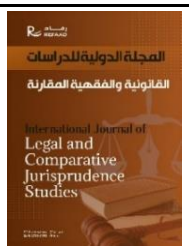
www.refaad.com

International Journal of Legal and Comparative Jurisprudence Studies (LCJS)
المجلة الدولية للدراسات القانونية والفقهية المقارنة
Journal Homepage: https://www.refaad.com/Journal/Index/9
E-ISSN 2708-6607 | P-ISSN 2708-6593
Vol. 6, specialissue, 2025, pp. 18 - 27



Law Applicable to Civil Liability for Cyberattack in the Perspective of Jordanian Legislation [2]

Ammar Mahmoud Al-Rawashdeh [1*]
[1] Associate Professor of Civil Law, Faculty of Law, Jerash University, Jordan
* Corresponding Author: Ammar Rawashdeh (salahammar650@yahoo.com)

القانون الواجب التطبيق على المسؤولية المدنية المترتبة عن الهجوم السيبراني في منظور التشريعات الأردنية [1]

عمار محمود الرواشده [*1]
[1] أستاذ مشارك في القانون المدني- كلية الحقوق- جامعة جرش- الأردن
*الباحث المراسل: عمار رواشدة (salahammar650@yahoo.com)
https://orcid.org/0000-0003-1485-4309

This file is licensed under a
Creative Commons Attribution 4.0 International

Received استلام البحث	Revised مراجعة البحث	Accepted قبول البحث
2024/10/8	2024 /11/13	2024 /12/13

DOI: https://doi.org/10.31559/LCJS2025.6.specialissue.3

Abstract:

Objectives: The purpose of this study is to demonstrate the legal regulation in private international law of such problems, as well as to address some applicable and practical problems relating to the subject matter of the letter, including the legal nature of cyberattacks.

Methods: The study adopted the inductive approach through extrapolation of the legal texts on the subject of the research in accordance with Jordanian legislation, as well as the analytical approach. The researcher analysed and described the legislative and doctrinal positions and international conventions relating to the subject of the letter and the descriptive approach through the legal nature of cyberattacks.

Results: The study found a number of results, the most important of which were the absence of clear and explicit texts specifying the applicable law on civil liability for cyberattack in the perspective of Jordanian legislation.

Conclusions: This study recommended that Jordan's legislature should provide detailed provisions on the determination of the law applicable to damages arising from cyberattacks.

Keywords: *Electronic ecology; conflict of laws; civil liability; cyberattacks; damage.*

الملخص:

الأهداف: تهدف هذه الدراسة إلى بيان التنظيم القانوني في القانون الدولي الخاص لمثل هذه الإشكالية إضافة لمعالجة بعض الإشكاليات العملية والتطبيقة المتعلقة بموضوع البحث والتي منها بيان الطبيعة القانونية للهجمات السيبرانية.

المنهجية: اعتمدت الدراسة المنهج الاستقرائي من خلال استقراء النصوص القانونية المتعلقة بموضوع البحث وفق التشريع الأردني، إضافة للمنهج التحليلي حيث عمل الباحث على تحليل وبيان المواقف التشريعية والفقهية والاتفاقيات الدولية المرتبطة بموضوع البحث، والمنهج الوصفي من خلال الطبيعة القانونية للهجمات السيبرانية.

النتائج: خلصت الدراسة إلى عدد من النتائج أهمها، عدم وجود نصوص واضحة وصريحة تحدد القانون الواجب التطبيق على المسؤولية المدنية المترتبة عن الهجوم السيبراني في منظور التشريعات الأردنية.

الخلاصة: أوصت هذه الدراسة أنه على المشرع الأردني إيراد أحكام تفصيلية بشأن تحديد القانون الواجب التطبيق على الأضرار الناشئة عن الهجمات السيبرانية.

الكلمات المفتاحية: *بئية إلكترونية؛ تنازع قوانين؛ مسؤولية مدنية؛ هجمات سيبرانية؛ أضرار.*

الاستشهاد

Citation

الرواشده، عمار. (2025). القانون الواجب التطبيق على المسؤولية المدنية المترتبة عن الهجوم السيبراني في منظور التشريعات الأردنية. المجلة الدولية للدراسات القانونية والفقهية المقارنة، 6 (عدد خاص)، 18- 27.

Al-Rawashdeh, A. (2024). Law Applicable to Civil Liability for Cyberattack in the Perspective of Jordanian Legislation. *International Journal of Legal and Comparative Jurisprudence Studies*, 6(specialissue), 18-27. https://doi.org/10.31559/LCJS2025.6.specialissue.3

[1] قُدمت الورقة في أعمال مؤتمر الثورة الصناعية الرابعة من منظور قانوني (التحديات- والحلول) كلية القانون بجامعة اليرموك -الأردن 22-23 يوليو 2024م.

[2] The paper was presented at the Conference on the Fourth Industrial Revolution from a Legal Perspective (Challenges and Solutions), Faculty of Law, Yarmouk University, Jordan, July 22–23, 2024.

المقدمة:

أدى التطور التقني والتكنولوجي في المعلومات إلى تحويلها إلى بيانات رقمية إلكترونية يتم استخدامها من قبل المستفدين، في كافة مجالات الحياة في هذه البيئة الإلكترونية الافتراضية، فقد باتت هذه البيئة الافتراضية ميدان للاتصال في مختلف نواحي التعاملات، حيث بإمكان الشخص العادي الوصول إلى المعلومات سواء كان في الشارع أو في بيته أو مكتبه، لذلك أصبح الوصول إلى هذه المعلومات متاحة للجميع.

إن الدمج ما بين وسائل الاتصال ونظام الحاسوب شكل أحد عناصر تقنية المعلومات، فشبكة المعلومات والتي تشكل الإنترنت، قامت بربط الملايين من أجهزة الحاسبات بعضها ببعض، بالإضافة إلى أن هذه التقنية أصبحت مرتكزًا رئيسًا لإدارة التعاملات التجارية، والاستثمار الدولي، فأصبحت تقنية المعلومات أحد متطلبات التنافس، فشبكة الأعمال الإلكترونية هي أحد أهم نتج تقنية المعلومات.

وعلى الرغم من الفوائد الكبيرة التي قدمتها تقنية المعلومات، إلا أنها خلقت أنماطًا جديدة في الأعمال غير المشروعة والتي أطلق عليها (الجريمة الإلكترونية والهجوم السيبراني) حيث أنه من الصعوبة بمكان في كثير من الأحيان بيان ما إذا كان الفعل السيبراني واحدًا أو آخر (أو كلاهما)، في وقت وقوع الفعل - ويرجع ذلك جزئيًا إلى أن هوية الفاعل والقصد قد لا يكون واضحً.

ونظرًا للغموض الذي يحيط بهذا الأمر، يوصى برد فعل عاجل ومناسب على تلك الجرائم السيبرانية أو الهجوم السيبراني، ومن هذه الأفعال غير المشروعة منها جرائم الكمبيوتر والإنترنت، كما أن التقنية الحديثة سهلت ارتكاب العديد من الأفعال غير المشروعة بسرعة وبفاعلية اكبر من الطرق التقليدية، ومن صور هذا الأفعال غير المشروعة أيضًا، نشر فيروسات الكمبيوتر، التي أثرت وتؤثر بشكل كبير على برامج الكمبيوتر مما يؤدي إلى إحداث خلل في برامجها أو بالوثائق المحفوظة عليه أو سرقة هذه الوثائق أو نشر هذه الوثائق الأمر الذي يترتب عليه إلحاق الضرر بصاحب هذه الوثائق أو المعلومات التقنية، كما عملت شبكة المعلومات على تسهيل الوصول إلى المعلومات وساهمت بالمساس بالخصوصية والتعدي عليها وعلى الحياة الخاصة لمتستخدمي هذه الشبكة، هذه الأفعال والأضرار لاتستلزم فقط تطوير القواعد الجزائية والإجرائية والموضوعية في الشق الجزائي إنما يجب أن يواكبه في نفس المسار تطوير القواعد الموضوعية والإجرائية المدنية وبالذات قواعد القانون الدولي الخاص.

