملموسة مثل التواصل أو المعاملات المالية.

أما فيما يتعلق بمحو أثر الجريمة السيبرانية أو الإلكترونية، فيجدر القول إن إزالة أو محو آثار الجرائم الإلكترونية التي تستهدف الأشخاص غالبًا ما يكون أقل تعقيدًا ويتطلب جهدًا أقل مقارنةً بتلك التي تستهدف شبكات أو أنظمة المعلومات مثل اختراق الأنظمة وسرقة البيانات؛ حيث تتطلب تدخلات متقدمة لإخفاء الأدلة أو تجاوز أنظمة الحماية، مما يزيد من التحديات أمام المحققين ويستدعي تشريعات وإجراءات أكثر تفصيلاً وتخصيصاً لمواجهة هذا النوع من التهديدات. على أية حال، إن اختلاف الجريمة الإلكترونية عن السيبرانية من حيث المفهوم والآثار يستلزم بيان مواطن التضارب بينهما في القوانين والتشريعات الوطنية الأردنية وهو ما سنتناوله.

72 Jenis Welukar and Gagan Bajoria, (2021). Artificial intelligence in cyber security - A review. International Journal of Scientific Research in Science and Technology, 8(6), 490.

المطلب الثاني: العلاقة بين الموطن لديه والحامل

رغم تباين مفهوم الجريمة الإلكترونية عن مفهوم الجريمة السيبرانية إلا أن المشرع الأردني خلط بينهما في قانون الجرائم الإلكترونية؛ فتارة ينص على جريمة إلكترونية يكون محلها الأشخاص، وتارة أخرى ينص على جريمة سيبرانية يكون محلها الأنظمة أو الشبكات. فبالرجوع إلى أحكام قانون الجرائم الإلكترونية الأردني، نجد أن أحكام القانون ركزت على تجريم الأفعال الواقعة على الأشخاص باستخدام وسائل إلكترونية في مواطن كثيرة. بالمقابل نجد أن الجرائم السيبرانية الواقعة على الشبكات وأنظمة المعلومات قد ورد النص عليها في مواطن معينة، منها المادتان 3 و 4 المتعلقتين بجرائم الدخول غير المصرح به إلى أنظمة المعلومات أو الشبكات، وهو تصرف سيبراني بحث يرتبط بالاعتداء على البنية التقنية نفسها. المادة 6 وتناولت جرائم متعلقة بالشبكات وأنظمة المعلومات عبر إدخال أوامر برمجية أو برامج خاصة، وهو ما يندرج تحت الجرائم السيبرانية نظرًا لأن الهجوم يستهدف البنية التقنية. المادة 7 وتناولت الجرائم التي تقع على البيانات، وهذه الجرائم تتداخل فيها الجريمة الإلكترونية والجريمة السيبرانية، حسب ما إذا كان الهجوم يستهدف البيانات الشخصية للأفراد أو البيانات المرتبطة بالأنظمة التقنية.

إن الجرائم المشار إليها في المادتين 3 و 4 من قانون الجرائم الإلكترونية تعتبر بمثابة الصورة البسيطة للجرائم السيبرانية المتمثلة في الدخول غير المصرح به لأنظمة المعلومات أو الشبكات أو تقنية المعلومات سواء أكانت هذه الأنظمة التقنية عائدة للأفراد أو المؤسسات أو الحكومة، فالركن المادي فيها قوامه الدخول غير المشروع إلى أنظمة المعلومات أو الشبكات أو موقع الكتروني؛ أي الدخول بدون تصريح أو بما يجاوز التصريح بالمعنى الوارد في المادة الثانية من قانون الجرائم الإلكترونية. فمناط عدم المشروعية هنا، هو: إما انعدام سلطة الفاعل في الدخول إلى هذا النظام أو الدخول إلى النظام بما يجاوز التصريح؛ وذلك بأن يتم الدخول دون إذن مالك النظام أو مالك الجزء منه أو صاحب الحق فيه ودون أن يكون ذلك النظام أو الشبكة متاحًا للعموم؛ أو أن يتم الدخول بإذن المالك ولكن بما يتجاوز الصلاحيات التي منحها عند ما منح الإذن، فمجرد الدخول بحد ذاته يُشكل جرمًا؛ ويُشترط توافر النتيجة الجرمية بالإضافة إلى السلوك الآثم؛ الذي يتمثل في أن ينجح الفاعل في الدخول فعلاً بسبب الأفعال غير المشروعة التي أتاها؛ أما الركن المعنوي في هذه الجرائم، فيتمثل في القصد العام المتمثل في توفر عنصري العلم والإرادة، أي علم الجاني بماهية وأركان فعله وأنه يقوم بالدخول إلى نظام معلومات أو شبكة معلوماتية من غير تصريح، واتجاه إرادته الحرة المدركة لارتكاب هذه الأفعال.

