مجلة النور للدراسات القانونية

https://jnls.alnoor.edu.iq/

المسؤولية المدنية عن الجرائم السيبرانية في العلاقات الخاصة الدولية (دراسة تحليلية في ضوء تنازع القوانين)

رجاء حسين عبد الأمير

جامعة القاسم الخضراء/ كلية العلوم

معلومات المقال

تاريخ المقال:
تم الاستلام: 5 نيسان 2025
تم المراجعة: 14 نيسان 2025
تم القبول: 5 ايار 2025

الكلمات المفتاحية:
الضرر
السيبراني
العابر للحدود
القانون الواجب التطبيق
المحكمة المختصة

تواصل:
أ.م.د. رجاء حسين عبد الأمير
rajaa_hussain@uoqasim.edu.iq

المستخلص

تؤثر التكنولوجيا على العلاقات القانونية العابرة للحدود الوطنية، إذ أدت إلى زيادة عدد الدعاوى القضائية العابرة للحدود الوطنية المتعلقة بالمسؤولية المدنية الناشئة عن الجرائم السيبرانية، الأمر الذي يفرض تحديات جديدة على القانون، وخاصة القانون الدولي الخاص، يدرس هذا المجال من القانون مسائل الاختصاص القضائي المطبق، واختيار القانون الواجب التطبيق، يهدف هذا البحث إلى تحديد السياسات والأطر المعيارية القائمة لتحديد الاختصاص القضائي المطبق واختيار القانون فيما يتعلق بالمسؤولية المدنية الناشئة عن الجرائم السيبرانية، كما تبرز مشكلة التركيز المكاني للمسؤولية المدنية عن الأضرار التي تسببها الجرائم السيبرانية، أي القانون الواجب التطبيق على تلك الأضرار، وسيتم تحليل قوانين نصوص القوانين مدى ملائمتها لهذا التطور ومن خلال منهجية تحليلية، يركز تحليلنا على المسائل المتعلقة بالاختصاص القضائي أي المحكمة المختصة بنظر هذه المنازعات، والقانون المطبق أي قانون يمكن تطبيقه على العلاقات القانونية ذات العنصر الأجنبي، واقترحنا أن يكون اختصاص المحكمة الأقرب إلى النزاع والقانون الأكثر ارتباطا به، لذلك نعتقد أن قانون الدولة التي يطلب فيها الحماية هو القانون الواجب التطبيق، لأن هذا القانون غالبا ما يكون قانون الدولة الأكثر ارتباطا بالعلاقة القانونية

DOI: https://doi.org/10.69513/jnfls.v2.i2.a3, ©Authors, 2025, College of Law, Alnoor University.
This is an open access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

Civil Liability Arising from Cybercrimes in International Private Relations: An Analytical Study in the Context of Conflict of Laws

Rajaa. H. Abdulameer

Al-Qasim Green University, Babylon 51013, Iraq/ College of Science

Abstract

Technology affects transnational legal relations, as it has led to an increase in the number of transnational lawsuits related to civil liability arising from cybercrimes, which imposes new challenges on the law, especially private international law. This area of law studies the issues of applicable

jurisdiction and the choice of applicable law. This research aims to identify the existing policies and normative frameworks for determining applicable jurisdiction and the choice of law in relation to civil liability arising from cybercrimes. The laws of the texts of the laws will be analyzed to what extent they are appropriate for this development. Through an analytical methodology, our analysis focuses on issues related to jurisdiction, i.e. the court competent to hear these disputes, and the applicable law, i.e. the law that can be applied to legal relations with a foreign element.

Keywords: harm, cyber, transnational, applicable law, competent court.

المقدمة

أن مقتضيات البحث العلمي في هذا الموضوع تلزمنا تناول الأمور الآتية:

أولاً/ أهمية البحث

عند دراسة موضوع المسؤولية المدنية عن الجرائم السيبرانية في العلاقات الخاصة الدولية، فأننا تناول أهم أحد ابرز مجالات القانون الدولي والمتمثل في **تنازع الاختصاص القضائي الدولي** لتحديد المحكمة المختصة، و**تنازع القوانين**، وينبغي إيلاء مسألة تحديد المحكمة المختصة والقانون الواجب التطبيق على المسؤولية المدنية الناشئة عن الجرائم السيبرانية المرتكبة عبر شبكة المعلومات اهتماماً تشريعياً أكبر، لأن معظم تلك الجرائم المرتكبة ذا ت طابع دولي، مما يستدعي اعتماد معيار خاص كمعيار قانون الدولة المطلوب فيها الحماية هو الأفضل لأنه يعطي حماية أكبر لمصالح المتضرر، كما يحقق الحياد والتوازن المطلوبين بين الأطراف.

ثانياً/ مشكلة البحث

تتخذ الجرائم السيبرانية بعد دولياً عندما تتخلل العلاقات القانونية عنصر أو أكثر من العناصر الأجنبية، وهذا يثير تحديات قانونية تتمثل في تحديد ما إذا كانت المحاكم تتمتع بالسلطة القضائية على الأنشطة التي تتم على شبكة الإنترنت، ومتى يمكن أن يتم ذلك لن يكون صعباً إذا كانت شبكة الإنترنت محصورة في منطقة جغرافية واحدة، أو إذا كانت قابلة للتقسيم بشكل واضح على طول الحدود الإقليمية إلى شبكات محلية متميزة، ولكن شبكة الإنترنت بطبيعتها دولية فهي لا تحترم الاختصاص المحلي والوطني، وبالتالي فإن التحدي يكمن في وضع قواعد تعمل بسلاسة عبر الحدود المحلية والوطنية والدولية، كما تبرز مشكلة التركيز المكاني للمسؤولية المدنية عن الأضرار التي تسببها الجرائم السيبرانية، أي القانون الواجب التطبيق على تلك الأضرار.

ثالثاً/ منهجية البحث

أن المنهج الأنسب لمعالجة إشكالية البحث، هو المنهج الوصفي التحليلي، من خلال استعراض النصوص وتحليلها، ومدى نجاعة تلك النصوص والأخذ بها، وهل تعد كافية أم نحن بحاجة لإيجاد نصوص جديدة؟، كذلك الاستعانة بالدراسة المقارنة، نظراً لما تتطلبه طبيعة الموضوع.