ولما كان الضرر الذي نتج عن هذا الفعل غير المشروع، له طبيعة مغايرة لمحل الضرر فيما عرفته القوانين في الجانب المدني، فقد اناّ للمشرع في (الشق المدني) أن يتدخل لتوفير الحماية اللازمة من هذه الأفعال غير المشروعة الخطرة والمستجدة والتي قد لايكون لها نصوص واضحة وصريحة، سيما أن موضوع تحديد القانون الواجب التطبيق على المسؤولية لم تحظى باهتمام تشريعي كافي وواضح بما يتعلق بها.

ويلزم لذلك أن تكون القواعد القانونية مواكبه للطبيعة الخاصة لأنماط الأفعال الغير مشروعة عبر الإنترنت، حيث أنه خلال هذا التطور الكبير الذي شهده العالم في هذه البيئة الإلكترونية، ظهرت الهجمات الإلكترونية السيبرانية، من خلال الهاكرز أو قراصنة الإنترنت، الذين يمتلكون قدرة وخبرة عالية تمكنها من اختراق الحماية الإلكترونية للمواقع الإلكترونية، الممنوعون من الدخول إليها، لتحقيق العديد من الأهداف والغايات غير المشروعة، والتي منها الحصول على وثائق أو أسرار خاصة بالأفراد أو المنشاءات التجارية أو الحكومية، وبالتالي اخذت هذه الهجمات السيرانية، مكانه هامة وبارزة للمشتغلين والعالمين في المجال الإلكتروني والقانوني، ففي مجال الإلكتروني تمثل في تطوير برامج قادرة على صد تلك الهجمات والتخفيف من محاولة اختراق تلك البيانات السرية، أما بالنسبة للاتجاه القانوني، فقد تمثل بتحديد وبيان طبيعة تلك الهجمات والأضرار المترتبة عليها بالإضافة إلى تحديد القانون الواجب التطبيق لبيان القواعد الموضوعية التي ستحكم هذه المسالة.

أهمية الدراسة:

تكتسب الدراسة أهميتها من مجموعة من النقاط، يمكن إيجازها فيما يلي:

- تكمن أهمية هذه الدراسة لهذه الظاهرة في معرفة القانون الواجب التطبيق على الأضرار الناتجة عن التسلل إلى مواقع إلكترونية غير المسموح الدخول إليها من أجل الاستحواذ عليها أو تعطيلها أو إتلاف البيانات الموجوده فيها، فكان لزامًا علينا أن نبين الطبيعة القانونية لهذه الظاهرة وخصائصها وصورها والقواعد القانونية الناظمة لمسالة التنازع الدولي الخاص، ولايتم ذلك إلا من خلال تحليل هذه الأفعال السيبرانية، وبيان صورها واستعراض القواعد القانوية الخاصة بها، ولا ياتي ذلك إلا بعد معرفة الطبيعة القانونية لها وصورها.

مشكلة الدراسة:

- تكمن مشكلة الدراسة التي يثيرها هذا البحث والتي تقتضي البحث عن إجابة هي: هل تم إيجاد قواعد قانونية خاصة لمعالجة تحديد القانون الواجب التطبيق على الأضرار الناجمة عن الهجمات السيبرانية التي لها طبيعتها الخاصة تستوجب قواعد قانونية خاصة تتلائم مع طبيعة هذه الأفعال، أم سيتم إعمال القواعد العامة بما يتعلق بالنزاعات الخاصة الدولية؟

أهداف الدراسة:

تهدف هذه الدراسة إلى:

- تحدد مفهوم الهجمات السيبرانية أو الجريمة السيبرانية.
- تحديد القانون الواجب التطبيق على الأضرار الناشئة عن الهجمات السيبرانية.

منهج الدراسة:

إنطلاقًا من هذه الأهمية للدراسة فقد حاول الباحث جاهدا البحث فيها من خلال اعتماد المنهج الوصفي، باعتباره المنهج الأفضل للوصول إلى أهداف الدراسة كما عملت هذه الدراسة استخدام المنهج التحليلي من خلال تحليل نصوص المواد والدراسات المتعلقة بهذا البحث كما تم استعمال المنهج الاستقرائي للوصول إلى أفضل النتائج والتوصيات لهذه الدراسة.

خطة الدراسة:

المبحث الأول: مفهوم الهجمات السيبرانية

المطلب الأول: تعريف الهجمات السيبرانية.

المطلب الثاني: الطبيعة القانونية للهجمات السيبرانية.

المبحث الثاني: تحديد القانون الواجب التطبيق على الضرر الناتج عن الهجمات السيبرانية

المطلب الأول: الحلول التشريعية لتحديد القانون الواجب التطبيق على الضرر الناتج عن الهجمات السيبرانية.

المطلب الثاني: الحلول الفقهية لتحديد القانون الواجب التطبيق على الضرر الناتج عن الهجمات السيبرانية.

المبحث الأول: مفهوم الهجمات السيبرانية

سيتم في هذا البحث بيان مفهوم الهجمات السيبرانية من خلال استعراض التعريفات الخاصة به، وبيان وسائل الهجمات السيبرانية وبعد ذلك سيتم الحديث عن التكييف القانوني للهجمات السيبرانية وطبيعته الخاصة.

المطلب الأول: تعريف الهجمات السيبرانية

مصطلح الهجمات السيبرانية اختلف وتعدد مفهومة باختلاف الأساس الذي يستند إليه مضمون الهجمات السيبرانية حيث تم تعريفه بأنه:

أولًا: التعريفات التشريعية

عُرف المشرع الأردني الهجمات السيبرانية في قانون الأمن السيبراني رقم 16لسنة (2019) بأنها:" الفعل أو الهجوم الذي يشكل خطرًا على البيانات أو المعلومات أو الشبكة المعلوماتية أو البنى التحتيه المرتبطة بها ويتطلب استجابة لإيقافه أو للتخفيف من العواقب أو الآثار المترتبة عليه.

ثانيًا: التعريفات الفقهية

تم تعريفه: بأنه عالم افتراضي مع عالمنا المادي، يتاثر به ويؤثر فيه بشكل معقد، وتعتمد الهجمات السيبرانية على نظم الكمبيوتر، وشبكات الإنترنت، والمخزون الهائل من المعلومات والبيانات، حيث يتم الاتصال بشبكات الإنترنت عبر الحواسيب، أو الهواتف، أو غيرها من الأجهزة دون تقيد بالحدود الجغرافية، لذلك فان الهجمات السيبرانية -في هذا الاتجاه- يمكن وصفها بانها عبارة عن تصرف واقعي، يدور في عالم افتراضي قائم على استخدام بيانات رقمية، ووسائل اتصال تعمل إلكتروني، ومن ثم تطور هذا المفهوم، حيث اصبح واسعًا يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة؛ جراء اختراق مواقع إلكترونية حساسة، عادة ماتقوم بوظائف تصنف بأنه ذات أولوية، كأنظمة حماية محطات الطاقة النووية، أو الكهربائية، أو المطارات، ووسائل النقل الأخرى (نورة، 2018، ص190).