رغم أن الانتهاكات في المادتين 3 و 4 تعتبر من الصور البسيطة للانتهاكات السيبرانية إلا أنه يتبين أن المشرع قد غلظ العقوبة في حال كان الدخول غير المصرح به إلى أنظمة المعلومات أو الشبكات في حال توفر القصد الخاص المتمثل في إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو نشر أو إعادة نشر أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو خسارة سريتها أو تشفير أو إيقاف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات أو تقنية معلومات. إن هذا التشديد يعكس خطورة التدخل في البيانات والمعلومات والأنظمة لغايات غير مشروعة؛ حيث إن هذه الإجراءات لا تؤدي فقط إلى انتهاك الخصوصية بل يمكن أن تتسبب في أضرار مادية

كبيرة أو إضعاف الثقة في النظام المعلوماتي.

أما فيما يتعلق بالمادة 6 من قانون الجرائم الإلكترونية لسنة 2023 فهي تشكل الصورة الأكثر صعوبة وتعقيدا من الجرائم السيبرانية إذ استدركت خطورة انتهاكات الأمن السيبراني فأوردت حكماً خاصاً للاعتداء المتمثل في إدخال برنامج أو أمر برمجي بواسطة الشبكة المعلوماتية أو وسيلة تقنية معلومات أو باستخدام نظام معلومات للاعتداء على نظام معلومات سواء بإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تشفير أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات محفوظة على نظام معلومات أو حتى بإعاقة أو تشويش أو وقف أو تعطيل النظام أو الموقع الإلكتروني أو انتحال هوية صاحبه⁷³.

نجد أن المشرع قد خلط بين أكثر من صورة جرمية في المادة 6 من قانون الجرائم الإلكترونية؛ حيث ساوى في التكييف بين الجرائم التالية: إدخال أمر برمجي أو برنامج لتعطيل أو إيقاف نظام معلومات، إدخال أمر برمجي أو برنامج للتشويش أو إعاقة نظام معلومات، إدخال أمر برمجي أو برنامج للاعتداء على البيانات المحفوظة على نظام معلومات أو موقع إلكتروني، وانتحال هوية صاحب موقع إلكتروني. لذا فإن النهج الذي اتبعه المشرع في هذه الحالة يتعارض مع التطور التشريعي في مجال الأمن السيبراني؛ حيث تختلف كل صورة جرمية عن الأخرى في أركانها وعناصرها. فالركن المادي مشترك بين الجرائم المختلفة، وهو قيام الجاني بإدخال برنامج أو أمر برمجي إلى أحد الأنظمة التقنية. كما أن الركن المعنوي، المتمثل في العلم والإرادة، هو ذاته؛ إذ يتطلب العلم بالأفعال المقترفة واتجاه الإرادة نحو تنفيذها. ومع ذلك، يختلف القصد الخاص الذي اشترطه المشرع في كل جريمة عن الأخرى.

في جريمة التعطيل أو الإيقاف، يتمثل القصد الخاص في تعطيل نظام المعلومات أو إيقافه عن العمل، وهي جريمة أكثر خطورة من جريمة التشويش أو إعاقة عمل النظام أو الشبكة المعلوماتية، إذ أن القصد في هذه الأخيرة ليس إيقاف النظام، بل التشويش عليه وإعاقة عمله. أما في الصورة الثالثة، فإن القصد الخاص يتمثل في الاعتداء على البيانات المحفوظة على النظام أو الشبكة المعلوماتية، وليس على النظام أو الشبكة نفسها محل الجريمة. ولم يكتفِ المشرع بخلط هذه الصور الجرمية، بل نص أيضاً على جريمة إدخال برنامج أو أمر برمجي بهدف وقف أو تعطيل أو تشويش أو إعاقة موقع إلكتروني، أو انتحال هوية صاحبه. وهذه صور جرمية لا تقتصر على الأنظمة أو الشبكات، بل قد تستهدف الشخص الطبيعي أو المعنوي أو الموقع الإلكتروني، وفق ما عرّفه القانون