رابعاً / خطة البحث

استنادا إلى ما سبق من منهج ومنهجية ومعطيات ستكون هيكلية الدراسة مقسمة إلى ثلاثة مطالب، نتناول في المطلب الأول تعريف الجرائم السيبرانية، ونتناول في المطلب الثاني الاختصاص القضائي الدولي بشأن المسؤولية المدنية الناشئة عن الجرائم السيبرانية، ونتناول في المطلب الثالث القانون الواجب التطبيق بشأن المسؤولية المدنية الناشئة عن الجرائم السيبرانية.

المطلب الأول:

تعريف الجريمة السيبرانية

ابتداءً لا بد من بيان المقصود بالسيبرانية، مصطلح السيبرانية هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وتشير كلمة "cyber" إلى أنها لفظة يونانية الأصل مشتقة من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم "governor"وتجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي (norbert wieners) وذلك للتعبير عن التحكم الآلي، فهو الأب الروحي المؤسس للسبرنيتيقية من خلال مؤلفه الشهير (السيبرنتيقية أو التحكم والاتصالات في "الحيوان والآلة") وأشار في كتابه إلى أن السبرنتيقية هي التحكم والتواصل عند الحيوان والآلة والإنسان والآلة ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب[1].

الجريمة السيبرانية تعد من الجرائم التي تباينت تسميتها عبر المراحل الزمنية، بسبب تطورها، ففي البداية كانت جريمة اساءة استعمال الكمبيوتر، ثم جريمة احتيال الكمبيوتر، والجريمة المعلوماتية، والجريمة التقنية العالية، جرائم الهاكرز، إلى الجرائم السيبرانية[2].

وعرفت الجريمة السيبرانية بعدة تعريفات، منها، (هي التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة على كمبيوتر آخر أو أحد وسائل التقنية الحديثة ، مع ضرورة توفر شبكة اتصال فيما بينهما)[3].

أو هي (كل نشاط أجرامي يؤدي فيه نظام الآلي الحاسوب دوراً لإتمامه، على أن يكون هذا الدور على قدر من الأهمية)[4]، أو هي، (هي السلوك غير المشروع أو المنافي للأخلاق أو غير المسموح به المرتبط بالشبكات المعلوماتية العالمية فهي جر ائم العصر الرقمي التي تطال المال والمعرفة والثقة والسمعة وتنفذ كلها عن طريق التقنية)[5].

أو هي، (أي سلوك غير قانوني أو غير أخلاقي أو غير مصلح يتعلق بالمعالجة الآلية للبيانات أو نقلها أو الاعتداء عليها، أو (هي فعل خاطئ أو غير قانوني من قبل مجرم سيتم تحديده بموجب القانون كعقوبة جنائية أو مدنية أو تدبير احترازي، يؤثر على المعرفة والاستخدام والثقة والأمن الوطني والسيادة الوطنية والربح والمال والسمعة والهيبة)[6].

وتقع الجرائم السيبرانية أما على البيانات فتسبب اضرار مادية ومعنوية لمالكي تلك البيانات، وتحدث عند اختراق النظام المعلوماتي عن طريق الدخول غير المصرح، وقيام الجاني بالاطلاع على البيانات واستغلالها، أو سرقتها أو تزويرها أو تخزينها على نحو غير مشروع، أو اساءة استعمالها، وقد تقع على الأشخاص، كجرائم التشهير والابتزاز واساءة السمعة أو الاعتداء على حقوق الملكية الفكرية والادبية للمؤلفين[7].

تتميز الجرائم السيبرانية عن الجرائم التقليدية بعدة خصائص تتمثل في لأنها جرائم لا تعرف الحدود الجغرافية للدول، لارتباط العالم بشبكة واحدة، ويمكن للجاني تنفيذ جريمته وهو في دولة بعيدة كل البعد عن المجني عليه وهذا قد يسبب إشكاليات لدى الاختصاص القضائي من حيث التحقيق والمحاكمة، وذلك تبعا لتعقيد الإجراءات التي تحكمها الاتفاقيات والمعاهدات والعلاقات الدولية، والتنازع فيما بينهما على القانون الواجب التطبيق[8].

كما انها تتميز بصعوبة الكشف عنها، ويعود ذلك إلى قدرة الجاني على محو الدليل في أقل من ثانية، فضلاً عن ذلك عادة ما ترتكب الجرائم السيبرانية في الخفاء مع مجهولية شخصية الجاني وعدم معرفة موقعه في كثير من الأحيان[9].

المطلب الثاني:
الاختصاص القضائي الدولي بشأن المسؤولية المدنية الناشئة عن الجرائم السيبرانية

وفقاً للقواعد التقليدية في القانون الدولي الخاص أن الجريمة وما ينشئ عنها من اضرار سواء كانت مادية أو معنوية، تخضع لمحكمة محل وقوع الفعل، استناداً لمعايير الإقليمية، الذي يقوم على اعتبارات السيادة، وأن الاختصاص القضائي مظهراً من مظاهر السيادة، كما أن الأصل براءة ذمة المدعى عليه، كما أن معيار الإقليمية يحقق الصلة الجدية والحقيقية ما بين الدعوى ودولة المحكمة، فيكون الاختصاص القضائي الدولي للمحكمة مبني على أسباب قوية وهو ما يمنح الأحكام قوة النفاذ الدولي، أي ستكون الأحكام قابلة للاعتراف والتنفيذ في الخارج[10].

وقد نصت المادة (7) لائحة الاتحاد الأوروبي رقم (2012/1215) على أنه، (يجوز مقاضاة شخص مقيم في دولة عضو في دولة عضو أخرى ... في المسائل المتعلقة بالضرر أو الجنحة أو شبه الجنحة، في محاكم المكان الذي وقع فيه الحدث الضار أو قد يقع فيه).

