مجلة الدراسات القانونية المقارنة
EISSN:2600-6154 المجلد12/ العـــدد01(2026)، ص.ص.288-313. ISSN:2478-0022

الحماية الجنائية الدولية للارتفاقات الرقمية

International Criminal Protection of Digital Easements

سفيان عيساوي

Soufyane AISSAOUI

أستاذ محاضر قسم "أ"، قانون دولي جنائي، كلية العلوم الاقتصادية و العلوم التجارية وعلوم التسيير،

جامعة الجزائر3، ابراهيم سلطان شيبوط

Lecturer "A" – International Criminal Law
Faculty of Economic Sciences, Business, and Management Sciences
University of Algiers 3, Ibrahim Sultan CHEIBOUT
Email:aissaoui.soufyane@univ-alger3.dz

تاريخ إرسال المقال:2026/03/15 **تاريخ القبول:2026/05/19** **تاريخ النشر:2026/06/08**

ملخص:

يعد موضوع الحماية الجنائية الدولية للارتفاقات الرقمية من أعقد الموضوعات المركبة من الناحيتين القانونية والقضائية، لما له من دقة وتقاطع لقواعد القانون الدولي الجنائي وقواعد الشرعة الدولية لحقوق الإنسان، وبالرغم من تعرّض القانون الدولي لموضوع الارتفاقات في العديد من المحطات الإجرائية في شقها الخاص، إلا أنه ظل محل نقاش فقهي وقانوني مستمر، وذلك بسبب ظهور أنماط مستحدثة كالارتفاقات الرقمية في شكلها الجديد، وهذا ما طرح عدة إشكالات وقضايا على مستوى الفقه والقضاء الدولي.

يسعى هذا البحث إلى تبيان التكييف القانوني الصحيح للجرائم المرتكبة ضد الارتفاقات الرقمية، وذلك من خلال تفعيل قواعد المسائلة الجنائية الدولية وقياس مختلف الآليات القانونية والقضائية الدولية المقررة، التي تعد ضابطا مفصليا لتحديد نجاعة وفعالية حماية الحق في الولوج إلى حقوق الملكية الرقمية، وبذلك يسعى المشرع الدولي إلى إيجاد الحلول الملائمة لمختلف الإشكالات العالمية المطروحة في ذات الإطار.

كلمات مفتاحية:

الارتفاقات الرقمية – القانون الجنائي الدولي – حقوق الإنسان – الجريمة السيبرانية.

Abstract:

The subject of international criminal protection of digital easements is considered one of the most complex composite topics from both legal and judicial perspectives, due to its precision and the intersection between the rules of international criminal

المؤلف المرسل: سفيان عيساوي ***Email**:aissaoui.soufyane@univ-alger3.dz*.

law and the rules of the international bill of human rights. Despite the fact that international law has addressed the issue of easements in several procedural stages in its specific aspect, it has remained the subject of continuous doctrinal and legal debate, particularly with the emergence of new patterns such as digital easements in their modern form. This has raised several issues and questions at the level of jurisprudence and international judiciary.

This research seeks to clarify the proper legal characterization of crimes committed against digital easements, through activating the rules of international criminal responsibility and examining the various established international legal and judicial mechanisms, which constitute a decisive benchmark for determining the efficiency and effectiveness of protecting the right of access to digital property rights Accordingly, the international legislator seeks to find appropriate solutions to the various global issues raised within this framework.

Keywords:
Digital easements; International criminal law; Human rights; Cybercrime.

مقدمة:

تؤدي التكنولوجيات الرقمية إلى تغيير عالمنا بشكل كبير، فهي توفر للمستخدم فوائد محتملة هائلة لرفاه وتقدم الناس والمجتمعات العالمية، وتبّشر بتسريع خطى جادة لتحقيق أهداف التنمية المستدامة، ولا يمكننا تحقيق ذلك إلا من خلال تعزيز التعاون الدولي الذي يسّد جميع الفجوات الرقمية بين البلدان الأعضاء في المجتمع الدولي المعاصر، ولذلك تسلم الدول بالتحديات التي تسببها الفجوات الرقمية للعديد من البلدان النامية، والتي لديها احتياجات إنمائية ملحة وموارد محدودة.

يمثل الإنترنت فرصة غير مسبوقة لأي شخص للتعبير عن نفسه على الساحة العالمية، ولذلك أصبح انتهاك حقوق الفضاء الرقمي أسهل بكثير مما كان عليه في الماضي، فسهولة رفع الملفات ومشاركتها أو توزيعها بأي شكل من الأشكال لم يكن من الممكن تخيل حدوثه سابقًا، ومع ظهور تقنيات الولوّج عبر الارتفاقات الرقمية أصبح مُلاك البيانات يواجهون موجة جديدة ومختلفة من الانتهاكات الفكرية، فقد أضحى التعاون الدولي لدى مزودي الخدمات الإلكترونية أمرًا بالغ الأهمية من أجل وقف الهجمات والجرائم السيبرانية.

لقد أدى ازدياد التفاعلات الرقمية العابرة للحدود، خاصة عند ظهور الشبكة العالمية النسبية والجديدة، إلى أن تصبح الارتفاقات الرقمية مسألة تتطلب نطاقًا حمائيا عابراً للحدود العالمية، كما أدى التطور العلمي والتكنولوجي إلى تحول في النظام القانوني والقضائي العالمي خلال العشرين عامًا الماضية، وذلك استجابةً للملاحظة القائلة بأن الدول القومية وحدها لم تعد قادرة على الاستجابة بفعالية لهذا المشهد الجديد بسبب حدودها الإقليمية والفضائية، ومع وصول الفضاء السيبراني إلى التطور المعرفي الحالي أصبحت قواعد العدالة الجنائية الدولية تواجه مجموعة من التحديات الجديدة

والمتغيرات التي تتضمن تهديدات غير مألوفة تستدعي مواجهتها، خاصة في ظل العولمة الرقمية الحديثة وحقوق الإنسان التي يتمتع بها الأفراد في إطار قواعد الشرعة الدولية.

إن التنظيم القانوني لحق الارتفاق منذ القدم جعل نطاقه قاصرا على نظام الملكية العقارية في شكله المادي الملموس فقط، حتى أن بعض الحضارات القديمة جعلته يمتد إلى الجنس البشري، وهو الأمر الذي جعل حقوق الارتفاق من أكثر المواضيع المرتبطة بحق الملكية إشكالا، فضلا عن أهمية هذا الحق باعتباره من المفاهيم القانونية التي تنظم الحياة البشرية وسلوك الأفراد في كل زمان ومكان قابل للتطور، وذلك بحكم تأثره بمجالات الحياة كافة، وعليه فقد أفرز الواقع العملي تطبيقات كثيرة متعددة لحقوق الارتفاق المستحدثة في المجتمع الدولي المعاصر.

في ذات الإطار، يعد موضوع الارتفاقات الرقمية من الموضوعات المهمة والجديرة بالدراسة لما له من أهمية في تنظيم عملية تداول البيانات الرقمية ومشاركتها، ومع أن هذا النوع من الحقوق قد أخذ اليوم طابع مختلفا، إلا أن الكتابات الفقهية والقانونية لا تزال قاصرة عن الوفاء بما يتطلبه هذا العصر، خاصة وأن هنالك مستجدات متعلقة بالهجمات السيبرانية في ظل البيئة الرقمية، فكان لابد من الحصول على حقوق الارتفاق لضمان وصول المستخدمين إلى حساباتهم الشخصية عبر الانترنت، ولعّل هذا البحث يعتبر إضافة جديدة لإثراء بعض جوانب موضوع حق الارتفاق وتطبيقاته المعاصرة عبر الفضاء الرقمي.

تظهر أهمية البحث في كونه يتناول التأثير الحقوقي للثورة المعلوماتية وما نتج عنها من جرائم الكترونية واقعة على المجتمع الدولي، وعند إلقاء الضوء على جهود المشرع الدولي في مكافحة هذه الجرائم، نرى أن الوقوف على آليات حماية الحق في الارتفاق الرقمي في ظل أحكام القانون الدولي هي ضرورة قانونية وواجب أخلاقي، ولذلك يمكننا أن نتساءل من خلال هذه الورقة البحثية عبر طرح الإشكالية الآتية: **هل نجح النظام الجنائي الدولي في توفير حماية فعّالة للارتفاقات الرقمية في ظل التطور التكنولوجي وتعدّد التهديدات السيبرانية؟**.