من اللافت أن المشرع لم يعاقب على الشروع في الصورة الأكثر خطورة من الجرائم السيبرانية الواردة في المادة 6، على خلاف ما فعل بجرم الدخول غير المشروع ذي القصد الخاص للأنظمة أو الشبكات العائدة للحكومة الواردة في المادة 4 من القانون. لذا، من الضروري أن يفرد المشرع أحكاماً خاصة تعالج حالات الشروع في هذه الجرائم السيبرانية وتحديد العقوبات الملائمة وفقاً للهدف من كل هجوم، مما يتيح للقضاء مساحةً لتطبيق عقوبات مناسبة وفقاً لخطورة الجريمة وتحقيق التوازن بين الأحكام الجرمية المتخذة.

73 المادة 6 من قانون الجرائم الإلكترونية لسنة 2023، مرجع سابق.

خاتمة

تناول البحث أحكام الأمن السيبراني في الأردن باعتباره موضوعاً جديداً في مجال القانون الجنائي؛ حيث جرى تحليل ومقارنة مفهوم الأمن السيبراني والمفاهيم ذات الصلة، بهدف تسليط الضوء على أوجه القصور في هذه المفاهيم. كما ناقش البحث الطبيعة القانونية لقانون الأمن السيبراني، وخلص إلى مجموعة من النتائج التي تبرز الجوانب القانونية لهذا الموضوع في التشريع الأردني، ومن أبرزها:

النتائج:

- قانون الأمن السيبراني في الأردن هو قانون ذو طابع تنظيمي، وليس تجريمياً؛ حيث عالج الجرائم المتعلقة بأنظمة المعلومات والشبكات من خلال قوانين أخرى مثل قانون الجرائم الإلكترونية.
- هناك تمييز واضح بين الجريمة الإلكترونية التي تستهدف الأشخاص الطبيعيين أو المعنويين، والجريمة السيبرانية التي تستهدف الأنظمة والشبكات. ومع ذلك، وضع المشرع الأردني الجرائم السيبرانية تحت مظلة قانون الجرائم الإلكترونية، مما أدى إلى تباين في المفاهيم القانونية.
- عدم تخصيص أحكام مستقلة للجرائم السيبرانية أدى إلى لبس في فهم هذه الجرائم وأثر على فعالية التصدي لها، على الرغم من التقدم الذي حققه الأردن بوضوله إلى المركز 27 عالمياً في مجال الأمن السيبراني.

التوصيات:

بناءً على هذه النتائج، يوصي البحث بما يلي:

- إعادة تصنيف الجرائم السيبرانية بتخصيص أحكام قانونية مستقلة للجرائم السيبرانية يعزز من فهم طبيعتها وتطبيق القانون عليها بشكل دقيق، مما يساهم في القضاء على اللبس القانوني الحالي.
- تعزيز دور المركز الوطني للأمن السيبراني؛ فيجب منح المركز الوطني للأمن السيبراني صلاحيات أوسع ليصبح الجهة الرئيسية لمتابعة الخروقات السيبرانية وإجراء التحقيقات الدقيقة فيها، مما يزيد من فعالية التصدي لهذه الجرائم.
- إنشاء غرف قضائية متخصصة بتأسيس غرف مختصة بالجرائم السيبرانية تساهم في تسريع الإجراءات القانونية وزيادة كفاءة تطبيق القانون، بالاعتماد على معرفة عميقة بالطبيعة الفريدة لهذه الجرائم.
- إجراء دراسات مقارنة للتشريعات الدولية والمحلية المتعلقة بالجرائم السيبرانية لاستنباط أفضل الممارسات العالمية وتطبيقها في الإطار القانوني الأردني.

- تطوير إطار قانوني مستقل؛ بصياغة قانون مستقل ينظم الجرائم السيبرانية بكل أبعادها الفنية والقانونية، ويعزز الحماية القانونية للبنية التحتية الرقمية للدولة.
- البحث في تأثير الجرائم السيبرانية على الأمن القومي والاقتصادي؛ بدراسة تأثيرات الجرائم السيبرانية بعيدة المدى على الدولة من النواحي الاقتصادية والأمنية لتوفير مبررات إضافية، وتعزيز الحماية القانونية.