كانت هذه القاعدة المتعلقة بالمسؤولية التقصيرية مهمة في قضيتين حديثتين متعلقتين بالإنترنت. ففي قضية شركة (ميكلر ميديا) ضد شركة (دي سي كونغرس جي إم بي إتش)، قضت محكمة المستشارية الإنجليزية بأنها تتمتع بالاختصاص للنظر في نزاع أقامته شركة أمريكية وفرعها الإنجليزي ضد شركة ألمانية زعمت أن المدعى عليه ارتكب المسؤولية التقصيرية المتمثلة في "التظاهر" بإساءة استخدام اسم تجاري ("عالم الإنترنت") على موقع ويب على الإنترنت يمكن الوصول إليه من إنجلترا، وقد تولت محكمة فرنسية الاختصاص في قضية رابطة مكافحة العنصرية ومعاداة السامية ضد (ياهو)، عندما رفعت دعوى قضائية ضد (ياهو) بسبب نشر تذكارات نازية على صفحات ويب يمكن الوصول إليها من فرنسا، وزعمت (ياهو) أنها شركة أميركية وأن المواد التي نشرتها لم تكن مخالفة للقانون الأميركي، ورد القاضي بأن المواد كانت مخالفة لبند من بنود قانون العقوبات الفرنسي (الذي يسمح للشخص الخاص بمقاضاة شخص آخر في فرنسا باعتباره جنحة أو تقصيراً)، وخلص إلى أنه بما أن "الضرر وقع في فرنسا، فإن اختصاصنا القضائي مختص في هذه المسألة وفقاً للمادة (46) من قانون الإجراءات المدنية الجديد"[11].

السؤال الذي يطرح الآن ما مدى انطباق القاعدة التقليدية على الجرائم السيبرانية، فهل تخضع لمحل وقوع الفعل، تقع في اختصاص محكمة الدولة التي ارتكب الفعل الضار ضمن حدوها الإقليمية؟

يرى البعض من الفقه[12]، أن معيار الإقليمية غير كافياً لحل مشكلة الاختصاص القضائي الدولي في الجرائم السيبرانية، لطبيعة هذه الجرائم التي لا حدود لها، كما أن تأثيرها يتجاوز حدود مبدأ المكان المُجرم، إذ لا يوجد شرط مسبق للارتباط بين المكان الذي حدث فيه النشاط غير المشروع والمكان الذي وقعت فيه الأضرار، كما من السهل نقل موقع ويب من منطقة إلى أخرى، كذلك يمكن استضافة موقع ويب في منطقة واحدة ولكن يتم توجيهه إلى المستخدمين من موقع جغرافي آخر، كذلك لا يمكن تحديد مكان موقع ويب أو المستخدم.

وقد تبنت المحاكم الإنجليزية نظرية المحكمة غير الملائمة، إذ تعد المحاكم الإنجليزية غير مناسبة للنظر في المطالبة بالتعويض عن الجرائم السيبرانية، متى ما كانت هناك عوامل أكثر تتركز في إقليم دولة اجنبية أخرى، فلم يعد مكان وقوع الفعل كافياً لانعقاد الاختصاص للمحاكم الإنجليزية، ومن هذه العوامل محل تحقق الضرر، مركز اعمال المتضرر صلاته العائلية، ففي المملكة المتحدة عام 2015 قضية تتلخص وقائعها، أن المدعى عليه الذي ولد في الولايات المتحدة لكنه تخلى عن جنسيته في عام 2014 وعاش في اليابان، وكان مواطنا من سانت كيتس ونيفيس، قد شتم مواطن انجليزي في مقطع فيديو على يوتيوب وفي تغريدات، وكانت المادة التشهيرية المزعومة عبارة عن وصف المدعى عليه للمدعي بأنه مطور بيتكوين احتيالي، واستأنف المدعي قرار المحكمة العليا الإنجليزية بأن إنجلترا ليست بوضوح المكان الأكثر ملاءمة لرفع دعوى التشهير، نظرت المحكمة العليا في المادة (9) من قانون التشهير لعام 2013 والتي بموجبها سيكون للمحكمة ولاية قضائية إذا كانت "إنجلترا هي بوضوح المكان الأكثر ملاءمة لرفع دعوى فيما يتعلق بالبيان التشهيري المزعوم " يُقارن هذا بجميع الأماكن التي نشر فيها البيان، وأيدت محكمة الاستئناف الإنجليزية قرار المحكمة العليا وقررت أن أي ولاية في الولايات المتحدة تقبل الاختصاص القضائي على المطالبة، ستكون الاختصاص القضائي الأكثر ملاءمة في كل عام من الأعوام التي تناولتها القضية، كان عدد مشاهدي قناة اليوتيوب في الولايات المتحدة حوالي أربعة أضعاف عدد مشاهدي المملكة المتحدة كان هذا هو السبب الأول من ثمانية أسباب لاتخاذ قرار بأن إنجلترا ليست بوضوح المكان الأكثر ملاءمة لرفع الدعوى على الرغم من أن الأسباب ليست بالضرورة مرتبة بأي ترتيب من حيث الأهمية (ويتضمن المحكمة غير المناسب النظر في عدة عوامل، فإن أدلة قناة اليوتيوب تشير " بقوة" إلى أن إنجلترا ليست بوضوح المكان الأكثر ملاءمة في مزاعمه، بأنه كان لديه علاقة وثيقة ومستقرة بالمملكة المتحدة "، ادعى المدعي أن وصفه بالاحتيال أضر بسمعته داخل مجتمع رجال الأعمال في المملكة المتحدة الذين تعامل معهم في المقام الأول كما كان لديه معظم أقرانه في مجال الأعمال في المملكة المتحدة على الرغم من سمعته العالمية، رفضت المحكمة هذه الحجج وقررت أن أهم علاقاته كانت في الولايات المتحدة ، وبالنسبة للمدعي الذي لم يتم التناقض مع أدلته بشأن عمله في شركة بريطانية، وتوظيف موظفين من المملكة المتحدة، وارتباطه العائلي بإنجلترا، بدا موقف المحكمة ضيقا إلى حد ما، كان المدعي يسعى إلى التعويض عن الضرر الذي لحق بسمعته في إنجلترا، لكنه كان موجها في الأساس إلى رفع دعوى للمطالبة بالتعويض عن الضرر في الولايات المتحدة، حيث لم يكن يطالب بالتعويض عن الضرر الذي لحق بسمعته، قد يكون شرط قانون التشهير لعام 2013 برفع دعوى في الولاية القضائية الأكثر ملاءمة بوضوح أمرا صعبا ومع ذلك تأخذ

المحاكم في الاعتبار حقيقة مفادها أن الشرط قد لا يكون علما دقيقا عند النظر في مركز مصالح المدعي، وينطبق هذا بشكل خاص على المدعين المعروفين بشكل أفضل خارج إنجلترا، أو الذين يتمتعون بسمعة عالمية[13].