وعرف أيضًا بأنه: وسيلة قتالية من خلال استخدامها بذاتها للتسلل إلى أنظمة إلكترونية، معدة لحماية أو لتنظيم سير عمل منشأت حيوية، كمحطات توليد الطاقة النووية، أو السدود أو وسائل النقل كالمطارات؛ بهدف تطويعها والسيطرة عليها؛ لتدمير ذاتها بذاتها من خلال تغذيتها بمعلومات غير صحيحة لأجهزة التحكم والحماية الإلكترونية (الفتلاوي، 2016، ص 619).

ويعرف بأنه: هجوم عبر الإنترنت يقوم على التسلل إلى مواقع إلكترونية غير مرخص الدخول اليها، بهدف تعطيل البيانات المتوفره فيها، أو اتلافها، أو الاستحواذ عليها، وهي عبارة عن سلسلة هجمات إلكترونية تقوم بها دولة ضد أخرى (الفتلاوي،2016،ص 619).

وهو عبارة عن هجوم يتم شنه من أحد أجهزة الكمبيوتر أو مجموعة من الأجهزة على جهاز كمبيوتر آخر أو عدة أجهزة كمبيوتر أو (بدون اسم الناشر، بدون سنة نشلر، بدون رقم ص) https://www.it-pillars.com/ar/blog-ar

وتعرف الهجمات الإلكترونية بأنها هجمات ذات دوافع اجتماعية أو سياسية يتم تنفيذها في المقام الأول عبر شبكة الإنترنت (كاي ايه وايز، مركز دبي لبحوث السياسة العامة، 2015 ، الهجمات الإلكترونية)

إذا الهجوم الإلكتروني (سايبر اتاك) عبارة عن اختراق عالمي لأنظمة الكمبيوتر، والشبكات، والشركات التي تعتمد على التكنولوجيا، تستخدم تلك الهجمات تعليمات برمجية ضارة لتعديل شفرة أجهزة الكمبيوتر أو البيانات او الأرقام، ويُفضي ذلك إلى نتائج مُدمِّرة يمكن أن تتسبب في الأضرار بالبيانات الخاصة بك وانتشار جرائم الفضاء الإلكتروني مثل سرقة المعلومات والهوية، كما يُعرف الهجوم الإلكتروني أو السيبراني بالهجوم باستخدام شبكة الكمبيوتر(بدون اسم الناشر، بدون سنة نشلر، بدون رقم ص)(CNA) . https://www.it-pillars.com/ar/blog-ar

وبعد أن قام البحث ببيان التعريفات الخاصة بالهجمات السيبرانية في الفرع الأول سيتم في الفرع الثاني بيان خصائص الهجمات الإلكترونية.

ثالثًا: خصائص الهجمات الإلكترونية

1. أنها لاتعرف الحدود الدولية بسبب ما تتميز به شبكة الإنترنت من انها شبكة عالمية. يمكن القول أن ظهور شبكات المعلومات ، حولت الحدود من ملموسة ومرئية إلى حدود غير مرئية أو ملموسة مما يسبب عدم القدرة بالوقوف أمام تدفق تلك المعلومات، من خلال الدول المختلفة، فالأجهزة الإلكترونية تتمتع بقدرة عالية على نقل المعلومات بكميات كبيرة عبر الآف الاميال الأمر الذي يترتب عليه تعدد أماكن الهجمات السيبرانية مما يؤدي إلى صعوبة تحديد مكان وقوع الفعل الضار (قورة، 2005، ص 52).
2. سهولة التنقل من قبل مرتكبي هذه الهجمات وهو جالس في مكانه أمام شاشة الحاسب الالي.
3. هذه الهجمات لها صفة الجرائم العابرة للحدود: تتميز الهجمات السيبرانية بتخطيها للحدود الجغرافية، الأمر الذي يترتب عليه إضفاء الصفة الدولية، وتعتبر بانها ذات طبيعة متعدية للحدود.
4. لها آليات خاصة يتم بها تنفيذ الهجمات الإلكترونية.
5. تعتمد على شبكات الإنترنت للقيام بها.
6. استخدام برامج معدة خصيصًا لتنفيذ الهجمات الإلكترونية.
7. القدرة على التلاعب بالبرامج الغلكترونية.

وبعد الانتهاء من بيان خصائص الهجمات الإلكترونية سيتم التعرف على أنواع الهجمات الإلكترونية في الفرع الثالث.

رابعًا: أنواع الهجمات الإلكترونية (الهجمات السيبرانية)

1. هجمات الحرمان من الخدمة

هي نوع من الهجمات التي تعمل من خلال آلية إغراق المواقع بكثافة عالية من البيانات التي لاتعتبر ضرورية، وتقوم هذه الآلية على إرسال هذه البيانات ببرامج ذكية متخصصة تقوم بنشر هذه الهجمات التي تتسبب في العديد من الأضرار منها ازدحامًا في استخدام هذه الموقع أو إحداث عجز في هذه الخدمات وبطئها، وقد تعرض العديد من المواقع الخدمية لهذه الهجمات ومن اهم هذه المواقع(Amazon,Word press) وغيرها، على الرغم من الإجراءات الاحتياطية المتخذة لمواجهة مثل هذه البرامج.

2. قراصنة مو اقع الويب واختراق الحواسيب

في هذا النوع من الهجمات يقوم الشخص المخترق بالدخول إلى موقع غير مخول له الدخول إليه، والعمل على إجراء تعديلات في البيانات المحتفظ بها على هذه الموقع الإلكترونية بدون اذن وموافقة مالك هذه البيانات مما يؤدي إلى الحاق الضرر بمستخدم ومالك هذه المواقع (SLobbe,2012,p2-3.).

3. الحصار الافتراضي

يتم العمل في هذا النوع من الهجمات على منع المستخدمون من الولوج إلى المواقع الإلكترونية التي يعملون عليها بإحداث خلل في اليات سريان العملية التقليدية (SLobbe,2012,p2-3) .

4. الفيروسات

في هذا النوع من من الهجمات يتم استخدام برنامج يتميز بقدرات عالية متنوعة، ومتغيرة من أهمها الاختفاء داخل البرنامج الأصل، حيث يعمل هذا البرنامج على تدمير المعلومات أو تعديلها أو تغيرها، لذلك أطلق عليه البرنامج الضارة، هي اختصار لكلمة برنامج ضار ويمكن أن يشير البرنامج الضار إلى أي نوع من البرامج، بصرف النظر عن طريقة تكوينه أو تشغيله، وهو "مصمم إلحاق الضرر بجهاز الكمبيوتر أو السيرفر أو شبكة جهاز الكمبيوتر مثلما تعرفه : Microsoft إن الفيروسات المتنقلة والفيروسات وحصان طروادة تندرج كلها تحت البرامج الضارة، ولا يميزها عن بعضها البعض سوى الوسائل التي يتم استخدامها لإنشائها ونشرها، قد تتسبب هذه الهجمات في تعطيل جهاز الكمبيوتر أو الشبكة، أو تمكن المهاجم من الوصول حتى يتمكن من التحكم في النظام عن بعد.