المراجع

أولاً: العربية

الكتب:

- الغامدي، عبد العزيز. جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية 1428 هـ دراسة مقارنة. دار الكتاب الجامعي للطباعة والنشر والتوزيع، السعودية، 2017.
- حجازي، عبد الفتاح. الجرائم الإلكترونية: دراسة مقارنة. دار الفكر والقانون، المنصورة، ط1، 2008.
- سرور، أحمد فتحي. القانون الجنائي: المبادئ العامة للجريمة. مج1، دار النهضة العربية، القاهرة، ط3، 2006.
- محمود، عبد الرحمن. الجرائم والعقوبات، ج1. دار الكتب القانونية، عمان، ط2، 2019.
- منير، البعلبكي. معجم أعلام المورد. دار العلم للملايين، بيروت 2004.

الرسائل والأطروحات:

- الرشيد، غازي. الحماية القانونية من جرائم المعلوماتية (الحاسب والإنترنت). [أطروحة دكتوراه]، الجامعة الإسلامية في لبنان، لبنان، 2004.

المقالات العلمية:

- الحسيني، عمار وجاسم، عبد الرازق. «تكمّل القاعدة الجنائية الإجرائية». مجلة العلوم القانونية والسياسية، جامعة بغداد، م7، ع1، 2018.
- بدوسي، محمد. «تصنيف الجرائم الإلكترونية وفقاً لطبيعة الحق المعتدى عليه: دراسة مقارنة بين التشريع الفلسطيني والإماراتي». مجلة جامعة العين للأعمال والقانون، ع1. 2023.
- لطفي، وفاء. «الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني». مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، م23، ع1، 2022.
- مصطفى، إسلام. «جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات بالقانون المصري». المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية)، مج12، ع2، 2022.

التقارير:

- الأمم المتحدة، تقرير مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، قطر، نيسان 2015.
- حكومة المملكة الأردنية الهاشمية، الأسباب الموجبة لمشروع قانون الجرائم الإلكترونية الأردني، الأردن، 2015، منشورات مركز قسطاس.

القوانين:

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية، رقم 214، سنة 2010.

القرار الأميري رقم (1) لسنة 2021 بإنشاء الوكالة الوطنية القطرية للأمن السيبراني، الجريدة الرسمية لدولة قطر، العدد (3)، تاريخ الإصدار: 2021/2/7.

تعليمات التكيف مع المخاطر السيبرانية، البنك المركزي الأردني، الأردن، 2018.

قانون الأمن السيبراني الأردني، الأردن، رقم 16 لسنة 2019، منشور بالجريدة الرسمية في العدد 5595 على الصفحة 5143 بتاريخ 2019-09-16 والساري بتاريخ 2019-09-16.

قانون الجرائم الإلكترونية، الأردن، رقم 17 لسنة 2023، منشور بالجريدة الرسمية في العدد 5874 على الصفحة 3579 بتاريخ 2023-08-13 والساري بتاريخ 2023-09-12.

قانون الجرائم الإلكترونية، الأردن، رقم 27، سنة 2015، منشور بالجريدة الرسمية في العدد 5343 على الصفحة 5631 بتاريخ 2015-06-01 والساري بتاريخ 2015-06-01 الملغي ب قانون الجرائم الإلكترونية 2023 رقم 17 لسنة 2023.

قانون العقوبات وتعديلاته رقم 16 لسنة 1960، الأردن، منشور بالجريدة الرسمية في العدد 1487 على الصفحة 374 بتاريخ 1960-05-01 والساري بتاريخ 1960-06-01.

قانون المعاملات الإلكترونية، الأردن رقم، 30، سنة 2015، منشور في العدد 5341 على الصفحة 5292 بتاريخ 2015-05-17 والساري بتاريخ 2015-05-17.

قانون جرائم أنظمة المعلومات المؤقت، الأردن، رقم 30، سنة 2010، منشور بالجريدة الرسمية في العدد 5056 على الصفحة 5334 بتاريخ 2010-09-16 والساري بتاريخ 2010-10-16.

القانون رقم (14) لسنة 2014 بشأن إصدار قانون مكافحة الجرائم الإلكترونية، دولة قطر، الجريدة الرسمية، العدد (15)، الصفحة (7) تاريخ الإصدار: 2014/10/2.