وقد ركزت المحكمة العليا الاسترالية، مبدأ مقتضاه تعد المحاكم الاسترالية مختصة بنظر التعويض عن الاضرار الناشئة عن الجرائم السيبرانية، إذا وقعت الاضرار في استراليا بغض النظر عن موقع ويب، ففي قضية تتلخص وقائعها بدأ المدعي رجل الأعمال الفيكتوري (جوزيف جوتنيك) إجراءات في المحكمة العليا الفيكتورية ضد دار النشر التجارية الدولية (داو جونز) مقرها في الولايات المتحدة، نشرت شركة (داو جونز) مقالاً بعنوان "المكاسب غير المقدسة" على موقع مجلة الأعمال كان النشر على الإنترنت محدودًا لأنه موقع مخصص للاشتراك فقط، زعم المقال أن السيد (جوتنيك) كان أكبر عميل لغاسل أموال ومتهرب ضريبي وتاجر مالي غير عادل، ادعى المدعي، كونه مقيمًا في فيكتوريا، أستراليا، أن المقال كان له تأثير سلبي أثرت سمعته بشكل كبير في فيكتوريا، إذ تم قراءة المقال التشهيري الذي تم نشره على الإنترنت من قبل سكان فيكتوريا في فيكتوريا، دفع المدعى عليه أن المقال المنشور على الإنترنت لم ينشر في فيكتوريا بل في الولايات المتحدة (نيوجيرسي)، وكان خادم الويب موقعه في ولاية فيكتوريا، لذلك قيل إن القضية يجب أن تنظر في ولاية نيوجيرسي ومع ذلك، مارست المحكمة العليا سلطتها على أساس الأسباب التالية، حدث النشر والضرر الذي صاب سمعته في فيكتوريا، قدم المدعي بلاغا يفيد بأن عددًا من سكان فيكتوريا قد دخلوا إلى الموقع الإلكتروني وقرأت المقال، وكان كافياً للمحكمة أن تعتبر أن المقال كان نشرت في فيكتوريا منذ أن تم تنفيذ عملية تنزيل المعلومات في فيكتوريا، وقد قضت المحكمة بأن البيان التشهيري قد تم نشره في فيكتوريا، حيث تم تنزيله وحيث تم نشره مطبوعا كما تم بيعها أيضًا، ثانيا، المدعي مقيم في فيكتوريا، ولديه أعماله مقره هنا وعائلته هنا، وحياته الاجتماعية والتجارية هنا.

يرى البعض من الفقه الأمريكي[14] وبما أن القانون الأميركي نظام قانوني عام، فإنه يتطور في المقام الأول من خلال الفقه القانوني وبعبارة أخرى، تشكل القرارات القضائية سوابق وترشد تطبيق وتفسير القانون في حالات مماثلة في المستقبل، ومن المبادئ الفقهية الأكثر استخداماً في الأنظمة القانونية ذات التقاليد الأنجلو أميركية، ما يسمى بالمبدأ القضائي غير المناسب، الذي ينص على أن المحكمة قد ترفض ممارسة اختصاصها على دعوى وفقاً لتحليل تقديري من أجل تجنب حل غير فعال أو غير عادل للدعوى على حساب الحكم الصادر عن محكمة أخرى قد تعتبر أكثر ملاءمة لحل النزاع في كثير من الأحيان، توجد في المناقشة القانونية في الولايات المتحدة إشارات إلى اختصاص قضائي يتعلق بشخص (اختصاص شخصي)، والذي يعارض، كقاعدة من قواعد الاختصاص القضائي، اختيار الاختصاص القضائي المتعلق بالمكان الذي يقع فيه الشيء/ الممتلكات اختصاص عيني)، وفي حالة استخدام اختصاص شخصي، تطبق المحاكم اختبار الحد الأدنى للاتصالات للمحكمة العليا، والذي تم تطويره في قضية شركة الأحذية الدولية ضد ولاية واشنطن في عام 1945.

إذا لم يكن لدى المدعى عليه أي ارتباط أو اتصال، فمن الضروري ضمان الإجراءات القانونية الواجبة، وبعد التحقق من وجود اتصال، تنتقل المحكمة إلى مرحلة التحليل اللاحقة، المعرفة نوعه، وفقا للتدرج في قضية هانسون ضد دينكلا لعام 1958، وبموجب هذه القضية، يتعين ملاحظة ما إذا كانت الأنشطة مباشرة بشكل مقصود إلى محكمة معينة، من أجل الاستفادة بشكل مقصود من التفاوض في مكان معين، حتى يتم التسليم التجاري للمنتجات ("تيار التجارة) إلى هذا المكان، لذلك يتعين علينا أن نولي اهتماما للقضايا الناشئة المتعلقة بالتفاعلات في الفضاء الإلكتروني، مثل السابقتين المهمتين قضية (كالدر ضد جونز وقضية زيبو مانوفاكتشرينج كو ضد جونز)، في قضية (كالدر ضد جونز)، أسست المحكمة العليا فهماً آخر لتعريف الاختصاص الشخصي، وحددت قاعدة مميزة لـ "الحد الأدنى من الاتصالات وفي هذه القضية، لوحظ المكان، الذي تم فيه الشعور بتداعيات مقال صحفي، لأنه تم نشره في ولاية فلوريدا، لكنه أشار إلى أحد سكان كاليفورنيا، الولاية التي تم توزيع الصحيفة فيها والتي تم رفع الدعوى القضائية أمام محاكمها وعلى الرغم من أنها سبقت النزاعات عبر الإنترنت التي يعود تاريخها إلى عام 1984 فإن المحاكم الأمريكية تستخدم هذه القضية التسوية النزاعات عبر الإنترنت[15].