أهداف الدراسة: تسعى هذه الدراسة إلى بلوغ الأهداف التالية:

- تبيان الوصف القانوني للارتفاقات الرقمية ومدى علاقتها بحقوق الإنسان.
- تكييف الجرائم المرتكبة وتوضيح مدى خطورتها عند انتهاك وخرق نطاق الارتفاقات الرقمية.
- تحديد الاختصاص الجنائي الدولي في إطار محاكمة مرتكبي الجرائم السيبرانية عبر الارتفاقات الرقمية.
- إبراز أهم الإشكالات التي يثيرها التعاون الدولي الجنائي في ذات الإطار.

المنهج المتبع:

اعتمدت الدراسة على المنهج الوصفي الذي تم توظيفه لإبراز الوصف القانوني لحقوق الارتفاق في شكلها المستحدث، مع تحديد مختلف الجرائم الدولية المرتكبة عبر نظام الارتفاقات الرقمية، كما تم الاستعانة بالمنهج التحليلي في تحليل مختلف التقنيات الدولية المتعلقة بإجراءات التحقيق في الجرائم السيبرانية المرتكبة عبر الارتفاقات الرقمية ، ومختلف الإشكالات الدولية المطروحة إطار إستراتيجية التعاون الجنائي الدولي في ذات الإطار.

تقسيم الدراسة:

لمعالجة إشكالية هذه الورقة البحثية لابد من تبيان الوصف القانوني للارتفاقات الرقمية وعلاقتها بقواعد الشرعة الدولية لحقوق الإنسان" **المحور الأول"**، لنعرج بعدها إلى معالجة قواعد المسؤولية الجنائية عن انتهاك حقوق الارتفاقات الرقمية "**المحور الثاني"**، مع تحليل بعض الإشكالات الدولية المطروحة في ذات الإطار "**المحور الثالث"**.

المحور الأول: الوصف القانوني للارتفاقات الرقمية

إن تقدم ورقي الإنسان في مختلف أوجه الحياة لا يتأت إلا إذا استخدم فكره لتحقيق هذا الهدف، وهو الأمر الذي يدل على أن الإنتاج الذهني القائم على توفير حياة أفضل للبشر في العالم المعاصر، وهذا ما يوجب إعطاء هذا الفكر الاهتمام المناسب، وذلك من خلال توفير الحماية القانونية المناسبة له، ومن خلال النظام القانوني الدولي يسعى الإنسان إلى التمتع بكافة الحقوق المرتبطة بمرافق الحياة، وقد أصبح العالم يشهد تقدما وتطورا في نظم الاتصالات ونقل المعلومات، حيث أضحى الكمبيوتر يمثل نقطة الارتكاز التي انطلق منها هذا الانقلاب الكبير، وكان بمثابة المحور الأساسي في نشوء ما عرف بطريق المعلومات فائقة السرعة، ومن أهم أجزائه شبكة المعلومات الدولية "الانترنت"، التي أدت لاختصار الكثير من الوقت والجهد والمال، والانترنت هي عبارة عن شبكة ضخمة جدا من بين الشبكات المختلفة والمترابطة مع بعضها البعض في مختلف بقاع العالم، وتستخدم هذه الشبكات بروتوكولات معينة كوسيلة للتخاطب فيما بينها من أجل توفير حق المرور الرقمي، وبذلك أدت القفزة الرقمية التي حدثت في العالم إلى إحداث أثر بالغ في كافة جوانب الحياة، وكان لها أثر مباشر على الملكية الفكرية، وتحديدا في مجال حق المؤلف الوارد على الملكية الرقمية (خنفوسي، 2019، صفحة 136).

أولا: انتقال مفهوم الارتفاقات من نظام الملكية العقارية إلى فضاء المحتوى الرقمي

يعرف حق الارتفاق على أنه:"حق عيني بمقتضاه يقرر القانون أو الاتفاق حدا لمنفعة عقار يسمى العقار الخادم لفائدة عقار مملوك لشخص آخر يسمى العقار المخدوم" (الجيلالي، 2009، صفحة 383)، والارتفاق حق مرتب على عقار لمنفعة عقار آخر يملكه شخص غير مالك للعقار الأول، فهو خضوع عقار لمصلحة عقار آخر تجاوزا لمصلحة المالك الأصلي، فيتبع العقار أين تنقل، ويتمتع صاحبه بسلطة استعماله ويستأثر بمنافعه، ولكنه لا يمكن أن يوَظف إلا بموافقة جميع المالكين ويبقى قائما حتى مع تجزئة العقار (كحلون، 2015، صفحة 321)، والطبيعة القانونية المضفاة على حق الارتفاق كحق عيني هي التي أدت إلى إخضاع انتقال ملكيته حسب المادة 324 مكرر من القانون المدني لأشكال جوهرية يترتب عن تخلفها عدم جواز الاحتجاج به اتجاه الغير (عمر، 2025، صفحة 284)، ويشترك حق الارتفاق مع حق المرور في ترتيب نفس الحقوق والالتزامات التي يرتبها حق الارتفاق بالمرور ما عدا ما يتعارض مع طبيعة حق المرور باعتباره قيدا على الملكية (بلحيمر، 2017، صفحة 150).

لقد تطور مفهوم الارتفاقات لينسجم قانون الارتفاق مع ظهور المفهوم الإداري في ظل تقنيات الإعلام والاتصال الحديثة، ويبرز ذلك من خلال ما تضمنته المادة 10 فقرة 02 من القانون رقم 18-04 المؤرخ في 10 ماي 2018 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ويتجلّى هذا الطرح في مضمون الارتفاق اللاسلكي الكهربائي الذي يتمحور حول كل ارتفاق في علو الحواجز بالمناطق المعينة حول مراكز الإرسال أو الاستقبال، وهذا

تفاديا لاضطراب الموجات اللاسلكية الكهربائية التي ترسلها أو تستقبلها هذه المراكز، وقد نص المشرع على إمكانية تركيب شبكات الاتصالات الالكترونية المفتوحة للجمهور على الأملاك العمومية عن طريق إقامة المنشآت (سبتي، 2021، صفحة 298)، وبذلك تطور مفهوم الارتفاق التقليدي إلى شكله الحديث في مجال تقنيات الإعلام والاتصال الالكتروني وقد توّصل العلم الحديث إلى مفهوم الارتفاق الرقمي في نهج متقدم يعكس ما وصل إليه التطور التكنولوجي والعلمي عبر تكريس القواعد الدولية لنظام الملكية الفكرية الرقمية (Mackenrodt, 2018, p. 252).

في ذات الإطار تحولت الارتفاقات الرقمية إلى إحدى الصور المستحدثة لحق الارتفاق، وما حق الارتفاق المستحدث إلا سلطة تحد من منفعة شيء أو حق ذو قيمة مالية مملوكة لأحد الأشخاص لفائدة شيء أو حق ذو قيمة مالية مملوك لشخص آخر، فالارتفاق المستحدث ما هو إلا سلطة تمنح للمالك باعتباره حقا رقميا له، وقول الباحث بأن هذه السلطة تقيد وتحد من منفعة شيء أو حق ذو قيمة مالية، ما هو إلا اعتبار بأّن هذه الارتفاقات تمتد إلى مضامين ذات قيمة مالية لم ينظمها المشرع كالارتفاقات الرقمية المختلفة الخاصة ببيانات الحاسوب والانترنت والذكاء الاصطناعي، والتي تكون مقننة على شكل قيود بالنسبة إلى الطرف الآخر، وبالتي فإن هذه التطبيقات المستحدثة لا يمكن الاستفادة منها إلا من خلال تحليل التطور الحاصل الذي عرفته فلسفة حق الارتفاق، وهذه الفلسفة تظهر بصورة جلية باعتباره حقا عينيا يحد من منفعة شيء لمصلحة شيء آخر، بمعنى أن حق الارتفاق يقيد ملكية أحد الأشخاص بما يخدم ملكية شخص آخر على نطاق معين من حق الملكية الرقمية (مطير و علي مطشر، 2023، صفحة 247).