نظام مكافحة جرائم المعلوماتية، السعودية، الصادر بالمرسوم الملكي رقم م/ 17 تاريخ 8 ربيع الأول 1428هـ.

الأحكام القضائية:

محكمة بداية جزاء عمان بصفتها الاستئنافية، الحكم الجزائي رقم 2021/1050، صدر بتاريخ 2021/5/9.

محكمة بداية جزاء عمان بصفتها الاستئنافية، الحكم الجزائي رقم 2024/1200، صدر بتاريخ 2024/2/27.

محكمة صلح جزاء عمان، الحكم الجزائي رقم 2023/16707، صدر بتاريخ 2023/11/20.

محكمة صلح جزاء عمان، الحكم الجزائي رقم، 2022/688، صدر بتاريخ 2023/11/23.

المواقع الإلكترونية:

<https://senate.jo/ar/2024/8/15> تاريخ الزيارة 15 / 8 / 2024
 المركز الوطني الأردني للأمن السيبراني، التقرير السنوي لعام 2023، الأردن، 2023، آخر زيارة 20 / 9 / 2024
<https://ncsc.jo/Ar/List/ReportPublic>.

ثانيًا: الأجنبية

References

Books:

- al-jarā'im al-iliktrūnīyah: dirāsah muqāranah, Hījāzī, 'Abd al-Fattāh, al-Ṭab'ah al-ūlā, Dār al-Fikr wa-al-qānūn, al-Mansūrah, 2008.
- al-jarā'im wa-al-'uqūbāt: al-juz' al-Awwal, Maḥmūd, 'Abd al-Raḥmān, al-Ṭab'ah al-thānīyah, Dār al-Kutub al-qānūnīyah, 'Ammān, 2019.
- al-qānūn al-jinā'ī: al-mabādī' al-'Āmmah lil-jarīmah, Surūr, Aḥmad Fathī, al-mujallad al-Awwal, al-Ṭab'ah al-thālithah, Dār al-Nahḍah al-'Arabīyah, al-Qāhirah, 2006.
- Cyber Crime and the Victimization of Women: Law Rights, and Regulations, Debarati Halder and Karuppannan Jaishankar, IGI Global, 2011.
- Cybernetics: Or Control and Communication in the Animal and the Machine, Norbert Wiener, 2nd revised edn, Hermann & Cie and MIT Press, 1961.
- Jarā'im al-Intarnit wa-'uqūbātuhā wafqa Nizām Mukāfahat al-jarā'im al-ma'lūmātīyah 1428 H dirāsah muqāranah, Al-Ghāmidī, 'Abd al-'Azīz, Dār al-Kitāb al-Jāmi'ī lil-Tibā'ah wa-al-Nashr wa-al-Tawzī', al-Sa'ūdīyah, 2017.
- Mu'jam A'lām al-Mawrid, Munīr al-Ba'labakkī, Dār al-'Ilm lil-Malāyīn, Bayrūt, 2004. **Thesis and dissertation**
- Al-Rashīd, Ghāzī. *al-Ḥimāyah al-qānūnīyah min Jarā'im al-ma'lūmātīyah (al-Ḥāsib wālāntrnt)* (in Arabic), doctoral dissertation, al-Jāmi'ah al-Islāmīyah fī Lubnān, Lubnān, 2004.

Journal Articles:

- Al-Ḥusaynī, 'Ammār and 'Abd al-Rāziq Jāsm. "takāmul al-Qā'idah al-jinā'īyah al-ijrā'īyah" (in Arabic), *Majallat al-'Ulūm al-qānūnīyah wa-al-siyāsīyah*, Jāmi'at Baghdād, Vol. 7, No. 1, 2018.
- Bdwsy, Muḥammad. "taṣnīf al-jarā'im al-iliktrūnīyah wafqan li-ṭab'at al-Ḥaqq alm'tdā 'alayhi: dirāsah muqāranah bayna al-tashrī' al-Filasṭīnī wa-al-Imārātī" (in Arabic), *Majallat Jāmi'at al-'Ayn lil-a'māl wa-al-qānūn*, No. 1.
- Burak Clinar. "A Study on Cyber Threat Intelligence Based on Current Trends and Future Perspectives," *Advances and Challenges in Science and Technology*, Vol. 5, 2023, p. 40.
- David Opperbeck. "Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry," *Maryland Law Review*, Vol. 75, 2016.