5. قنبلة البريد الالكتروني

تقوم هذه الطريقة على إرسال سيل من الرسائل الإلكترونية، إلى صندوق البريد الالكتروني، تفوق القدرة الاستيعابية، لهذا البريد الإلكتروني مما يؤدي إلى إحداث خلل في التعامل مع هذه الرسائل الكبيرة، وعدم استعيابها وتلقها (الزرو، 2007، ص216).

قمنا بدراسة أنواع وصور الهجمات الإلكترونية وتم الحديث عن أنواعها بشكل مختصر وتبين لنا خطورة هذا النوع من الهجمات لانه لايمكن حصرها بصورة أو نمط واحد وانما تعددت صورها وأنماطها.

المطلب الثاني: الطبيعة القانونية للهجمات السيبرانية

يعد ازياد استخدام شبكة الإنترنت في العقود الأخيرة على كافة المستويات، والتي كانت سببًا كبيرفي ترابط الأعمال التجارية وغير التجارية التي يتم إنشاءه من قبل المجتمعات والدول والأفراد، وفي الوقت نفسه زادت الخروقات وعمليات الاختراق لهذه التعاملات فأصبح العالم في الأونه الأخيرة يتصدى لنوع جديد من أطلق عليه مصطلح الهجمات السيبرانية أو الجرائم السيبرانية.

وعليه قد أحدث الفضاء السيبراني نوع جديد من التطورات مما تترتب على ذلك السعي إلى إيجاد قواعد قانونية قادرة على موكبة التطور التقني السيبراني، في ظل قواعد قانونية موجودة غير قادرة على تنظيم هذا النوع من التعاملات، وفي ظل ما تتميز بها هذا البيئة الإلكترونية من خصائص مميزه للفضاء الإلكتروني، وعليه فإنه لابد من بيان التكييف القانوني للهجمات السيبرانية، ثم بيان المسؤولية المدنية للأضرار الناتجة عن الهجمات السيبرانية.

أولًا: التكييف القانوني للهجمات السيبرانية

لقد شكلت الهجمات السيبرانية عبء من حيث بيان الطبيعة القانونية لهذه الهجمات السيبرانية والأضرار الناجمة عنها، التي يختلف تكييفها باختلاف جهة منفذ هذه الهجمات فإذا كان منفذ هذا الفعل غير المشروع هو دولة فإن تكييفها يخضع إما للقانون الدولي الإنساني أو الدولي العام بينما إذا كان منفذ هذه العمليات هم أفراد لا يتأمرون لدولة أو يتأمرون ولكن ليسوا من أشخاص القانون العام وإنما من أشخاص القانون الخاص، كما يجب التفريق في بين الطبيعة القانونية للهجمات السيبرانية مابين الشق الجزائي وما بين الشق المدني، حيث أن البحث عن الطبيعة القانونية للجانب المدني يتطلب البحث في أنواع المسؤولية المدنية هل يتم اخضاعها للمسؤولية العقدية أو المسؤولية التقصيرية، أما في الشق الجزائي فإنه يتم البحث في قانون العقوبات وأعمال الجريمة وعقوبة الابنص، إذا كان الهجوم ضمن الإطار الوطني الداخلي وهذا لا يدخل في نطاق دراستنا، وإنما يتم البحث في هذه الدراسة عن الأضرار الناجمة عن هذه الأفعال غير المشروعة والاستعمال غير المشروع والتعدي والفعل الضار، وفي القانون الواجب التطبيق على الأضرار الناشئة عن هذه الهجمات السيبرانية.

إذا هذه الظاهرة الإلكترونية لها طبيعة خاصة، ذلك أن الهجوم السيبراني ينصب على الحاسب الآلي وما تحتويه من معلومات أو بيانات محتفظ بها داخل ذاكرة الجهاز الإلكتروني، من أجل الوصول والاطلاع على تلك المعلومات المخزنة والمحتفظ بها بشكل سري أو غير سري لا يسمح لغير المخولين بالإطلاع عليها أو حذفها أو تعديلها، مما يؤدي إلى إلحاق الضرر بأصحاب تلك المعلومات المخزنة من خلال نشرها أو حذفها أو سرقتها أو تعديلها أو حتى منعهم من الوصول إليها، ومن أهم خصائص هذا النوع من الهجمات قلة حالات اكتشافها حيث تعتبر من الجرائم النظيفة التي لا يترك فاعلها أو مرتكبها أي آثار الأمر الذي يؤدي إلى صعوبات في اكتشافها وإثباتها.

لقد عملت الهجمات السيبرانية على تشكيل تهديدًا لحقوق الأفراد والشركات والمنشآت من خلال الاعتداء عليها، وإلحاق الضرر بها، فاحترام حقوق الأفراد أو الجماعات يشكل أهم المبادئ التي تقوم عليها التعاملات بين الأفراد، والتعويض عن هذه الأضرار أيضًا يعتبر من المبادئ الأساسية التي يجب ترسيخها في نصوص قانونية واضحة وصريحة، ففي ظل اتساع نطاق المسؤولية المدنية، بسبب الأفعال غير المشروعه التي تتم من خلال هذه البئية الافتراضية الإلكترونية، التي تعددت صوره وأشكالها كسرقة المعلومات أو الدخول إلى الحسابات البنكية والتلاعب فيها أو تخريبها، أو الدخول إلى حسابات خاصة، الأمر الذي يتطلب نصوص واضحة لتعويض المتضررين الذين لحق بهم ضرر بسبب هذه الهجمات السيبرانية، حيث أن هذه العملية الإلكترونية، إذا الحقت ضرر بالأفراد أو المؤسسات أو المنشآت فإنها تقوم وتنشأ المسؤولية المدنية في هذا الوضع.

وبالبناء على ما سبق فإن طبيعة هذه الهجمات التي تعددت صوره وأشكالها وما يتم القيام به من أفعال سواء كان بسرقة المعلومات أو حذفها أو نشرها وتعديلها أو منع أصحابها من الدخول إليها من أجل ابتزازهم، ترتب عليها أضرار، مما يستوجب قيام المسولية المدنية (التقصيرية) التي تعطي إلحاق للأفراد المطالبة بالتعويض عما تعرضوا له من خسائر وأضرار بسبب هذه الأفعال غير المشروعة، وبما أن هذه الهجمات في أغلبها عابرة للحدود فانها تدخل في مفهوم القانون الدولي الخاص من أجل الإرشاد إلى القانون الواجب التطبيق، مما يستوجب البحث في القواعد الخاصة للمسؤولية المدنية عن أضرار الهجمات السيبرانية العابرة للحدود،الأمر الذي يستدعي البحث في هذه القواعد من أجل الوصول إلى القانون الواجب التطبيق على المسؤولية المدنية للأضرار الناتجة عن هذه الهجمات السيبرانية.