ينصرف مفهوم الارتفاقات الرقمية إلى إنشاء أو استخدام البيانات الالكترونية، والتي من خلالها يتم الولوج أو العبور إلى فضاء الانترنت ومختلف المنصات الرقمية، وذلك عبر واجهات برمجة التطبيقات على مستويين للفهم، يتمثل الأول في المستوى العقلاني، حيث تنطبق المبادئ الموجودة في قانون الارتفاق على حوكمة واجهات البرمجة لتطبيقات الانترنت والذكاء الاصطناعي، وذلك لأنها تمتلك مبررات سياسية موازية تتعاون من أجل خلق توازن بين المصالح الرقمية المتنافسة والمتجانسة، والمستوى الثاني الذي يوفر استخدام قانون الارتفاق باعتباره خيارًا عمليًا للحوكمة والخوارزميات التي تتضمن الوضّوح والدقة في الشكل الصحيح الذي يبين للشخص القانوني كيفية تنفيذ هذه الحقوق (O'Reilly, 2025, p. 170).

يتيح الإنترنت فرصًا غير مسبوقة للتعبير على نطاق الارتفاق والولوج إلى المحتوى الرقمي العالمي، لكن هذه الفرصة تُضاعف الأضرار الناتجة عن استخدام المواد المحمية بحقوق الارتفاق، ومع سهولة تحميل وتوزيع الملفات، أصبح انتهاك حقوق الارتفاق الرقمي أكثر سهولة وتكرارًا، ما يجعل تعاون المرتفقين الدوليين ضروريًا للحد من الانتهاكات، لاسيما وأن أصحاب حقوق الارتفاق غالبًا ما يمثلون الجهة الوحيدة القادرة على الوصول إلى المحتوى الرقمي وتنفيذه أو اتخاذ الإجراءات القانونية المناسبة (Taddeo & Floridi, 2017, p. 237).

في هذا المجال أشار بعض الفقه الدولي المعاصر إلى أن الارتفاقات الرقمية تتضمن حقوق قانونية تُمنح لطرف معين لاستخدام مورد رقمي مملوك لطرف آخر بطريقة محدّدة، دون نقل الملكية، بمعنى آخر، هي شبيهة بحق المرور أو الانتفاع في العقار، لكن بدل الأرض أو العقار، يكون محلها البيانات والمنصات الرقمية، البرمجيات،واجهات البرمجة (APIs)، والارتفاقات الرقمية تمثل تطورًا حديثًا في الفكر القانوني المعاصر، حيث يتم نقل مفاهيم تقليدية من القانون

المدني إلى الفضاء الرقمي لتنظيم العلاقات بين الأطراف في عالم يعتمد بشكل متزايد على البيانات والتكنولوجيا (O'Reilly, 2025, p. 159).، كما تهدف الإصلاحات القانونية الجارية على الساحة الدولية إلى جعل المجتمع الدولي أكثر حماية وخصوصية في مجال البيانات الالكترونية المقدمة عبر العالم، وذلك من خلال توفير حماية مناسبة لمزودي خدمات الإنترنت وشركات الاتصالات، وبذلك أصبح الارتفاق الرقمي مرشحًا مهمًا لعبور الأنشطة العديدة مثل الحوسبة الفائقة وتعدين العملات الافتراضية مثل Bitcoin، إضافة إلى استضافة فعاليات صناعة الحوسبة السحابية في مختلف أنحاء العالم (Iorliam, 2019, p. 36).

لقد أصبحت حماية الفضاء الإلكتروني مهمَّة عالميَّة صعبة في ظل سرعة المعلومات التي يتم إرسالها يوميا عبر الفضاء السيبراني، في وقت أقل مما يستغرقه توجيه ظرف واحد يدويًا، علاوة على ذلك، يمكن للمرسل اختيار وسائل متعددة في الفضاء السيبراني لضمان بقاء هويته مجهولة بالكامل (Sellers & Maxeiner, London, p. 47)، والنظام الدولي المعمول به حاليا والمسمى "نظام المشاع الرقمي"، يتطلب لاستخدامه تحديد قواعد أخلاقية مناسبة، لكنه في ذات الإطار يترك إمكانية الوصول إلى المحتوى الرقمي مفتوح أمام أي مستخدم محتمل مستعد لقبول التداخل وإدارته، ومثال ذلك نظام تداول المعلومات الالكترونية، حيث تُعد الشبكات اللاسلكية التي تعمل عبر تقنيات مثل Wi-Fi و Bluetoothمن أبرز المنتجات الناتجة عن التخصيص الرقمي العالمي، إلى جانب الهواتف اللاسلكية، والميكروفونات الممغنطة، وأجهزة مراقبة الأطفال، وغيرها الكثير...، ومن الواضح أن اختيار نظام إدارة الارتفاقات الرقمية يؤثر تأثيراً كبيراً في النتائج النهائية لتداول المعلومات الرقمية وخصائصها عبر منصات التواصل الاجتماعي (Alaydrus, 2012, p. 188)، و في ذات الإطار يتميز نظام الارتفاق الرقمي عن غيره من الارتفاقات من خلال عدة خصائص يمكن تبيانها كالآتي:

1.تدويل الارتفاق الرقمي

يقوم النظام القانوني المستحدث للارتفاق الرقمي على إضفاء الطابع العابر للحدود من خلال الحقوق المرتبطة باستعمال الموارد الرقمية أو البنى التحتية المعلوماتية (حسين، 2011، صفحة 53)، بحيث تتجاوز هذه الحقوق الإقليم الوطني للدولة، وتخضع لتفاعل وتداخل عدة أنظمة قانونية، الأمر الذي يثير إشكالات تتعلق بتحديد القانون الدولي الواجب التطبيق، والاختصاص القضائي، وضمان التوازن بين حرية تدفق البيانات ومتطلبات السيادة الرقمية، وهذا هو جوهر الاختلاف بين الارتفاق الرقمي الدولي والارتفاق الوطني الذي يبقى كحق عيني محصور في نطاق الوعاء العقاري داخل الدولة (الطباخ، 2014، صفحة 376).

2.عالمية المشاركة

تعتبر عالمية مشاركة البيانات عبر الارتفاق الرقمي ظاهرة قانونية وتقنية تعكس الانتشار العابر للحدود لتبادل الحق في تداول البيانات عبر البيئة الرقمية، حيث يتم إنتاج البيانات ومعالجتها وتخزينها ونقلها عبر أنظمة معلوماتية موزعة دولياً، الأمر الذي يؤدي إلى تداخل الاختصاصات القانونية، ويثير إشكاليات تتعلق بحماية البيانات الشخصية، وأمن المعلومات، وتحديد القانون الواجب التطبيق (محمد ح.، 2020، صفحة 134)، في ظل سعي الدول والمنظمات الدولية إلى وضع

أطر تنظيمية موّحدة توازن بين حرية تدفق البيانات ومتطلبات السيادة الرقمية، عكس نظام الارتفاق العادي الذي يقوم على توزيع حق المرور داخل العقار بين أفراد الدولة (الطباخ، 2014، صفحة 375).

3.رقابة مقدمي الخدمات

يُقصد برقابة مقدّمي الخدمات عبر الارتفاق الرقمي "ذلك الإطار القانوني الذي ينظم مسؤولية الجهات الوسيطة الرقمية، مثل منصات التواصل الاجتماعي" (القبطان، 2025، صفحة 114)، ومحركات البحث، ومزودي الاستضافة في الإشراف على المحتوى المتداول عبر خدماتها، سواء من خلال رقابة استباقية أو لاحقة (حسين، 2011، صفحة 54)، وذلك لتحقيق التوازن بين متطلبات إنفاذ القانون وحماية الحقوق والحريات الأساسية داخل نطاق الارتفاق، خاصة حرية التعبير والحق في الخصوصية، في ظل بيئة رقمية عابرة للحدود وتعدد للأنظمة القانونية للحماية (محمد ح.، 2020، صفحة 132).

4. خاصية الولوّج الدولي عبر المنصات وقواعد البحث

تشمل خاصية الولوج الدولي إنشاء إطار تقني وقانوني متكامل يعتمد على البرمجيات والخوارزميات لتنظيم حركة البيانات داخل الارتفاق الرقمي "كمنصة إلكترونية أو شبكة معلوماتية"، بحيث يتم التحكم في كيفية دخول البيانات وخروجها وتداولها بين المستخدمين والأنظمة عند دخول فضاء الارتفاق الرقمي، مع تضمين آليات التحقق من الهوية الشخصية، وتحديد مستويات الوصول، وضمان أمن المعلومات، والامتثال للتشريعات الوطنية والدولية المتعلقة بحماية البيانات وتدفقها عبر الحدود من خلال تطبيق نظام العقوبات السيبرانية (الصادق، 2022، صفحة 19).