كما ذهب الفقه الأمريكي[16] إلى اتجاه معاكس لما ذهبت إليه المحاكم الاسترالية، إذ تبنى معيار المقياس المتدرج لتحديد الاختصاص القضائي في بيئة الانترنت، وقد تبنت المحاكم الأمريكية هذا المعيار لأول مرة في قضية (Zippo Manufacturing v. Zippo Dot Com)، وبموجب هذا المعيار تم تصنيف المواقع على الإنترنت على أنها سلبية أو نشطة أو تفاعلية، الموقع السلبي ذلك الموقع الذي يتضمن معلومات معينة دون أن يكون هناك اتصال بين الموقع والاشخاص، أما الموقع التفاعلي يمكن لمستخدمي الأنترنيت تبادل المعلومات مع الكمبيوتر المضيف، أما الموقع النشط ذلك الموقع الذي يوفر امكانية اتصاله بمواقع خارج موقعة، وتكون المحكمة الأمريكية مختصة عندما يكون الموقع نشطاً وموقعه في الولايات المتحدة الأمريكية، وبالتالي تكون المحاكم الأمريكية صاحبة الاختصاص بشأن المطالبة بالتعويض عن الضرر الناشئ عن الجرائم السيبرانية متى ما صدر الفعل الجرمي من الموقع النشط[17]، وتبنت المحاكم الأمريكي مؤخراً محل وقوع الضرر كمعيار لاختصاصها[18].

ونرى أن المحكمة المختصة بنظر منازعات المسؤولية المدنية الناشئة عن الجرائم السيبرانية هي المحكمة المرفوع أمامها النزاع كون المتضرر طلب الحماية في تلك المحكمة، والتي تبدو أكثر ملائمة لنسبة للطرفين وما يتوافق مع مبدأ العدالة والانصاف.

المطلب الثالث:

القانون الواجب التطبيق بشأن المسؤولية المدنية الناشئة عن الجرائم السيبرانية

وفقاً للقواعد التقليدية أن القانون الواجب التطبيق بشأن المسؤولية التقصيرية هو القانون المحلي، والقانون المحلي أما أن يكون، قانون الدولة التي حدث فيها الفعل، أن منح الاختصاص للقانون المحلي يحقق التوازن المطلوب بين

حقوق الجاني والضحية وأيضاً توقع الحلول، كما أنه يسمح بخضوع سلوك مرتكب الفعل الضار وفقاً للقانون الذي وقع في هذا الفعل، مما يؤدي إلى ارتفاع مستوى الأمن القانوني، وقد عرفنا هذا المبدأ في عصر فقهاء المدرسة الإيطالية للوضعية في القرن الثالث عشر، حيث أخضع الفقهاء الفعل الضار لما يسمى بقانون مكان الجريمة، كما أقره فقهاء المدرسة الهولندية في القرن السابع عشر، وفقاً للقاعدة العامة في فقههم وهي الإقليمية للقوانين، وقد تبناها أيضا الفقيه مانشيني في القرن التاسع عشر بإخضاع الفعل الضار للقانون الذي وقع فيه الفعل استثناءً من نظريته القائمة على مبدأ شخصية القوانين الناشئة عن الفعل ومن ثم يعتبر هذا القانون مناسبا لتنظيم المسؤولية قانونيا[19].

وهذا ما أخذ به المشرع العراقي في المادة (27) من القانون المدني العراقي رقم (40) لسنة1951، أذ نصت على أنه، (1- الالتزامات غير التعاقدية يسري عليها قانون الدولة التي حدثت فيها الواقعة المنشئة للالتزام، 2- على انه لا تسري احكام الفقرة السابقة فيما يتعلق بالالتزامات الناشئة من العمل غير المشروع على الوقائع التي تحدث في الخارج وتكون مشروعة في العراق وان عدت غير مشروعة في البلد الذي وقعت فيه).

أو يكون القانون المحلي قانون الدولة التي وقع فيها الضرر، كون الضرر أهم عنصر في المسؤولية التقصيرية، ويدور وجوداً وعدماً معها[20]، كما أن قواعد المسؤولية تهدف إلى تحقيق التوازن بين مصلحتي الطرفين، ذلك التوازن الذي لحقه الاختلال في البلد الذي حدث فيه الضرر[21]، كما أن مكان تحقق الضرر هو الذي تتركز فيه مكانيا المسئولية باعتباره المكان الذي تظهر فيه العناصر المادية للواقعة المنشئة للالتزام إلى حيز الوجود[22].

وقد تبنى القانون الدولي الخاص السويسري لسنة 1987 قانون الدولة التي وقع فيها الضرر، إذ نصت المادة (133) على أنه، (1 إذا كان مرتكب الفعل الضار والطرف المتضرر يقيمان عادة في نفس الدولة، فإن المطالبات بالتعويض عن الفعل الضار تخضع لقانون تلك الدولة، إذا لم يكن مرتكب الفعل الضار والطرف المتضرر يقيمان عادة في نفس الدولة، فإن هذه المطالبات تخضع لقانون الدولة التي ارتكب فيها الفعل الضار ومع ذلك، إذا حدثت النتيجة في دولة أخرى، فإن قانون تلك الدولة ينطبق ...)[23].

ويرد التساؤل حول امكانية تطبيق القواعد التقليدي على المسؤولية المدنية الناشئة عن الجرائم السيبرانية؟

يرى البعض من الفقه، أن قانون محل وقوع الفعل أو قانون تحقق الضرر كلاهما غير قادر على وضع حلول عادلة ومناسبة في إطار المسؤولية المدنية الناشئة عن الجرائم السيبرانية، وذلك لانعدام الحدود المكانية المادية التي تفصل بين الدول عبر الانترنيت، فلا بد من تبني ضوابط تحقق العدالة وتنسجم مع البيئة الرقمية، لذلك طرحت عدة اراء بهذا الصدد.