ثانيًا: المسؤولية المدنية عن أضرار الهجمات السيبرانية العابر للحدود

لقد اختلف الأساس الذي تقوم عليه المسؤولية التقصيرية في التشريعات الأردنية عنه في بعض الاتجاهات منها الجزائري المادة 125 مسؤولية القاصر المميز وهذا بعد إلغاء الفقرة الثانية من هذه المادة التي تنص على مسؤولية عديم التميز بمقتضى القانون 05-10 المتمم والمعدل للقانون المدني ومنه تنص المادة 124 من القانون المدني:" كل فعل أيًا كان يرتكبه الشخص بخطئة ويسبب ضررًا للغير يلزم من كان سببًا في حدوثه بالتعويض" فيقصد بها مسؤولية الشخص عن الفعل الذي يصدر منه نفسه دون وساطة شخص آخر أو تدخل شيء مستقل عنه. الذي أسست المسؤولية التقصيرة على الخطا لا على الفعل (الضار) الذي لايشترط الإدراك والتمييز حيث نصت المادة (256) من القانون المدني الأردني على أنه:" كل أضرار بالغير يلزم فاعله ولو غير مميز بضمان الضرر القانون المدني الأردني رقم 34 لسنة 1976"

وعليه فان النظام القانوني الذي تقوم عليه المسؤولية المدنية بغض النظر عن اشتراط إدراكه أو عدم إدراكه يترتب عليه التزام مرتكب العمل (الغير مباحًا قانونًا)، بدفع التعويض عن الضرر الذي الحقه في المال أو في النفس، لذلك تقوم رابطة قانونية بسبب هذا العمل (الضار) بين المضرور وفاعل الضرر، فيتم الزام مرتكب الفعل بدفع التعويض للمضرور عن هذا الفعل والعمل الذي تم من قبلها، وعليه فإن الفاعل السيبراني في الهجمات السيبرانية إذا ألحق ضرر بممتلاكات الآخرين، بسبب سرقة المعلومات الإلكترونية أو تعديلها أو تحريفها أو نشره بدون موافقة صاحبه، أو دخوله إلى موقع غير مرخص له الدخول إليه أو غير مسموح له الوصول إليه، فإن الفاعل أو مرتكب هذا الفعل ملزم بدفع كافة التعويضات للمتضرر بسبب هذا الهجوم السيبراني.

أن تطبيق الأحكام العامة في الأنظمة القانونية للمسؤولية المدنية لا تثير أية إشكالية أو صعوبة، فيتم العمل بها بكل سهولة ويسر، لكن هذا التطبيق وهذا العمل، لهذه الأحكام العامة في مجال المسؤولية عن أضرار الهجمات السيبرانية ليس كذلك، ويعود السبب في ذلك إلى حداثة المشكلات المثارة التي لا يمكن تطويعها بشكل كبير في تطير القواعد القانونية التقليدية، وتبرز أهم الصعوبات في هذا النوع من الأضرار فيما يلي:

1. صعوبة تحديد مرتكب الفعل الغير مشروع

إن قوام المسؤولية المدنية في نظامه يقوم على نسبة الخطأ أو الفعل الضار أو التعدي أو الضرر إلى الفاعل أو المسؤول، حيث يقع على عاتق المضرور أو طالب التعويض إثبات مخالفة الفاعل أو المسؤول للسلوك المعتاد، من خلال قيامه بمخالفة القوانين أو ارتكابه الفعل غير المشروع بشكل عمدي أو وجود إهمال أو تقصير أو عدم تبصر، لذلك فإن عملية إثبات ركن الخطأ أو الفعل الضار في مجال المسؤولية عن أضرار الهجمات السيبرانية يثير العديد من الإشكاليات، فإذا كان بالإمكان إثبات بعض النشاطات غير المشروعة، فإنه لايمكن أو يصعب إثباته في كل صور هذه الهجمات السيبرانية، لذلك فإن الخطأ أو الانحراف عن السلوك المعتاد سواء كان مدركًا أو غير مدرك فإنه واجب الإثبات الذي يكاد يكون متعذر في هذا النوع من الأفعال غير المشروعة، بسبب الطبيعة الخاصة للنشاط المتعلق بالهجمات السيبرانية، ولا أدل على ذلك من أن المسؤولية الناجمة عن الهجمات السيبرانية القائمة على الخطأ أو التعدي أو الفعل الضار يتعذر فيه تحديد العمل أو الفعل محل المسؤولية، وحتى لو تم اللجوء إلى الفنيين والخبراء المختصين والعاملين في هذا المجال، الأمر الذي يترتب عليه صعوبات بالغة في معرفة المخالفين والحصول على إقرار منهم حول مسؤوليتهم عن هذا الأفعال أو الاعتداءات أو المخالفات غير القانونية، وبالذات إذا كان هذا الهجوم السيبراني، قد تجاوز حدود الدولة الواحدة، بإحداث أضرر إلكترونية في دولة أخرى.

2. خصوصية الضرر السيبراني

الأذى الناتج عن الهجمات السيبرانية الذي أدى إلى الاخلال بمصلحة مشروعة سواء كانت معنوية أو مادية أو بمصلحة مشروعة أو بحق من حقوقه (العربي، 59ص،2007)، يعتبر الركن الثاني لقيام المسؤولية المدنية التقصيرية بسبب الأفعال أو الهجمات السيبرانية، حيث يرتبط بهذا الضرر مقدرًا التعويض الذي قد يصعب تقديره بسبب عدم وجود قواعد قانونية واضحة لتقديره ولاثباته بنفس الوقت نظرًا للخصائص التالية:

- أنه ضرر شخصي وغير شخصي وغير مباشر: أي أنه ضرر عيني يلحق بالبيئة الإلكترونية وشبكة الإنترنت ثم بعد ذلك يلحق بالأشخاص وبالأموال.
- أنه ضرر آني وغير آني: أي أن نتائجه قد لا تظهر مباشرة في بعض أنوع الهجمات إلا أنه في بعض أنواع الهجمات الأخرى فإن نتائجه تظهر في أغلب الأحيان في الحال، حيث لا تظهر نتائجه في زمن معين، بل قد يظهر بعد أيام أو أشهر وفي بعض الأحيان بعد سنوات.
- أنه ضرر يتحقق من نشاط غير مشروع: حيث أن غالبية النشاطات الناتجة عن الهجمات السيبرانية، تجد مصدرها في نشاط غير مسموح، إن إنهاء النزاع في دعوى المسؤولية يتطلب بخصوص الدعاوى ذات العنصر الأجنبي حل مشكلة تنازع القوانين؛ في ظل وجود العديد من الأنظمة القانونية التي تدعي الحاق في التطبيق على المنازعة: قانون الدولة التي تم فيها الهجوم السيبراني، قانون الدولة التي تحقق فيها الضرر، قانون الدولة التي ينتمي إليها المدعي والمدعى عليه بجنسيته، قانون وقوع الفعل الضار، قانون محل وقوع الفعل المنشئ للالتزام.