Gagandeep Singh & Vikrant Sharma. "Cyber-Security and Its Future Challenges," *International Journal of Information Security and Cybercrime*, Vol. 10, No. 1, 2021, p. 38.

Iris Bjelica Vlajić, Branko Nikolić, and Nadežda Gudelj. "Legal Aspects of Fighting Cyber Crime in the European Union," *ODITOR*, 2023, p. 31.

Jenis Welukar and Gagan Bajoria. "Artificial Intelligence in Cyber Security – A Review," *International Journal of Scientific Research in Science and Technology*, Vol. 8, No. 6, 2021. Available at DOI: <https://doi.org/10.32628/IJSRST218675>

Luṭfī, Wafā'. "al-Juhūd al-Dawlīyah fī majāl Mukāfahat Jarā'im al-irhāb alsybrāny" (in Arabic), *Majallat Kullīyat al-iqtisād wa-al-'Ulūm al-siyāsīyah*, Jāmi'at al-Qāhirah, Vol. 23, No. 1, 2022.

Muṣṭafā, Islām. "Jarīmat ikhtirāq al-amn alsybrāny wa-ḥimāyat istikhdām al-bayānāt wa-al-Ma'lūmāt bi-al-qānūn al-Miṣrī" (in Arabic), *al-Majallah al-qānūnīyah*, Vol. 12, No. 2, 2022.

Raghavan and Latha Parthiban. "The Growing Case of Cybercrime & Types of Cybercrime on Global Scale," *Journal of Computer Science Engineering and Information Technology Research*, Vol. 4, No. 2, 2014. Available at <https://www.tjprc.org/data/publishpapers/--1395743919-ABS%20The%20growing%20case.Pdf?>

Legislations:

AI-ttifāqīyah al-'Arabīyah li-mukāfahat Jarā'im Taqnīyat al-ma'lūmāt (in Arabic), Jāmi'at al-Duwal al-'Arabīyah, raqm 214, sanat 2010.

Budapest Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) ETS No 185.

European Parliament and Council, Directive 2013/40/EU of 12 August 2013 on attacks against information systems [2013] OJ L 218, pp 8-14. <https://eur-lex.europa.eu/legal-content/EN/TX-T/?uri=celex:32013L0040>

European Parliament and Council of the European Union, Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, (NIS Directive) Official Journal of the European Union, L 194 (2016), 1–30.

European Parliament and Council of the European Union, Directive (EU) 2022/2555 of 14 December 2022 on the Security of Network and Information Systems (NIS2 Directive), Official Journal of the European Union L 334/1 (2022) 80-152. <https://eur-lex.europa.eu/legal-content/EN/TX-T/?uri=CELEX%3A32022L2555>

Federal Information Security Modernization Act of 2014, 44 USC § 3551 et seq (2014).

Nizām Mukāfahat Jarā'im al-ma'lūmātīyah, al-Sa'ūdīyah (in Arabic), al-ṣādir bi-al-marsūm al-Malakī raqm M /17 Tārīkh 8 Rabī' al-Awwal 1428h.

Qānūn al-amn alsybrāny al-Urdunī, al-Urdun, raqm 16 li-sanat 2019 (in Arabic), manshūr bi-al-Jarīdah al-Rasmīyah fī al-'adad 5595 'alā al-Ṣafḥah 5143 bi-tārīkh 16-09-2019 wālsāry bi-tārīkh 16-09-

2019.

Qānūn al-jarā'im al-iliktrūniyah, al-Urdun, raqm 17 li-sanat 2023 (in Arabic), manshūr bi-al-Jarīdah al-Rasmīyah fī al-'adad 5874 'alā al-Şafḥah 3579 bi-tārīkh 13-08-2023 wālsāry bi-tārīkh 12-09-2023.

Qānūn al-jarā'im al-iliktrūniyah, al-Urdun, raqm 27, sanat 2015 (in Arabic), manshūr bi-al-Jarīdah al-Rasmīyah fī al-'adad 5343 'alā al-Şafḥah 5631 bi-tārīkh 01-06-2015 wālsāry bi-tārīkh 01-06-2015 al-mulghī b Qānūn al-jarā'im al-iliktrūniyah 2023 raqm 17 li-sanat 2023.