ومن خلال تتبع آراء فقهاء القانون الدولي الخاص بشأن القانون الواجب التطبيق على الاضرار الناشئة عن الجرائم السيبرانية، لا نجد اتفاق على تبني ضابط معين، كذلك القضاء والتشريع في دول العالم، خاصة في الولايات المتحدة الأمريكية لا توجد قواعد تنازع قوانين ملزمة وأن قواعد تنازع القوانين بالصيغة الثانية والثالثة المعدلة ليست ملزمة للقضاء، لذلك القضاء الأمريكي عادة يجتهد ويبتدع الحلول، لذا يرعى قضاة المحاكم الأمريكي، بضرورة وجود قواعد عالمية يتم الاتفاق عليها بين الدول، لتكون قابلة للتطبيق بشأن منازعات الانترنيت بصورة عامة.

ويرى البعض[24] بأن القانون الواجب التطبيق هو القانون الشخصي للمتضرر فيما يتعلق بالاعتداءات التي تقع على البيانات الشخصية من خلال وسائل الاتصال، ووسائل الإعلام، وخاصة الصحافة أو الإذاعة أو التلفزيون أو أي وسيلة أخرى من وسائل الإعلام العامة، وقد أخذ بهذا الاتجاه القانون الدولي السويسري لسنة 1987، إذ نصت المادة (139) على أنه، (1. تخضع الدعاوى المبنية على انتهاك حقوق الشخصية من قبل وسائل الإعلام، وخاصة الصحافة أو الإذاعة أو التلفزيون أو أي وسيلة أخرى من وسائل الإعلام العامة، لاختيار الطرف المتضرر: أ. بموجب قانون الدولة التي يقيم فيها الطرف المتضرر عادة، بشرط أن يكون مرتكب الفعل الضار قد توقع حدوث النتيجة في تلك الدولة، ب. بموجب قانون الدولة التي يوجد فيها مرتكب الفعل الضار أو محل إقامته المعتاد؛ أو ج. بموجب قانون الدولة التي وقعت فيها نتيجة الانتهاك، بشرط أن يكون مرتكب الفعل الضار قد توقع أن النتيجة سوف تحدث في تلك الدولة، 2- يخضع حق الرد على وسائل الإعلام التي تظهر دورياً حصراً لقانون الدولة التي ظهر فيها المنشور أو تم بث البرنامج فيها، 3- تنطبق الفقرة 1 أيضًا على انتهاكات حقوق الشخصية الناتجة عن معالجة البيانات الشخصية، وكذلك على الإضرار بحق الوصول إلى البيانات الشخصية).

يرى البعض[25] أن القانون الواجب التطبيق بشأن الأضرار الناشئة عن الجرائم السيبرانية، هو قانون الدولة التي يطلب فيها الحماية، لأن هذا القانون غالبا ما يكون قانون الدولة الأكثر ارتباطا بالعلاقة ، ولابد من إيلاء مسألة تحديد القانون الواجب التطبيق على المسؤولية المدنية الناشئة عن الجرائم السيبرانية المرتكبة عبر شبكة المعلومات اهتماماً تشريعياً أكبر، لأن معظم تلك الجرائم المرتكبة ذات طابع دولي، مما يستدعي اعتماد معيار يتلائم مع الضرر السيبراني ويحقق العدالة، ولذلك أن معيار قانون الدولة المطلوب فيها الحماية هو الأفضل لأنه يعطي حماية أكبر المصالح المتضرر، كما يحقق الحياد والتوازن المطلوبين بين الأطراف.

الخاتمة

توصلنا من خلال بحثنا إلى أهم النتائج والمقترحات ونبينها في فقرتين: -

أولاً/ النتائج

1- أن الجرائم السيبرانية تثير العديد من المشاكل التي تحتاج إلى حلول تتناسب مع طبيعتها وتحقق لها الأمان والرخاء.
2- الإنترنت يتمتع بالبيئة المثالية التي تمكن الإنسان من فعل ما يريد، مما يسهل ارتكاب الجرائم الإلكترونية، فبالإضافة إلى وجود مجرم سيبراني، فإن نسبة كبيرة من جرائم القرصنة التي يرتكبها لا تزال غير مكتشفة بسبب

تعقيد منظومة الإنترنت وعدم قدرة التشريعات على ملاحقته.

3- هناك بعض الدول التي عالجت بعض المشاكل مثل الجماعة الأوروبية، في حين أن التشريعات العربية بشكل عام لم تتخذ خطوة جادة لمواجهة مشاكل العصر الرقمي، وفي الفترة الحالية أصبح القانون الدولي الخاص خاصة القواعد المنظمة لعلاقات المسؤولية المدنية ذات الطبيعة الدولية.

ثانياً/ المقترحات

1- نقترح اعتماد قواعد تنازع القوانين تنسجم مع الطبيعة غير المكانية أو الافتراضية للمجتمع الرقمي.

2- نقترح اعتماد معايير تتفق مع التوقعات المشروعة لأطراف دعوى المسؤولية، والتي تعد أحد المحددات المهمة لتوصيف الجريمة السيبرانية على نحو يؤدي إلى اختصاص المحكمة الأقرب إلى النزاع.

3- تقترح أن يكون قانون الدولة التي يطلب فيها الحماية هو القانون الواجب التطبيق، لأن هذا القانون غالبا ما يكون قانون الدولة الأكثر ارتباطا بالعلاقة القانونية،

المصادر

أولاً / المصادر العربية

أ- المؤلفات

1- د. أحمد عبد الكريم سلامة، علم قاعدة التنازع والاختيار بين الشرائع، مكتبة الجلاء الجديدة، ١٩٩٦ .

2- د. جابر جاد عبد الرحمن، تنازع القوانين، دار النهضة العربية، القاهرة، 1962.