وبعد أن قام الباحث في المبحث الأول دراسة وتحديد مفهوم الهجوم السيبراني من خلال تحديد التعريفات الخاصة به وبيان صوره وأشكاله ثم الحديث عن خصائصها من أجل الوصول إلى الطبيعة القانونية للهجمات السيبرانية، ونوع المسؤولية المدنية من أجل تحديد القانون الواجب التطبيق على الأضرار النانجة عن هذه الأعمال غير المشروعة وهذا ماسيتم الحديث عنه تاليًا:

المبحث الثاني: تحديد القانون الواجب التطبيق على الضرر الناتج عن الهجمات السيبرانية

إن الخصائص التي يتميز به الفضاء الإلكتروني ساهم إلى حد كبير في اتساع الهجمات السيبرانية (الفتلاوي، 2016،ص 615-617)، وسهولة اختراقها بسبب ضعف شبكات الإنترنت والمعلومات (الموصلي، 2021، ص1)، بالإضافة إلى ضعف القدرة على معرفة هوية مرتكبي هذه الهجمات وإمكانية تحديد مكان وموقع صاحبها، وعليه أصبحت هذه الهجمات تشكل تهديد متزايدًا لمصالح الافراد، وقد تتعدى آثارها إلى الحاق ضررًا ماديًا ومعنويًا بسبب هذه الأفعال غير المباحة، مما يتطلب وجود قواعد قانونية قادرة وكافية لتحديد مسالة التعويض عن الأضرار والخسائر التي تلحق الأفراد والمنشأت الخاصة والعامة جراء هذه الهجمات السيبرانية، ذلك أن إقرار جزاءات قانونية لمرتكبي الهجمات السيبرانية إداريًا وجنائيًا وحتى دوليًا، غير كافي وفعال للتصدي لكل مظاهر التعدي السيبراني، مما أدى إلى العمل على إيجاد وسائل تكفل التعويض عن الأضرار الناتجة عن هذه الهجمات السيبرانية، ذلك أن القيمة النفعية للجزاءات الدولية والجنائية أو الإدارية، ستنهار إن لم يوجد نظام قانوني هدفه تدارك مثالب الأنظمة الحماية السيبرانية الردعية منها والوقائية، وذلك لا يتم الوصول إليه إلا من خلال أعمال الحماية المدنية للبيئة الإلكترونية، من خلال دعوى المسؤولية المدنية التقصيرية من أجل تعويض المتضرر عن الأضرار الناشئة عن الهجمات السيبرانية.

ولكن بالنظر لفكرة خصوصية الضرر السيبراني ذي الطابع الانتشاري؛ فإن الغالب إن تمتد آثاره خارج حدود الدولة الواحدة، بأن يتم إحداث الهجوم السيبراني في دولة، بينما تكون نتيجته الضارة التي تمس بالأشخاص والممتلكات في دولة أخرى، الأمر الذي يثير العديد من الإشكاليات النوعية الجديدة بشأن الاختصاص التشريعي (القانون الواجب التطبيق عليها) وتكون قواعد القانون الدولي الخاص هي واجبة الأعمال.

المطلب الأول: الحلول التشريعية لتحديد القانون الواجب التطبيق على الضرر الناتج عن الهجمات السيبرانية

إن الخصائص التي يتميز به الفضاء الإلكتروني ساهم إلى حد كبير في اتساع الهجمات السيبرانية (الفتلاوي،2016،ص615-617)، وسهولة اختراقها بسبب ضعف شبكات الإنترنت والمعلومات (نور،2001،ص1)، بالإضافة إلى ضعف القدرة على معرفة هوية مرتكبي هذه الهجمات وإمكانية تحديد مكان وموقع صاحبها، وعليه أصبحت هذه الهجمات تشكل تهديدًا متزايدًا لمصالح الافراد، وقد تتعدى آثارها إلى الحاق ضررًا ماديًا ومعنويًا بسبب هذه الأفعال غير المباحة، مما يتطلب وجود قواعد قانونية قادرة وكافية لتحديد مسالة التعويض عن الأضرار والخسار التي تلحق الأفراد والمنشآت الخاصة والعامة جراء هذه الهجمات السيبرانية.

إن إقرار جزاءات قانونية لمرتكبي الهجمات السيبرانية إداريا وجنائيا وحتى دوليا، غير كافي وفعال للتصدي لكل مظاهر التعدي السيبراني، مما أدى إلى العمل على إيجاد وسائل تكفل التعويض عن الأضرار الناتجة عن هذه الهجمات السيبرانية، ذلك أن القيمة النفعية للجزاءات الدولية والجنائية أو الإدارية، ستنهار إن لم يوجد نظام قانوني هدفه تدارك مثالب الأنظمة الحماية السيبرانية الردعية منها والوقائية، وذلك لا يتم الوصول إليه إلا من خلال أعمال الحماية المدنية للبيئة الإلكترونية، من خلال دعوى المسؤولية المدنية التقصيرية من أجل تعويض المتضرر عن الأضرار الناشئة عن الهجمات السيبرانية.

ولكن بالنظر لفكرة خصوصية الضرر السيبراني ذي الطابع الانتشاري؛ فإن الغالب أن تمتد آثاره خارج حدود الدولة الواحدة، بأن يتم إحداث الهجوم السيبراني في دولة، بينما تكون نتيجته الضارة التي تمس بالأشخاص والممتلكات في دولة أخرى، الأمر الذي يثير العديد من الإشكاليات النوعية الجديدة بشأن الاختصاص التشريعي (القانون الواجب التطبيق عليها) وتكون قواعد القانون الدولي الخاص هي واجبة الأعمال.

أولًا: اختصاص القانون المحلي

تخضع المسؤولية المدنية في القانون الخاص الأردني إلى القانون المحلي وفق مانصت عليه الفقرة الأولى من المادة (22) من القانون المدني الأردني: "يسري على الالتزامات غير التعاقدية قانون البلد الذي وقع فيه الفعل المنشئ للالتزام....." وقد اخذت بهذا الاتجاه العديد من التشريعات منها المصري والسوري، حيث أن الأخذ بهذا الاتجاه كان معمولًا به منذ القرون الوسطى، فقد استقرء هذا الاتجاه على اعتبار ضابط الاسناد الأصيل في ما يتعلق بمجال المسؤولية التقصيرية هو مكان وقوع الواقعة المنشئة للالتزام (منصور، 1956-1957، ص،326)، ويستند هذا التطبيق على العديد من المبررات القوية والهامة؛ والتي منها أن قانون المكان الذي وقع فيه الإخلال بالسلامة العامة أو بالأمن، وإحداث فيها السبب المنشئ للالتزام الذي ترتب عليه التعويض هو القانون الواجب التطبيق، ذلك أن القانون وجد من أجل ردع الفعل الضار قبل اللجوء إلى التعويض، لذلك فإنه من الطبيعي أن يتم اللجوء إلى هذا الضابط، كذلك فإن هذا القانون هو الأقدر على بيان فيما إذا تم مخالفة القواعد القانونية، وبيان فيما إذا تحققت عناصر المسؤولية التقصيرية، وهذا الضابط الوحيد الذي يعتبر حيادي مقارنة مع الضوابط الأخرى كجنسية الفاعل أو المتضرر، أو مكان إقامتها، بالإضافة إلى أن تطبيق مكان وقوع الفعل الضار يحقق العدالة والتوازن بين حقوق المتضرر ومرتكب الفعل، كما أن سهولة الوصول إلى القانون الواجب التطبيق وسهولة الإثبات وفعاليته تعطيه تميزًا (المصري ، 2021، ص197-198)،حيث يعتبر مركز الثقل فيها هو مصدر العلاقة القانونية الناتجة عن الفعل الضار أو سببها، ذلك أنه لا يتم النظر إلى أطراف الواقعة أو موضوعها إنما يتم النظر إلى مصدرها أو سببها، وهو الفعل الضار (الروابي، 2005، ص57) بالإضافة إلى أن اللجوء إلى هذا الضابط يحقق استقرار للمعاملات كما أنه يؤدي إلى محاربة الغش نحو الاختصاص، ويحقق وحدة القواعد القانونية بين النظم القانونية، التي تلبي توقعات الأطراف من حيث علمهم بالقانون الواجب التطبيق (يمنية ، 2022، ص898). وقد أخذت العديد من الاتفاقيات الدولية (اتفاقية لاهاي بشأن القانون الواجب التطبيق على الحوادث المرورية، 1971المادة 3 منها وكذلك فعلت العديد من التشريعات (اتفاقية لاهاي بشأن القانون الواجب التطبيق على الحوادث المرورية، 1971).