ثانيا: الارتفاقات الرقمية كحق من حقوق الإنسان

لقد أفرزت التحولات الرقمية السريعة التي يشهدها العالم المعاصر واقعا قانونيا جديدا، أصبحت فيه التقنيات الرقمية جزءا لا يتجزأ من الحياة اليومية لحقوق المجتمعات، ووسيلة أساسية لممارسة العديد من الحقوق والحريات الأساسية للأفراد، لاسيما في مجال التعبير والاتصال والحصول على المعلومات، والمرور بالارتفاقات الرقمية، ولم يعد الفضاء الرقمي مجرد أداة تقنية محايدة، بل أصبح مجالا مؤثرا في تشكيل العلاقات الاجتماعية والسياسية والاقتصادية، الأمر الذي استدعى إعادة النظر في منظومة الحماية القانونية التقليدية للحقوق وتوسيعها لتشمل ما بات يعرف بالحقوق الرقمية لارتفاق المواطن (سكينة، 2026، صفحة 336)، ولا جدال في أن الحقوق الرقمية أضحت واقعا ملموسا يجب التعامل معه بحكم ما أفرزته التكنولوجيا الحديثة في إطار ممارسة هذه الحقوق، تلك الحقوق التي تستدعي إعطاء مفهوم واضح وجلي لها، لاسيما وأن تعريفها بشكل جامع ومانع أمر ليس من السهولة بمكان، وذلك بحكم تعدد وتعقيد وسائل التكنولوجيا الحديثة وممارسة الإنسان لحقوقه عبر هذه الوسائل (يوسف، 2025، صفحة 770).

تُعد مسألة الإنفاذ القضائي الفعّال لحقوق الارتفاق الرقمي مشكلة أخرى قائمة بذاتها، وفي مواجهة جميع هذه التحديات، أصبح التنظيم القانوني لحق الولوّج عبر الإنترنت مسألة دولية تتجاوز الحدود الوطنية عبر الدول في إطار التطور التكنولوجي (Giovanella, 2015, p. 203)، ولذلك تتوّجه معظم التشريعات الدولية والسياسات الإنمائية والآليات المتطورة في مجتمع الإنترنت إلى التوافق بشأن تنظيم اتفاقيات دولية موحدة تتضّمن تطوير الإنترنت واستخدامه في شتى مجالات البحث العلمي (Sarlet, 2022, p. 24)، وفي هذا الإطار تضمن الإعلان العالمي لحقوق الإنسان الذي اعتمدته

الجمعية العامة للأمم المتحدة في 10 ديسمبر 1948، أداة دولية غير ملزمة توفر إلهاماً للأدوات الدولية اللاحقة لحقوق الإنسان،وقد تم اعتبار بعض أحكام الإعلان العالمي لحقوق الإنسان من قبل المحاكم والهيئات الدولية قواعد من القانون الدولي العرفي، ويظهر ذلك من خلال ممارسة الدول واعتقادها القانوني، ومن ثم فإن الدول تتحمل مسؤولية قانونية وأخلاقية في ضرورة تمكين أفرادها من التمتع بحق الارتفاق الرقمي عبر الوسائط الالكترونية (يوسف، 2025، صفحة 774).

اعتمد الاتحاد الأوروبي في عام 2000 ميثاق الحقوق الأساسية للاتحاد الأوروبي، وتتضمن المادة 52(3) من الميثاق على أنه طالما يحتوي الميثاق على حقوق تتوافق مع الحقوق المضمونة في الاتفاقية الأوروبية لحقوق الإنسان، فإن معنى ونطاق هذه الحقوق سيكون مطابقاً لما ورد في الاتفاقية الأوروبية، لكن هذا لا يمنع القانون الأوروبي من توفير حماية أوسع مما تقدمه الاتفاقية الأوروبية، باعتبار أن قواعد ممارسة حقوق الإنسان الرقمية ترتكز أساسا على مبادئ وقوانين تمثل حماية فعّالة للحقوق الفردية داخل الفضاء الرقمي (جعفر، 2025، صفحة 115)، ومن المناسب في هذا المجال أن يبدأ التحليل التالي من منظور حقوق الإنسان الدولية في الفضاء السيبراني وفق نظام العهد الدولي الخاص بالحقوق المدنية والسياسية، وذلك مع الاستعانة بالأنظمة الإقليمية لحقوق الإنسان، وكذلك، كما هو الحال في دولة الولايات المتحدة الأمريكية، والأنظمة الوطنية الدستورية لحقوق الإنسان، التي يمكن قياسها في هذا المجال البحثي وفق معيار العهد الدولي الخاص بالحقوق المدنية والسياسية (Kittichaisaree, 2017, p. 52).

باستقراء القضاء الدولي في مجال الارتفاقات الرقمية وحماية الخصوصية الفردية شهدت قضية Kyllo v. United States، استخدم ضباط إنفاذ القانون لجهاز تصوير حراري موّجه نحو منزل خاص من شارع عام للكشف عن كمية الحرارة النسبية داخل المنزل، وقد قضت المحكمة العليا الأمريكية بأنه عندما تستخدم الحكومة جهازًا ليس شائع الاستخدام بين الجمهور، لاستكشاف تفاصيل منزل خاص كانت في السابق غير قابلة للمعرفة دون اقتحام فعلي، فإن هذه المراقبة تُعتبر "تفتيشًا" بموجب التعديل الرابع من قانون الخصوصية الأمريكي، ويفترض أنها غير معقولة دون الحصول على مذكرة إذن بالتفتيش، وبذلك يعد الحق في الخصوصية الرقمية عند ولوج الارتفاقات من الحقوق التي تحميها المواثيق والاتفاقيات الدولية (ابراهيم، 2026، صفحة 207)، وبشكل عام، يبقى الحق في الخصوصية عبر الارتفاق في الفضاء السيبراني موجود وقابل للتنفيذ بموجب الاتفاقيات الدولية المختلفة الملزمة للدول الأطراف، كما يتلقى هذا الحق حماية دستورية ضمن النظام القانوني الداخلي للدول، وبذلك يخضع هذا الحق لبعض الاستثناءات بالنسبة للمستفيدين من خدمات فضاء الإنترنت، باعتبار هؤلاء قد يواجهون إجراءات قانونية لاستخدامهم البيانات الشخصية بدون إذن، وبذلك يعتبر الحق في الخصوصية من أبرز الحقوق المرتبطة بشخصية الإنسان (تحسين، 2025، صفحة 200).

على سبيل المثال، واجهت شركة Facebookدعوى جماعية في الولايات المتحدة بزعم أنها مسحت الرسائل الخاصة للبحث عن روابط لمواقع أطراف ثالثة، ثم شاركتها مع المعلنين والمسوّقين و"جامعي البيانات الآخرين"، دون معرفة المستخدمين أو موافقتهم، وذلك بما يخالف قانون الخصوصية للاتصالات الإلكترونية (ECPA) وقوانين الخصوصية في كاليفورنيا، وقد زُعم أن Facebookحققت 2.7 مليار دولار أمريكي من مبيعات الإعلانات المستهدفة في 2011، وبالمثل، تم اتهام Googleبمسح محتويات رسائل Gmail لغرض مشابه (Kittichaisaree, 2017, p. 57).

إن لجوء دولة ثالثة إلى نظام يقوم على التصديق الذاتي لا يتعارض في حد ذاته مع الشرط الوارد في المادة 25(6) من التوجيه 46/95،الصادر عن البرلمان الأوروبي في 24 أكتوبر 1995 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وبشأن حركة تداول تلك البيانات، الذي يقضي بأن تضمن الدولة المعنية مستوى كافٍ من الحماية بحكم قانونها الداخلي أو التزاماتها الدولية، غير أن موثوقية هذا النظام، في ضوء هذا الشرط، تقوم أساساً على وجود آليات فعّالة للكشف والرقابة التي تتيح تحديد أي انتهاكات للقواعد التي تكفل حماية الحقوق الأساسية في إطار نظام شرعة الحقوق في الفضاء السيبراني (Ziccardi, 2013, p. 153) ، ولاسيما الحق في احترام الحياة الخاصة والحق في حماية البيانات الشخصية، وفي هذا الإطار تمتاز الحقوق الرقمية عبر ارتفاق البيانات بكونها ليست حقوقا مستقلة منعزلة عن منظومة حقوق الإنسان، بل هي امتداد للحقوق الأساسية في العصر الحديث((سكينة، 2026، صفحة 341)،) وعليه لا يجوز للدولة الناقلة للبيانات أن تتخلى عن مسؤوليتها في مراقبة أمن البيانات عند ممارسة حق الارتفاق الرقمي، إذ يكمن في ذلك إثبات المسؤولية من خلال جوهر واجبها في الحماية، على أساس أن الحقوق الرقمية أصبحت جزءا أساسيا من حقوق الإنسان في عصر التكنولوجيا الحديثة (جعفر، 2025، صفحة 118).