3- د. عبد الرسول عبد الرضا، القانون الدولي الخاص، الطبعة الأولى، دار السنهوري، بيروت، 2018

4- د. فؤاد رياض د. سامية راشد الوسيط في القانون الدولي الخاص، الجزء الثاني (تنازع القوانين وتنازع الاختصاص القضائي الدولي، دار النهضة العربية، ١٩٩٢.

5- د. هشام صادق تنازع القوانين، منشأة المعارف بالإسكندرية، ١٩٧٤.

6- د. نائلة عادل محمد، جرائم الحاسوب الاقتصادية (دراسة نظرية وتطبيقية)، القاهرة، 2004.

ب- الدوريات

1- روان بنت عطية الله، الجرائم السيبرانية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد 24، 2020.

2- . عبد الحكيم ملاي ابراهيم، الجرائم الإلكترونية، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، الجزائر، المجلد 2 العدد 23، 2015.

ت- الرسائل

1- أسامة مهمل، الإجرام السيبراني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، 2017.

ث- المواقع الالكترونية

1- د. جلال فضل محمد، مقالات في الجريمة السيبرانية، متوفر على الموقع الالكتروني لمكتبة النور العلمية، https://www.noor-book.com

2- د. صالح علي عبد الرحمن الربيعة ، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت ، هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية، مقال منشور على الموقع الإلكتروني http://myhistar1.blogspot.com

ج- القوانين واللوائح

1- القانون المدني العراقي رقم (40) لسنة1951 .

2- القانون الدولي السويسري لسنة 1987.

3- لائحة الاتحاد الأوروبي رقم (2012/1215).

A. Books (المؤلفات):

1. Salama, Ahmed Abdel Karim. *The Science of Conflict of Laws and the Choice Between Legal Systems*. El-Galaa Al-Gadida Library, 1996.
2. Abdel Rahman, Gaber Gad. *Conflict of Laws*. Dar Al-Nahda Al-Arabiya, Cairo, 1962.
3. Abdul Redha, Abdul Rasool. *Private International Law*, 1st ed. Al-Sanhouri Publishing, Beirut, 2018.
4. Riyad, Fouad, and Samia Rashed. *Al-Waseet in Private International Law: Volume II (Conflict of Laws and International Jurisdictional Conflict)*. Dar Al-Nahda Al-Arabiya, 1992.
5. Sadiq, Hesham. *Conflict of Laws*. Al-Maaref Establishment, Alexandria, 1974.
6. Mohamed, Naela Adel. *Computer Economic Crimes: A Theoretical and Practical Study*. Cairo, 2004.

B. Journals (الدوريات):

1. Atia Allah, Rowan Bint. "Cybercrimes." *The Comprehensive Electronic Multidisciplinary Journal*, no. 24 (2020).
2. Ibrahim, Abdel Hakim Malay. "Electronic Crimes." *Journal of Law and Human Sciences*, University of Ziane Achour, Djelfa, Algeria, vol. 2, no. 23 (2015).

C. Theses (الرسائل):

1. Mouhmel, Osama. *Cybercrime*. Master's Thesis, Faculty of Law and Political Science, University of Mohamed Boudiaf, 2017.

D. Online Sources (المواقع الالكترونية)

1. Fadl, Jalal Mohammed. "Articles on Cybercrime." Noor Scientific Library.

Accessed June 25, 2025. https://www.noor-book.com

2. Al-Rabeeah, Saleh Ali Abdulrahman. "Digital Security and User Protection from Internet Risks." Communications and Information Technology Commission, Saudi Arabia. Accessed June 25, 2025. http://myhistar1.blogspot.com

E. Laws and Regulations (القوانين واللوائح):

1. Iraqi Civil Code, No. 40 of 1951.
2. Swiss Private International Law Act of 1987.
3. European Union Regulation No. 1215/2012

ثانياً / المصادر الأجنبية (Foreign Sources)

1- Ahmed Ashraf Musharraf, The law applicable to civil liability arising from electronic crimes, International Journal of Doctrine, Judiciary and Legislation, Volume 3, Issue3, 2022.

2- Bill A. Forum Shopping and Place in Transnational Litigation, Oxford, UK, Blackstone Press, 2002.

3- Bimal Raut, T., "Determining Jurisdiction in Transnational Cyberspace" PhD Thesis, Queensland University of Technology, 2004.

4- Dr. Dan Jerker B. Svantesson, EU Jurisdiction Claims on the Internet – An Analysis of Three Key Developments Recent, Journal of Intellectual Property, Information Technology and E-Commerce Law, Volume 9, Issue 2, 2018.

5- Evelyne Studer and Jacques de Werra, Regulating Cybersecurity - What Civil Liability in Case of Cyber-Attacks?, p512, Article available on the website, https://papers.ssrn.com .

6- Feierstein, Alan R. Personal Jurisdiction and the Internet: Viewing Due Process Through the Lens of Regulatory Precision. Northwestern University Law Journal, Northwestern University Law Journal, Volume32, 2004,

7- Darrel C. Menthe, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review Volume 4, Issue 1, 1998.

8- Jimenez, William Guillermo. Jurisdiction Rules on the Internet and Offline: A Global Overview and Colombian Cases. International Law, Colombian Journal of International Law, No. 26, 2016.

9- Metsiligas, Valsamis. Anti-Money Laundering Measures in the European Union: A New Model of Security Governance in the Face of Fundamental Legal Principles. Volume 20 Kluwer Journal Law International B.V., 2003,.

10- Mark Addey, Conflict of Laws: Choice of Law Theories in Tort, University of Professional Studies, Accra, 2023, Available at http://dx.doi.org/10.2139/ssrn.4574112

11- Oona` A.Hathway , Rebecca Crootof , Philip Levtiz , aley Nix, Aileen Nowlan ,William Perdue and Julia Spiegel, "The Law of Cyber –Attack", California Law Review, 2012 .

12- Pontian N. Okoli, Judicial basis in conflict of laws Challenges of policy and security on the Internet Harms with commercial implications, General Journal of International and Comparative Law, Volume 51, Issue 2, 2023.