ثانيًا: شروط تطبيق القانون المحلي

1. أن يكون كلًا من قانون القاضي الناظر في النزاع والقانون الواجب التطبيق بناء على ضابط الاسناد ينصا على عدم مشروعية الفعل، فإنه تنعقد المسؤولية في هذه الحالة بمفهوم المخالفة لنص المادة (22) في الفقرة الثانية بقولها لا تسري أحكام الفقرة السابقة بالنسبة إلى الالتزامات الناشئة عن الفعل الضار على والوقائع التي تحدث في الخارج وتكون مشروعة في البلد الذي وقعت فيه" القانون الليبي (المادة 21 الفرع الأول)، والسوري (المادة 22 الفرع الأول)، والمصري (المادة 21 الفرع الأول)، والإماراتي (المادة 20 الفرع الأول)، بينما لا تنعقد المسؤولية إذا كان الفعل مشروع في الأردن وغير مشروع في دولة قانون المحلي فإنه لايتم تطبيقه في هذه الحالة وإنما يتم إعمال قانون القاضي الناظر بالنزاع.
2. أن تكون جميع عناصر الواقعة القانونية التي يتم الاستناد إليها لتحديد القانون الواجب التطبيق تتجمع في مكان واحد، فإذا وقع الضرر وترتب على الضرر عليه سيتم في هذه الحالة تطبيق ضابط الإسناد، ولكن إذا لم يتحقق هذا الشرط بسبب توزع عناصر الإسناد في أكثر من دولة، ففي مجال تحقق المسؤولية عن الأضرار السيبرانية، حيث يتم القيام بارتكاب الفعل بدولة ما ويتحقق الضرر بدولة أخرى، فهنا تظهر إشكالية صعوبة تطبيق هذا الضابط (بلقاسم،2001، ص 334). فاذا لم تتحقق الشروط السابقه وتوزعت عناصر الإسناد في العديد من الدول، فإن الحالة هنا تحقق المسؤولية عن الأضرارالناتجة عن الهجمات السيبرانية قد يتم الفعل في دولة ما وتظهر آثاره في العديد من الدول، نتيجة لذلك ظهرت العديد من الاتجاهات الفقهية التي عملت على تحديد القانون الواجب في حال لم تتوافر الشروط السابقة ومن هذه الاتجاهات نظرية تطبيق قانون مكان تركيز الفعل الضار؟ نظرية مكان وقوع الضرر وسيتم بيان هذه الاتجاهات الفقهية تاليًا.

المطلب الثاني: الحلول الفقهية لتحديد القانون الواجب التطبيق على الضرر الناتج عن الهجمات السيبرانية

بعد أن تم الحديث في المطلب الأول عن الحلول التشريعية لبيان وتحديد القانون الواجب التطبيق وجدنا أنها غير كافية لتحديد القانون الواجب التطبيق على الأضرار الناشئة عن الهجمات السيبرانية مما يتطلب استعراض وبيان الحلول الفقهية لبيان القانون الواجب تاليًا:

أولًا: قانون الدولة التي تحقق فيها الضرر

تقوم هذه النظرية على مفاده أن الهدف والغاية من النظام القانوني للمسؤولية المدنية، هو التعويض المدني، فبدون الضرر الذي يعد من الشروط الواجب توافرها لقيام المسؤولية المدنية التقصيرية لا يمكن المطالبة بالتعويض، وبالتالي إذا لم يلحق المدعي من هذا الهجوم السيبراني ضرر فإن المصلحة تنتفي في هذه الحالة، كما أن أغلب التشريعات جعلت تقدير قيمة التعويض عن الضرر مرتبطة بوقت تحقق الضرر بالإضافة إلى تقدير قيمة التعويض عن الضرر (سلامة،احمد عبد الكريم،2000،ص 1196)، وفي هذا الاتجاه استجابة لروح العامة في تنظيم المسؤولية المدنية عن أضرار الهجمات السيبرانية العابره للحدود، حيث تنعقد المسؤولية بمجرد تحقق الضرر وبالتالي فهي مسؤولية موضوعية قوامها تحقق الضرر، الأمر الذي يعني أنه لا يشترط القيام بنشاط غير مشروع أو القيام بفعل غير مشروع، أو إثبات ذلك من طرف المضرور.

بالرجوع أيضًا إلى الهدف والغاية التي وجد من أجلها القانون في تنظيم المصالح المتعارضة المتضاربة فإن القانون الذي اختلت في ظلها هذه المصالح قادرة على إعادة هذا التوازن بين هذه المصالح (الداوودي، غالب،2001،ص141). وقد اكد أيضًا على هذا الاتجاه التنظيم الأوروبي في الفقرة الأولى من المادة 4 رقم 2007/864 الخاص بالقانون الواجب التطبيق على الالتزامات غير التعاقدية.حيث تنص هذه الفقرة على أنه:" إذا لم يوجد نص خاص في هذا التنظيم يخالف ذلك، فإن القانون الواجب التطبيق على الالتزام غير التعاقدي الناشئ عن الفعل الخاطئ هو قانون البلد الذي تحقق فيه الضرر بغض النظر عن البلد الذي وقع فيه الفعل الضار وبغض النظر عن البلد الذي تحققت فيه الاثار غير المباشرة لهذا الفعل(of the European Union https://eur-lex.europa.eu/legal-content/EN/TXT(ISSN 1725-2555 /وقد أخذ بهذا الاتجاه العديد من التشريعات من السويسري لعام 1987 في المادة 133 الفرع الثاني، البرتغالي لعام 1966(المادة 45 الفرع الثاني).

ثانيًا: قانون الدولة التي تقع فيه أكبر عناصر العلاقة المشوبة بعنصر أجنبي.

في هذا الاتجاه يتم اللجوء إلى تحديد القانون الواجب التطبيق خلاف للنظريات السابقه من خلال الاعتماد على جمع اكبر عدد ممكن من عناصر العلاقة، فإذا كان مرتكب الهجمات السيبرانية والمتضرر من جنسية واحد، ويقيمان بنفس الوقت في مكان واحد رغم أن مكان ارتكاب الجريمة في دولة والضرر في دولة أخرى، فإن عنصري الإقامة والجنسية يشكلان نقاط إسناد أكثر أهمية من مكان وقوع الفعل الضار(المصري، محمد، 2022، ص198).

الخاتمة:

أولًا: النتائج

خلصت الدراسة إلى مجموعة من النتائج أهمها ما يلي:

- لقد فرض التطور على البشرية التعامل من خلال هذه البيئة الإلكترونية.
- أفرز هذا التطور الإلكتروني مجموعة من الجوانب الإيجابية وأيضًا بعض الثار السلبية.
- تعد الهجمات السيبرانية أحد أهم المصطلحات المستحدثة في البيئة الإلكترونية.
- عدم وجود قواعد قانونية أو دراسات تتحدث عن هذا المصطلح الجديد بشكل كافي.
- وجود اختلاط في المصطلحات مابين الهجمات السيبرانية والجرائم السيبرانية.
- اختلاف الطبيعة القانونية للهجمات السيبرانية باختلاف فاعل ومرتكب الهجوم والجهة التي قامت بالفعل.
- وقوع الأضرار سواء كانت مادية ومعنوية بسبب هذه الأفعال أو الهجمات غير المشروعة.
- تعدد صور وأشكال الهجمات السيبرانية، مما يتطلب قواعد قانونية خاصة بطبيعة هذه الأفعال.
- عدم وجود قواعد قانونية تحدد القانون الواجب التطبيق على الأضرار الناشئة عن الهجمات السيبرانية.