أما ما يترتب على ذلك بالنسبة لحماية البيانات الشخصية في شبكات التواصل الاجتماعي، فهو ضرورة وجود مساءلة نهائية تقع على عاتق السلطة السيادية المسؤولة لضمان حماية هذه البيانات، وقد يصل هذا الواجب القائم على المساءلة عند الضرورة إلى حد حماية الفرد حتى من نفسه، كما يمتد أيضاً ليُحدث أثراً أفقياً غير مباشر على الفاعلين من القطاع الخاص فيما يتعلق بالحقوق الأساسية ذات الصلة، وفي جميع الحالات الممكنة ينبغي أن يتمتع الأشخاص الذين تتعلق بهم البيانات الشخصية بضمانات كافية تتيح حماية بياناتهم بفعالية من مخاطر إساءة الاستخدام أو من أي وصول غير مشروع إليها أو استعمال غير قانوني لها (Sarlet, 2022, p. 27).

ثالثا: النظام القانوني للارتفاقات في ظل التعاهد الرقمي العالمي

يرتكز هذا التعاهد على القانون الدولي في ظل تعديلات 2024، بما في ذلك القانون الدولي لحقوق الإنسان، إذ يجب فيه احترام جميع حقوق الإنسان، بما في ذلك الحقوق المدنية والسياسية والاقتصادية والاجتماعية والثقافية والحريات الأساسية، وحمايتها وتعزيزها عبر شبكة الإنترنت وخارجها، وسيُسخَّر التعاون بين الدول من خلال التكنولوجيات الرقمية للنهوض بجميع حقوق الإنسان، بما في ذلك حقوق الطفل وحقوق الأشخاص ذوي الإعاقة والحق في التنمية، ومع تزايد التهديدات السيبرانية التي تستهدف الدول أصبحت الحاجة إلى وضع معايير دولية لتعزيز الأمن السيبراني الدولي أكثر إلحاحا من أي وقت مضى (حيدري، 2025، صفحة 102).

لكي يتمكن كل شخص من المشاركة الكاملة في العالم الرقمي، فلا بد من توافر بيانات وتكنولوجيات وخدمات رقمية ميسورة وبأسعار معقولة، وسيؤدي التعاون الرقمي بين الدول إلى تعزيز إمكانية الوصول الرقمي والارتفاق للجميع بما في ذلك دعم التنوع اللغوي والثقافي في الفضاء الرقمي، وبذلك يتبين أن الهوية الرقمية في ضوء التطورات التقنية الحديثة تمثل صورة حديثة لحق الارتفاق اللصيق بالشخصية القانونية (كوثر، 2026، صفحة 217).

تعمل تقنيات الارتفاقات الرقمية على تحويل عالمنا بشكل جذري، فهي توّفر إمكانات هائلة تعود بالفائدة على رفاهية وتقدم الأفراد والمجتمعات، كما أنها تبّشر بإمكانية تسريع تحقيق أهداف التنمية المستدامة، وذلك من خلال توفير التكنولوجيات الناشئة والموثوقة، بما في ذلك الذكاء الاصطناعي وتحقيق التنمية المستدامة، ويتجلى هذا الطرح من خلال إقامة التعاون بين الدول على إتباع نهج سليم يتسم بالمسؤولية والخضوع للمساءلة والشفافية، بما في ذلك التركيز على الإنسان في كافة مراحل الدورة العمرية للتكنولوجيات الرقمية والناشئة، التي تتضمن مراحل ما قبل التصميم والتصميم والإنشاء، والتقييم والاختبار، والنشر والاستعمال، كما تتضمن البيع والشراء والتشغيل والإخراج من الخدمة، في ظل إشراف بشري فعّال، ولذلك أصبح المجتمع الدولي يواجه تحديات متصاعدة في حماية الخصوصية الرقمية في ظل التطور السريع لتقنيات الذكاء الاصطناعي (نور، 2025، صفحة 500).

لا يمكن للمجتمع الدولي تحقيق التعاون إلا من خلال تعزيز التوافق القانوني الدولي الذي يساهم في سد جميع الفجوات الرقمية بين الدول وداخلها، والمجتمع الدولي المعاصر يدرك جيدا معنى التحديات التي تطرحها هذه الفجوات بالنسبة للعديد من البلدان، ولاسيما الدول النامية التي تواجه احتياجات تنموية ملحة وموارد محدودة، كما أن سد الفجوات الرقمية يتطلب وسائل تنفيذ كافية ومناسبة يمكن التنبؤ بها (Hert, 2015, p. 35)، وبذلك يقوم التعاون الرقمي في إطار الارتفاقات على القانون الدولي، بما في ذلك ميثاق الأمم المتحدة، والقانون الدولي لحقوق الإنسان، والقانون الدولي الإنساني، إضافة إلى أجندة 2030 للتنمية المستدامة، وبذلك تظل الدول في هذا الإطار ملتزمة بنتائج القمة العالمية لمجتمع المعلومات طبقا لمقتضيات إعلان جنيف للمبادئ والمعلومات، وتوّفر الأمم المتحدة في هذا الإطار منصة أساسية للتعاون الرقمي العالمي الذي تحتاجه الدول في مجال الحفاظ على البيانات الشخصية (Rybski, 2021, p. 73).

يسعى التعاهد الرقمي في إطار الارتفاقات إلى سد جميع الفجوات الرقمية وتسريع التقدم نحو تحقيق أهداف التنمية المستدامة، بما في ذلك توسيع الشمول في الاقتصاد الرقمي وتعزيز الاستفادة منه للجميع، بالإضافة إلى تعزيز فضاء رقمي شامل ومفتوح وآمن ومضمون يحترم ويحمي ويعزز حقوق الإنسان بموجب قرار الجمعية العامة للأمم المتحدة رقم A/79/L.2 المؤرخ في 20 سبتمبر 2024، كما يتطلب النهوض بالشمول الرقمي بيئة مواتية تتسم بالشفافية وإمكانية التنبؤ بها، وتشمل هذه البيئة أطر سياسية وقانونية وتنظيمية تدعم الابتكار في إطار بيانات الاتصال الخاصة بالتعريف عبر ولوّج الانترنت (Rybski, 2021, p. 229).

كما يسلم المجتمع الدولي في إطار التعاهد الرقمي العالمي بأن إدارة البيانات على نحو مسؤول وقابل للتطبيق المتبادل تعتبر ضرورة أساسية للنهوض بأهداف التنمية وحماية حقوق الإنسان من أجل تعزيز الابتكار وتشجيع النمو الاقتصادي، وفي غياب معايير فعالة لحماية البيانات الشخصية وحرمة الحياة الخاصة، قد يؤدي تزايد جمع البيانات ومشاركتها وتجهيزها، في نظم الذكاء الاصطناعي وغيرها، إلى زيادة حجم المخاطر، كما يسعى المجتمع الدولي في نفس المجال إلى إشباع الحاجة الملحّة للدول من أجل تعزيز التعاون في مجال إدارة البيانات على جميع المستويات، وذلك بمشاركة فعّالة ومنصفة وحقيقية من جميع البلدان وبالتشاور مع أصحاب المصلحة المعنيين، للانتفاع إلى أقصى حد بالتكنولوجيات الرقمية الناشئة في ظل الارتفاقات (Hert, 2015, p. 153).

المحور الثاني: المسؤولية الدولية الجنائية عن انتهاك الارتفاقات الرقمية

تُعد البنية التحتية الحيوية هدفًا جذابًا للهجمات السيبرانية بسبب أهميتها للمجتمع الرقمي العالمي، وعلى الرغم من عدم وقوع هجمات سيبرانية واسعة النطاق حتى الآن، إلا أن إثارة المسؤولية الجنائية للأفراد والدول في هذا المجال لازالت في طور النشأة، خاصة وأن التطور السريع في التكنولوجيا وانتشار البرمجيات الخبيثة وثغرات الانترنت تزيد من احتمال وقوع مثل هذه الهجمات عبر الارتفاقات الرقمية في المستقبل القريب،كما أن التعاون المحتمل بين القراصنة والمنظمات الإجرامية والجماعات الإرهابية قد يسهّل تنفيذ هجمات سيبرانية معقدة ضد البنى التحتية الحيوية للدول والمنظمات الدولية الفاعلة في المجتمع الدولي المعاصر.