13- Stacey Duggan, Trends and Perspectives on Cybersecurity Liability in the United States, A working paper presented at the international conference entitled (Civil Liability for Electronic Attacks), Geneva, 2018.

14- T Rice, "Consumer Protection in E-Commerce," Conference Proceedings, CLA Conference, Lisbon, 11-12 October; J Green, J Ryan, S Wooden, J McKown, C McWhinney, 2001; "The Sliding Scale of Personal Jurisdiction on the Internet," Stanford Technology Law Review 2000 (2001).

الهوامش:

[1] -Oona` A.Hathway , Rebecca Crootof , Philip Levtiz , aley Nix, Aileen Nowlan ,William Perdue and Julia Spiegel, "The Law of Cyber –Attack", California Law Review, 2012 , p702.

[2] - د. جلال فضل محمد، مقالات في الجريمة السيبرانية، متوفر على الموقع الالكتروني لمكتبة النور العلمية،

https://www.noor-book.com

تاريخ الزيارة 2024/9/12، الساعة 4:48 مساءً.

[3] - أسمامة مهمل، الإجرام السيبراني، رسالة ماجستير، كلية الحقوق والعلوم السياسية ، جامعة محمد بوضياف، 2017، ص1.

[4] - د. نائلة عادل محمد، جرائم الحاسوب الأقتصادية (دراسة نظرية وتطبيقية)، القاهرة، 2004، ص25.

[5] - د. صالح علي عبد الرحمن الربيعة ، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت ، هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية، ص9، مقال منشور على الموقع الإلكتروني

http://myhistar1.blogspot.com

تاريخ الزيارة 2024/9/12، الساعة 5:44 مساءً.

[6]- Metsiligas, Valsamis. Anti-Money Laundering Measures in the European Union: A New Model of Security Governance in the Face of Fundamental Legal Principles. Volume 20 Kluwer Journal
Law International B.V., 2003, p89.

[7] - Pontian N. Okoli, Judicial basis in conflict of laws Challenges of policy and security on the Internet Harms with commercial implications, General Journal of International and Comparative Law, Volume 51, Issue 2, 2023, p399-410.

[8] - روان بنت عطية الله، الجرائم السيبرانية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد 24، 2020، ص12.

[9] - د. عبد الحكيم ملاي ابراهيم، الجرائم الإلكترونية، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، الجزائر، المجلد 2 العدد 23، 2015، ص213.

[10]- د. عبد الرسول عبد الرضا، القانون الدولي الخاص، الطبعة الأولى، دار السنهوري، بيروت، 2018، ص413-414.

[11] - Darrel C. Menthe, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review Volume 4, Issue 1, 1998, p78.

[12] - Bill A. Forum Shopping and Place in Transnational Litigation, Oxford, UK, Blackstone Press, 2002, p221, Bimal Raut, T., "Determining Jurisdiction in Transnational Cyberspace" PhD Thesis, Queensland University of Technology, 2004, p54.

[13] - Evelyne Studer and Jacques de Werra, Regulating Cybersecurity − What Civil Liability in Case of Cyber−Attacks?, p512, Article available on the website, https://papers.ssrn.com, Date of visit 8−2−2025, 3:32 pm.

[14] -Feierstein, Alan R. Personal Jurisdiction and the Internet: Viewing Due Process Through the Lens of Regulatory Precision. Northwestern University Law Journal, Northwestern University Law Journal, Volume32, 2004, p415.

[15] -Jimenez, William Guillermo. Jurisdiction Rules on the Internet and Offline: A Global Overview and Colombian Cases. International Law, Colombian Journal of International Law, No. 26, 2016 p. 22.

[16] -T Rice, "Consumer Protection in E-Commerce," Conference Proceedings, CLA Conference, Lisbon, 11-12 October; J Green, J Ryan, S Wooden, J McKown, C McWhinney, 2001; "The Sliding Scale of Personal Jurisdiction on the Internet," Stanford Technology Law Review 2000 (2001).

[17] - Dr. Dan Jerker B. Svantesson, EU Jurisdiction Claims on the Internet – An Analysis of Three Key Developments Recent, Journal of Intellectual Property, Information Technology and E-Commerce Law, Volume 9, , Issue 2m 2018, p124, Bimal Raut, op. cit, p68-73.

[18] - Bimal Raut, op .cit, p80.

[19] - د. جابر جاد عبد الرحمن، تنازع القوانين، دار النهضة العربية، القاهرة، 1962، ص100، 490-491.

[20] - Mark Addey, Conflict of Laws: Choice of Law Theories in Tort, University of Professional Studies, Accra, 2023, p5, Available at http://dx.doi.org/10.2139/ssrn.4574112 , Visited at 14/9/2024, 5:21 pm.

[21] - د. فؤاد رياض د. سامية راشد الوسيط في القانون الدولي الخاص، الجزء الثاني (تنازع القوانين وتنازع الاختصاص القضائي الدولي، دار النهضة العربية، ١٩٩٢ ، ص ٣٥٥، د. هشام صادق تنازع القوانين، منشأة المعارف بالإسكندرية، ١٩٧٤، ص ٧٣٨ وما بعدها.

[22] - د. فؤاد رياض د. سامية راشد، مرجع سابق، ص ٣٥٥؛ د. أحمد عبد الكريم سلامة، علم قاعدة التنازع والاختيار بين الشرائع، مكتبة الجلاء الجديدة ١٩٩٦ ، ، ص ١١٩٥

[23] - القانون الدولي الخاص السويسري لسنة 1987، متوفر على الموقع الالكتروني

https://www.bj.admin.ch

تاريخ الزيارة 2024/9/15، الساعة 11:13 صباحاً.

[24]- Stacey Duggan, Trends and Perspectives on Cybersecurity Liability in the United States, A working paper presented at the international conference entitled (Civil Liability for Electronic Attacks)، Geneva, 2018, p33.

[25]- Ahmed Ashraf Musharraf, the law applicable to civil liability arising from electronic crimes, International Journal of Doctrine, Judiciary and Legislation, Volume 3, Issue3, 2022, p903.