Qānūn al-'uqūbāt wa-ta'dīlātuh raqm 16 li-sanat 1960, al-Urdun (in Arabic), manshūr bi-al-Jarīdah al-Rasmīyah fī al-'adad 1487 'alā al-Şafḥah 374 bi-tārīkh 01-05-1960 wālsāry bi-tārīkh 01-06-1960.

Qānūn al-mu'āmalāt al-iliktrūniyah, al-Urdun raqm 30, sanat 2015 (in Arabic), manshūr fī al-'adad 5341 'alā al-Şafḥah 5292 bi-tārīkh 17-05-2015 wālsāry bi-tārīkh 17-05-2015.

Qānūn Jarā'im anẓimat al-ma'lūmāt al-mu'aqqat, al-Urdun, raqm 30, sanat 2010 (in Arabic), manshūr bi-al-Jarīdah al-Rasmīyah fī al-'adad 5056 'alā al-Şafḥah 5334 bi-tārīkh 16-09-2010 wālsāry bi-tārīkh 16-10-2010.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (The European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15.

Ta'līmāt al-takayyuf ma'a al-makhāṭir alsybrānyh (in Arabic), al-Bank al-Markazī al-Urdunī, al-Urdun, 2018.

Reports and decisions :

Al-Umam al-Muttaḥidah, taqrīr Mu'tamar al-Umam al-Muttaḥidah al-thālith 'ashar li-man' al-jarīmah wa-al-'adālah al-jinā'iyah (in Arabic), Qaṭar Nisyān 2015.

Ḥukūmat al-Mamlakah al-Urdunīyah al-Hāshimīyah, al-asbāb al-mūjibah li-mashrū' Qānūn al-jarā'im al-iliktrūniyah al-Urdunī (in Arabic), al-Urdun, 2015, Manshūrāt Markaz Qistās.

Maḥkamat bidāyat Jazā' 'Ammān bi-şifatihā al-Isti'nāfiyah, al-ḥukm al-jazā'ī raqm 1050/2021 (in Arabic), Şadr bi-tārīkh 9/5/2021.

Maḥkamat bidāyat Jazā' 'Ammān bi-şifatihā al-Isti'nāfiyah, al-ḥukm al-jazā'ī raqm 1200/2024 (in Arabic), Şadr bi-tārīkh 27/2/2024.

Maḥkamat Şulḥ Jazā' 'Ammān, al-ḥukm al-jazā'ī raqm 16707/2023 (in Arabic), Şadr bi-tārīkh 20/11/2023.

Maḥkamat Şulḥ Jazā' 'Ammān, al-ḥukm al-jazā'ī raqm 688/2022 (in Arabic), Şadr bi-tārīkh 23/11/2023.

Websites:

Al-Markaz al-Waṭanī al-Urdunnī lil-Amn al-Saybarānī, *Al-Taqrīr al-Sanawī li-Ām 2023*, Al-Urdun,

- Tārīkh al-ziyārah 20/9/2024. available at <https://ncsc.jo/Ar/List/ReportPublic>
- Asbāb al-mūjibah lsn Qānūn al-amn alsybrāny (in Arabic), Majlis al-a'yān, Tārīkh al-ziyārah 15/8 /2024 <https://senate.jo/ar>.
- Demandsage. Shocking Cybersecurity Statistics for 2024. visit date 20/9/2024. <https://www.demand-sage.com/cybersecurity-statistics>
- National Cybersecurity Center (Jordan). (2023). Annual Report 2023. Jordan: National Cybersecurity Center. Available at: <https://ncsc.jo/Ar/List/ReportPublic> (Accessed 20/9/2024).
- The European Union Agency for Cybersecurity (ENISA), ENISA threat landscape report 2023, date of last visit 2/9/2024. file:///C:/Users/Dell/Downloads/ENISA%20Threat%20Landscape%202023.pdf.
- Varonis. 157 Cybersecurity Statistics and Trends [Updated 2024] visit date 20/9/2024. <https://www.varonis.com/blog/cybersecurity-statistics>
- World Economic Forum. 2023 was a Big Year for Cybercrime – Here's How We Can Make Our Systems Safer. Available at <https://www.weforum.org/stories/2024/01/cybersecurity-cyber-crime-system-safety/> visit date 20/9/2024.