فقد جذبت شعبية الشبكات الاجتماعية على الإنترنت"OSNs "مرتكبي جرائم القرصنة الالكترونية وصانعي البرمجيات الخبيثة الذين يستخدمون هذه الشبكات كمنصات لنشر الفيروسات والديدان الآلية من حاسوب مستخدم إلى آخر، وقد أظهرت الأبحاث أن الجرائم السيبرانية الدولية عبر الارتفاقات الرقمية المستندة إلى الويب يمكن أن تنتشر بسرعة أكبر بكثير من الجرائم الدولية التقليدية(Alhajj & Glässer, 2013, p. 143) .

أولا: التكييف القانوني الدولي للجرائم المرتكبة عبر الارتفاقات الرقمية

تعتبر جرائم الارتفاقات الرقمية من ضمن الجرائم ذات البعد الدولي، فهذا النوع من الجرائم لا يتحّدد بحدود دولة معينة، ويرجع ذلك إلى استخدام شبكات الانترنت العالمية، وهي بذلك تثير الكثير من التحديات القانونية، وسبب صعوبة مواجهتها يعود إلى الإشكالات القانونية المتعلقة بملاحقة وتسليم المجرمين عبر الحدود الدولية (زهراء، 2025، صفحة 392) ، وفي هذا المجال تتجلى الاتفاقيات والمواثيق الدولية باعتبارها من أهم صور التعاون الدولي، ويبرز هذا التعاون في تكييف حقل مكافحة الجرائم السيبرانية عبر الارتفاقات الرقمية، ومن بين هذه المعاهدات ظهرت على الساحة الدولية عدة نصوص قانونية ناجعة أثبتت فعاليتها في مكافحة الجرائم السيبرانية والقرصنة الالكترونية،كمعاهدة بودابست لمكافحة جرائم الانترنت وتوصيات المجلس الأوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات (زهراء، 2025، صفحة 398).

في هذا الإطار يهتم العديد من الباحثين بموضوع الإجرام السيبراني عبر الارتفاقات وكيفية الوقاية منه، إلا أنه من الصعب الاتفاق على تعريف أو تكييف دقيق له، فالتمييز بين الجريمة السيبرانية والقرصنة الالكترونية عبر الارتفاقات ومختلف الجرائم الدولية التقليدية يصبح غير واضح عند محاولة وصف القرصنة أوالهجوم على الشبكة الحاسوبية بطريقة مشابهة للهجمات في العالم المادي(Chen, Jarvis, & Macdonald, 2014, p. 123) ، وعندما يتعلق الأمر بالجريمة السيبرانية، فإن الموقع يشمل كلا المجالين المادي والرقمي، ومع ذلك فإن الحدود والأماكن الواضحة والمتعارف عليها في العالم المادي غير متوفرة في العالم الافتراضي، ولذلك لا تزال هناك بعض الحدود التي تميز بين العالم المادي والعالم السيبراني؛ فالكيبورد، الشاشة، المؤشر، وكلمة المرور كلها تعمل كوسيط بين العالمين، لكن بمجرد الدخول إلى الفضاء السيبراني، تصبح فكرة الحدود أقل وضوحًا، فالعالم السيبراني لا يمتلك حدودًا جغرافية واضحة كما في العالم المادي، وبذلك تلعب

التكنولوجيا دورًا رئيسيًا في تعريف الجرائم السيبرانية حسب الدور الذي تؤديه بما يشمل إنهاك التجارة، الأمن الوطني، السلامة العامة، النزاعات، وسبل الرد على الإساءة(Ramírez, A, & García-Segura, 2017, p. 27) .

باستقراء أهم آراء الفقه والقضاء الدولي حول تكييف الجريمة الدولية نجد أن العلاقة بين الارتفاقات الرقمية وجرائم الحرب السيبرانية تتجلى في اعتبار هذه الأخيرة عبارة عن انتهاكات جسيمة للقواعد العرفية وقواعد المعاهدات الدولية التي تشكل جزءا من القانون الإنساني الدولي، أو ما يسمى أيضا بالقانون الدولي للنزاعات المسلحة (كاسيزي، 2015، صفحة 137)، كما أن دخول الذكاء الاصطناعي إلى ميدان النزاع المسلح عبر تقنية الارتفاقات لا يعد مجرد تطور تقني في علوم الحرب السيبرانية، بل يمثل تحولا نوعيا في طبيعة الفاعلية الجنائية الدولية، ويطرح تحديات عميقة أمام القانون الدولي الإنساني، فغياب الفاعل البشري المباشر في بعض الجرائم الدولية المرتكبة بواسطة الأنظمة الذكية يربك مفهوم النية والسيطرة والمساءلة، ويهدد فعالية منظومة العدالة الدولية، ومع ذلك فإن هذا التحدي يمكن أن يتحول إلى فرصة لإعادة صياغة المفاهيم القانونية، وتطوير أدوات مساءلة أكثر شمولا، تراعي في ذلك تعقيدات الواقع الرقمي دون التفريط في المبادئ الإنسانية (بحص، 2025، صفحة 327).

لقد تبلور مفهوم الحرب السيبرانية في شكله العالمي مع ظهور التكنولوجيا الجديدة، وتطور إحدى أكثر التقنيات الحديثة إثارة للاهتمام والمتمثلة استخدام أنظمة الطيران بدون طيار، وذلك عبر توظيف تقنيات الذكاء الاصطناعي والتحكم عبر منصات الارتفاقات الرقمية، والتي تسمح بإمكانية استقبال وتوجيه للطيران بطائرات دون وجود طيار على متنها، وهو ما يعرفه الجمهور العام بشكل أوسع باستخدام "الدرون" في المجال العسكري، مما يفتح أفقًا جديدًا تمامًا للحرب وتسييرها عبر فضاءات الارتفاقات الرقمية، وهذا بلا شك يساهم بشكل كبير في الجاذبية الحالية لدراسة استخدام أنظمة الطيران الموجهة عن بعد(RPAS) (Heintze & Thielborger, 2016, p. 107) .

ترتكز جريمة العدوان السيبراني عبر الحدود الرقمية الدولية على المضمون الوارد في المادة 8 مكرر من نظام روما الأساسي للمحكمة الجنائية الدولية، والتي تم اعتمادها في مؤتمر كمبالا لسنة 2010 بشأن الأفعال التي تعد جريمة عدوان من خلال التخطيط أو التحضير أو شن أو تنفيذ عمل سيبراني عدواني يشكل بحدته وجسامته وحجمه انتهاكا واضحا لميثاق الأمم المتحدة، من قبل شخص يتمتع بمنصب يخوله التحكم أو السيطرة على العمل السياسي أو العسكري للدولة، ويشير القسم 02 إلى أن العمل العدواني يشمل استعمال القوة المسلحة من قبل دولة ما ضد سيادة دولة أخرى أو سلامتها الإقليمية أو استقلالها السياسي، أو بأي صورة آخري تتنافى مع ميثاق الأمم المتحدة (كاسيزي، 2015، صفحة 271)، والعدوان السيبراني هو جريمة عابرة للارتفاقات الرقمية والحدود الدولية من خلال عناصر مختلفة بموجب القانون الدولي الجنائي (ريكان، 2025، صفحة 606)

تتعرض الارتفاقات الرقمية في العالم إلى هجمات الإرهاب السيبراني الدولي ، وفي هذا الإطار تتجلى العلاقة بين ارتكاب جرائم الإرهاب الدولي واستخدام تقنيات الولوج عبر الارتفاقات الرقمية، والغرض من العمليات الإرهابية عبر الارتفاقات هو استهداف الارهابيين في نشر الخوف بين رواد مواقع التواصل الاجتماعي وإضعاف اقتصاديات الدول أو إرغام حكومة ما أو منظمة دولية على القيام أو الامتناع عن القيام بفعل معين (كاسيزي، 2015، صفحة 288)، وقد

تصاعدت في العقود الأخيرة وتيرة التهديدات الإرهابية بفعل التقدم التكنولوجي المتسارع، إذْ لم تعد الأفعال الإرهابية الدولية تقتصر على ساحة المعركة التقليدية، بل باتت الارتفاقات الرقمية تستخدم كجبهات جديدة للصراع السيبراني، وقد أفرز هذا التحول مفهوما معقدا ومتعدد الأبعاد يعرف بالإرهاب السيبراني الدولي، وهو نوع جديد من الإرهاب الدولي الذي يقوم بتوّظيف تقنيات المعلومات والاتصالات بما في ذلك حقوق الارتفاق الالكتروني، وذلك بهدف زعزعة وإخلال استقرار الدول، وتهديد أمن المجتمعات من خلال هجمات الكترونية تستهدف البنى التحتية الحيوية (عواد، 2025، صفحة 102).