ثانيًا: التوصيات

وبناءً على النتائج التي خلصت إليها الدراسة فإننا نوصي بما يلي:

- نوصي المشرع إيجاد القواعد القانونية الكافية للتعامل مع هذه البيئة الإلكترونية.
- البحث في الآثار السلبية بشكل كافي من خلال اجراء العديد من الدراسات عن هذه الآثار السلبية ووضع القواعد القانونية الكافة لهذه الإشكاليات.
- إيجاد القواعد الكافية لبيان وتنظيم وتوضيح كافة المصطلحات المتعلقة بهذه المصطلحات.
- العمل إزالة الغموض والفروق بين مصطلحي الجرائم السيبرانية، والهجمات الإلكترونية.

المراجع:

أولًا: المراجع العربية

بلقاسم، اعراب. (2001). *القانون الدولي الخاص الجزائري: تنازع القوانين*. دارهومة.

الداوودي، غالب. (2001). *القانون الدولي الخاص، الكتاب الأول في تنازع القوانين وتنازع الاختصاص القضائي الدولي وتنفيذ الاحكام الأجنبية*. الطبعة الثالثة، دار وائل للطباعة والنشر.

الروبي، محمد. (2005). *تنازع القوانين في مجال الالتزامات غير التعاقدية*. دار النهضة العربية.

الزرو، حسن. (2007). *الفضاء المعلوماتي*. مركز دراسات الوحدة العربية.

سلامة،احمد عبد الكريم. (2000). *القانون الدولي الخاص النوعي: الإلكتروني، السياحي، البيئي*. الطبعة الأولى، دار النهضة العربية.

السمحان، منى عبدالله. (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. *مجلة كلية التربية، جامعة المنصورة* العدد2020،11.

العربي، بلحاج. (2007). *النظرية العامة للالتزام في القانون المدني الجزائري (الواقعة القانونية)*. ج2، ديوان المطبوعات الجامعية.

الفتلاوي، احمد عبيس نعمة.(2016). الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر. *مجلة المحقق المحلي للعلوم القانونية والسياسية*، العدد4، جامعة بابل، ص 615-617.

فهمي، عبد القادر. (2018). الحروب التقليدية وحروب الفضاء الإلكتروني؛ دراسة مقارنة في المفاهيم وقواعد الاشتباك. *مجلة العلوم القانونية والسياسية*. المجلد (16). السنة الثامنة. العدد (2).

قورة، نائلة. (2005). *جرائم الحاسب الالي الاقتصادية*. منشورة الحلبي الحقوقية.

المصري، محمد وليد. (2021). *الوجيز في شرح القانون الدولي الخاص، دراسة مقارنة للتشريعات العربية والقانون الفرنسي*. دار الثقافة للنشر والتوزيع.

الموصلي، نور أمير. (2021). *الهجمات السيبرانية في ضوء القانون الدولي الإنساني*. بحث مقدم استكمالا لمتطلبات نيل درجة ماجستير التأهيل والتخصص في القانون الدولي الإنساني، الجامعة الافتراضية السورية .

يمنية، قصير.(2022). دور القانون الدولي الخاص في فض منازعات المسؤولية المدنية الناشئة عن أضرار التلوث البيئي العابر للحدود. *مجلة العلوم القانونية والاجتماعية* جامعة زيان عاشور باجلفة، المجلد07-العدد03.

ثانيًا: المراجع الأجنبية:

J. Slobbe. (2012). *Hacktivists: Cyberterrorists or Online Activists?"* http://arxiv.org/pdf/1208.4568.pdf

JO de Iunion europeenne, L199/40 du 31-7-2007, p.1.k.

ثالثًا: المواقع الإلكترونية

https://www.it-pillars.com/ar/blog

https://bhuth.ae/ar/publication/cyber-attacks-what-we-know-and-what-we-can-do-about-it

https://www.it-pillars.com/ar/blog

http://compnetworking.about.com/od/networksecurityprivacy/g

رابعًا: القوانين

القانون المدني الأردني رقم (43) لسنة 1976.

قانون الامن السيبراني رقم 16 (2019).

القانون الليبي(المادة 21 الفرع الأول)، والسوري (المادة 22 الفرع الأول)، والمصري (المادة 21 الفرع الأول)، والإماراتي (المادة 20 الفرع الأول).

خامسًا: الاتفاقيات

اتفاقية لاهاي بشان القانون الواجب التطبيق على حوادث الطرق المبرمة عام 1971، والتي دخلت حيز النفاذ عام 1971، والتي دخلت حيز النفاذ عام 1975(المادة الثالثة منها).

سادسًا: ترجمة المراجع العربية

Al-Daoudi, G. (2001). *Private International Law, Volume I: Conflict of Laws, International Jurisdiction Conflicts, and Recognition of Foreign Judgments.* 3rd Edition, Dar Wael Publishing. [In Arabic]

Al-Masry, M. W. (2021). *A Brief Explanation of Private International Law: A Comparative Study of Arab Legislation and French Law.* Dar Al-Thaqafa for Publishing and Distribution. [In Arabic]

Al-Mawsili, N. A. (2021). *Cyber Attacks in Light of International Humanitarian Law.* A dissertation submitted for the fulfillment of the Master's degree in International Humanitarian Law, Syrian Virtual University. [In Arabic]

Al-Samhan, M. A. (2020). *Requirements for Achieving Cybersecurity for Administrative Information Systems at King Saud University.* Journal of the Faculty of Education, Mansoura University, Issue 11, 2020. [In Arabic]

Al-Zaru, H. (2007). *The Informational Space.* Center for Arab Unity Studies. [In Arabic]

Belhaj, A. (2007). *The General Theory of Obligations in Algerian Civil Law (Legal Facts).* Volume 2, University Publications Office. Al-Fatlawi, Ahmed Abis Nima. (2016). *Cyber Attacks: Their Concept and the International Responsibility Arising Therefrom in Light of Contemporary International Regulation. Journal of Al-Muhaqqiq Al-Hilli for Legal and Political Sciences*, Issue 4, University of Babylon, pp. 615-617. [In Arabic]

Belkacem, A. (2001). *Algerian Private International Law: Conflict of Laws.* Dar Houma. [In Arabic]

El-Roubi, M. (2005). *Conflict of Laws in the Field of Non-Contractual Obligations.* Dar Al-Nahda Al-Arabia. [In Arabic]

Fahmy, A. (2018). *Traditional Wars and Cyber Wars: A Comparative Study of Concepts and Rules of Engagement. Journal of Legal and Political Sciences,* Vol. 16, 8th Year, Issue 2. [In Arabic]

Qoura, N. (2005). *Economic Computer Crimes.* Halabi Legal Publications. [In Arabic]

Salama, A A. (2000). *Specialized Private International Law: Electronic, Tourism, and Environmental.* 1st Edition, Dar Al-Nahda Al-Arabia. [In Arabic]

Yamaniya, K. (2022). *The Role of Private International Law in Resolving Civil Liability Disputes Arising from Transboundary Environmental Pollution Damages.* Journal of Legal and Social Sciences, Ziane Achour University of Djelfa, Vol. 07, Issue 03. [In Arabic]