ثانيا: إجراءات التحقيق الدولي في حالة انتهاك قواعد الارتفاق الرقمي

يعد الذكاء الاصطناعي "AI" فرعًا راسخًا من فروع علوم الحاسوب الذي يهتم بجعل الآلات ذكية بما يكفي لأداء مهام حسابية كبيرة أو معقدة تتطلب عادةً ذكاءً بشريًا، كما أنه يتكون من مجموعة من التقنيات القادرة على استخراج الرؤى والأنماط من كميات هائلة من البيانات، وهو عنصر أساسي فعّال في التحليل الجنائي الرقمي والتنقيب عن البيانات المتعلقة بالأدلة الجنائية الرقمية، ولذلك، وبما أن التحليل الجنائي يتطلب تحليلًا ذكيًا لبيانات كبيرة ومعقدة (Ruggeri, 2022, p. 119)، فإن الذكاء الاصطناعي يمثل خيارًا مثاليًا لمعالجة المشكلات التحليلية الرئيسية التي تواجه الأدلة الجنائية الرقمية، ويمكن للذكاء الاصطناعي في هذا المجال أن يساعد في أتمتة بعض العمليات واكتشاف المحتوى المشبوه بسرعة أكبر، أو تقديم رؤى قد يستغرق اكتشافها وقتًا أطول من قبل المحققين، وأثناء التحليل الجنائي عند الخبراء يمكن تحديد مجموعات مختلفة من البيانات باستخدام التعرف على الأنماط الرقمية، والذي يعتمد في وظيفته على الإحصاء أو الاستدلال الاحتمالي أو كليهما، ويمكن تطبيق الذكاء الاصطناعي على الصور والنصوص وصور الأقراص لتحديد مجموعات ذات أهمية أثناء التحقيق، كما يستطيع الذكاء الاصطناعي تحديد هذه الأنماط في البيانات المعقدة بدقة أكبر(Iqbal, Debbabi, & Fung, 2020, p. 140) .

يعد التحقيق في الأجهزة المحمولة في العالم مهمة صعبة نسبيًا، وذلك بسبب وجود أنواع مختلفة من الأجهزة المتداولة في إطار التقدم التكنولوجي الحديث، ولهذا يحتاج خبير الأدلة الجنائية للأجهزة المحمولة إلى مهارات عالية حتى يتمكن من إجراء التحقيقات بكفاءة، كما أن امتلاك معرفة جيدة بالأدلة الجنائية للحاسوب وأدواتها لا يكفي ليصبح الشخص خبيرًا في الأدلة الجنائية للأجهزة المحمولة، أما على المستوى المنطقي، فرغم أن البيانات تكون مقروءة للبشر، إلا أن كمية البيانات المستخرجة تكون أقل، وقد يؤدي ذلك إلى فقدان بعض المعلومات الحساسة المهمة للمحقق، ولهذا يجد خبير الأدلة الجنائية نفسه أمام مأزق في اختيار الطريقة الأنسب لاستخراج البيانات(Iorliam, 2019, p. 37) .

توضح هذه التحليلات أيضًا أن الجرائم السيبرانية المرتكبة عبر الارتفاقات الرقمية تتعلق بالبرمجيات الخبيثة مثل ديدان XSSو Trojanو Clickjacking التي لا تنتشر بشكل عشوائي، بل تستغل الهيكل الشبكي الفعلي للشبكة الاجتماعية والارتفاقات على الإنترنت، مستفيدة بذلك من خصائص عديدة، مثل قصر المسافات الشبكية وارتفاع التجميع المحلي وتوزيع درجات العقد وفقًا لقانون القوة العالمي، هذه الخصائص تجعل الشبكة الاجتماعية بيئة مثالية لانتشار البرمجيات الخبيثة والجرائم الدولية الرقمية بسرعة وكفاءة، مقارنة بالبيئات التقليدية أو الشبكات الأقل تواصلاً عبر

العالم، ومن خلال النماذج التحليلية والمحاكاة، يمكن أيضًا اختبار سيناريوهات مختلفة للوقاية، مثل تعطيل روابط معينة أو تصفية المحتوى المشبوه، وتقييم مدى فعاليتها قبل تطبيقها في العالم الحقيقي، كما تساعد هذه الدراسات مطوري الشبكات الاجتماعية والباحثين في الأمن السيبراني على فهم التهديدات الجديدة وتصميم أدوات كشف الجرائم السيبرانية المرتكبة عبر نظام الارتفاقات، وإزالة البرمجيات الخبيثة بشكل أكثر دقة وفعالية(Alhajj & Glässer, 2013, p. 146) .

ثالثا: محاكمة مرتكبي جرائم الارتفاقات الرقمية أمام القضاء الدولي الجنائي.

بموجب قواعد القانون الدولي الجنائي، يمكن للدولة أن تمارس الولاية القضائية خارج حدودها للبحث عن الأدلة الحاسوبية بموافقة الدولة الإقليمية التي توجد بها الأدلة، ما لم يكن هناك اتفاق ملزم بين الدول المعنية ينص على خلاف ذلك، فعلى سبيل المثال، تتضمن المادة 4 من اتفاقية مكافحة الجريمة المنظمة العابرة للحدود 2000 على القاعدة المقبولة عمومًا بأن الدول الأطراف يجب أن تنفذ التزاماتها بموجب الاتفاقية بما يتوافق مع مبادئ المساواة السيادية وسلامة أراضي الدول وعدم التدخل في الشؤون الداخلية للدول الأخرى، كما أن الاتفاقية لا تمنح أي دولة طرف الحق في ممارسة الولاية القضائية أو القيام بوظائف محجوزة حصريًا للسلطات المحلية للدولة الأخرى وفق قانونها الداخلي بالكامل (Sellers & Maxeiner, London, p. 47).

تأخذ مسألة الولاية القضائية خارج الإقليم بعدًا جديدًا عند تطبيقها على الحوسبة السحابية، نظرًا لغياب أي أجهزة مادية محددة، وقد تتجاوز مواقع البيانات الحدود الوطنية وقد لا تكون معروفة للمستخدمين، مما يطرح التساؤل عن ولاية أي دولة في المقام الأول، وقد تتم معالجة البيانات في الحوسبة السحابية في عدة دول في وقت واحد، ومن ثم، يُفترض أن أكثر من دولة قد يكون لديها اختصاص قضائي متزامن على جريمة ارتكبت عبر الحوسبة السحابية، وفقًا لأي من أسس الاختصاص القضائي المذكورة أعلاه، طالما أنها قابلة للتطبيق على الوقائع محل البحث، وقد أصبح من المقبول أن تمارس الدولة الاختصاص القضائي استنادًا إلى مبدأ الشخصية السلبية، ومبدأ الشخصية الإيجابية، ومبدأ الحماية للتعامل مع الترابط العالمي، والتقنيات الهشّة، بما في ذلك الطابع المجهول للهوية في الفضاء السيبراني خاصة عند استخدام الارتفاق الرقمي عبر البطاقات الذكية (Leslie, 2014, p. 285).

بموجب مبدأ الشخصية الإيجابية للاختصاص القضائي يمكن إحالة مرتكبي الجرائم المنتهكة لفضاء الارتفاق الرقمي أمام المحكمة الجنائية الدولية في حالة ما إذا تم تكييفها على أنها جرائم دولية حسب مقتضيات المادة 05 من نظام روما الأساسي، كما يمكن للدولة ممارسة اختصاصها على الجاني على أساس أن الجاني مواطن من مواطني تلك الدولة، وفي هذا الإطار قد أعلنت عدة دول اختصاصها على الجاني على أساس أن ضحية الجريمة مواطن من مواطني تلك الدولة، ويستند هذا إلى مبدأ الشخصية السلبية للاختصاص القضائي، وقد أشار ثلاثة قضاة في المحكمة الجنائية الدولية في فبراير/شباط 2002 إلى أن اختصاص الشخصية السلبية، الذي كان يُعتبر سابقًا مثيرًا للجدل، أصبح اليوم جزءًا من تشريعات عدة دول بما في ذلك الولايات المتحدة الأمريكية وفرنسا، ويلاقي اليوم معارضة قليلة نسبيًا، على الأقل فيما يتعلق بفئة معينة من الجرائم السيبرانية، وكلما كانت الجرائم أكثر خطورة، كلما قل احتمال مواجهة المعارضة الدولية لممارسة اختصاص الشخصية السلبية، وبناءً على مبدأ الحماية، يمكن للدولة ممارسة الاختصاص القضائي على الجاني

الذي يشكّل سلوكه في الخارج تهديدًا لأمن تلك الدولة أو يتدخل في أداء وظائف حكومتها بخلاف الاختصاص القضائي التقليدي (Callanan, 2015, p. 50).

أما أكثر أسس الاختصاص القضائي إثارة للجدل فهو الاختصاص القضائي العالمي، حيث تمارس الدولة اختصاصها على جريمة ليس لها أي صلة بالدولة على الإطلاق، بمعنى أن الجريمة ارتُكبت خارج أراضيها، ولا تؤثر فيها، ولا يكون الجاني أو الضحية من مواطنيها، وقد أصبح مقبولًا منذ فترة طويلة أن لكل دولة الحق في ممارسة الاختصاص القضائي العالمي على مرتكبي القرصنة الالكترونية عبر ارتفاقات الانترنت (Callanan, 2015, p. 52)، أما غير ذلك، فلا يزال مثيرا للجدل ما إذا كان يمكن للدولة ممارسة الاختصاص القضائي العالمي في غياب التزامات معاهدة تلزم الدول المعنية، كما هو الحال في الالتزام بالملاحقة القضائية أو التسليم المنصوص عليه في العديد من الاتفاقيات الدولية.

وفي هذا السياق، تجدر الإشارة إلى أن الاتفاقية المتعلقة بالجريمة الالكترونية أو اتفاقية بودابست لعام 2001، والتي تعد الاتفاقية متعددة الأطراف الوحيدة السارية بشأن الجرائم السيبرانية، تستخدم الاختصاص القضائي الإقليمي والاختصاص القضائي القائم على جنسية الجاني كأساس لممارسة الاختصاص على الجرائم السيبرانية، ووفقًا لدراسة أجراها مكتب الأمم المتحدة الإقليمي المعني بالمخدرات والجريمة، فإن أشكال الاختصاص القضائي القائمة على الإقليمية أو الجنسية تكون عادة قادرة على ضمان وجود صلة كافية بين أفعال الجرائم السيبرانية ودولة واحدة على الأقل، ويُشير الاختصاص القضائي القائم على الإقليمية إلى أنه يمكن تحديده بالرجوع إلى عناصر أو آثار الجريمة السيبرانية، أو موقع أنظمة الحاسوب أو البيانات المستخدمة في ارتكاب الجريمة (Giovanella, 2015, p. 70) .

تتضمن المادة 22 من اتفاقية مجلس أوروبا بشأن الجرائم السيبرانية "المعروفة باتفاقية بودابست"مجموع المبادئ الأساسية للاختصاص القضائي فيما يتعلق بالجرائم السيبرانية، وتتضمن المادة 22(1)(أ) من الاتفاقية على وجوب إقرار الاختصاص القضائي بالنسبة لجرائم الجرائم السيبرانية الواردة في الاتفاقية عندما تُرتكب داخل إقليم الدول الأطراف في الاتفاقية، كما تتضمن المادة 22(1)(د) من الاتفاقية على أنه ينبغي أيضًا إقرار الاختصاص القضائي بالنسبة لجرائم الفضاء السيبراني المنصوص عليها في الاتفاقية، في حالة إذا ارتكبها أحد مواطني دولة طرف في الاتفاقية، وذلك في حال كانت الجريمة معاقبًا عليها بموجب القانون في الولاية القضائية التي اكتملت فيها الجريمة، أو إذا ارتكبت خارج النطاق الإقليمي لأي دولة (Leslie, 2014, p. 295).

المحور الثالث: الإشكالات التي يثيرها التعاون الدولي في إطار الحماية الجنائية للارتفاقات الرقمية

نتيجة لتزايد قلق المجتمع الدولي إزاء التصاعد المطرد للجريمة، وتطورها المتلاحق واقترانها بالتقدم التقني في مجال الارتفاقات الرقمية، وما أحدثه من ثورة واسعة النطاق في نظم المواصلات والاتصالات والمعلومات، ازدادت قناعة المجتمع الدولي بالحاجة الماسة لمواجهة التحديات التي يفرضها الفضاء الرقمي العالمي (العطوي، 2013، صفحة 9)، باعتبار أن هذا العالم الجديد يقوم على شبكة الانترنت التي تمثل المكون الرئيسي للفضاء السيبراني أو الالكتروني.

فقد أصبح الارتفاق الرقمي يمثل أحد أهم تقنيات الاستخدام المزدوج الذي يمكن أن يكون لأغراض ايجابية أو سلبية، بحسب نية مستخدميها، مما أوجب على الدول في مختلف المحافل العالمية أن تولي اهتماما خاصا لهذا الموضوع

الحساس، الذي يتطلب بالضرورة أن يتعامل المجتمع الدولي مع التحديات القانونية والحقوقية التي تفرضها أنشطة الفضاء السيبراني (سعد، 2025، صفحة 223).

أولا: إشكالية توحيد قواعد القانون الدولي بشأن حماية الارتفاقات الرقمية

أصبحت مشاركة المعرفة والتعاون الدولي حول الهجمات السيبرانية تتحقق بمجرد نقرة واحدة في الفضاء السيبراني، وهذا ما أدى إلى تسهيل انتشار الأسلحة السيبرانية أو طرق الهجوم، وقد أُشير إلى أنه خلال أسابيع من اكتشاف نظام "Stuxnet"بالولايات المتحدة الأمريكية، ظهرت دراسة قانونية حديثة لمشروع "راند" للقوات الجوية حول دمج الأسلحة الحركية وغير الحركية بعنوان "القدرات غير الحركية للولايات المتحدة والتهديدات"، المنشورة في عام 2011، إلا أن مبرر سباق التسلح النووي والأسلحة الحركية الأخرى لا ينطبق على الأسلحة السيبرانية، فالهجمات السيبرانية في حد ذاتها لا يمكنها تعطيل القدرات السيبرانية لدولة أخرى بالكامل، كما أنه لا يوجد سبب قانوني مقنع لتطوير أسلحة سيبرانية هجومية لمجرد أن لدى الدولة المحتملة عدواً يمتلكها، إذ أن أفضل رد على الهجوم السيبراني الهجومي هو معالجة الثغرات في نظام الدولة السيبراني، الذي قد يسمح بحدوث هذا الهجوم، وبالتالي لم يتوصل الفقه والقضاء إلى تعريف محدد ودقيق للذكاء الاصطناعي باعتباره موضوع واسع ومعقد، فلا يوجد تعريف متفق عليه (محمّد، 2025، صفحة 17).

فعلى المستوى المحلي، تثير أنشطة المراقبة لأنظمة" RPAS "مخاوف كبيرة فيما يتعلق بحماية البيانات، إذا تم استخدام" RPAS "لأغراض المراقبة المدنية، وبالتالي يجب أن تكون مثل هذه المبادرات متوافقة مع القانون الفيدرالي لحماية البيانات وقوانين أخرى تتعلق بحماية الخصوصية الرقمية للأشخاص المحميين بموجب القانون الدولي (Heintze & Thielborger, 2016, p. 110)، كما أن الفضاء السيبراني أصبح يحتاج إلى التنظيم القانوني، وبذلك لم تبدأ بعد المناقشات حول إثارة المسؤولية الجنائية الدولية، وكيفية الإدارة، وبأي تكلفة يمكن تأسيس التنظيم والسيطرة، ولكن حتى يتم تنفيذ ذلك بفعالية، سواء على المستوى الفردي أو الجماعي الدولي، يظل التعرّف على التحديات القائمة، وتوظيف الموارد، وإدارة الجهود لمواجهة التهديدات البيئية الرقمية القائمة، والتي يمكن القول أنها عالمية بحسب مختلف الدراسات الحديثة في القانون الدولي(Ramírez, A, & García-Segura, 2017, p. 29) .

يدعو مشروع مدونة السلوك الدولية لأمن المعلومات المقدم في عام 2013 من قبل الصين، وروسيا، وطاجيكستان، وأوزبكستان إلى حظر استخدام تكنولوجيا المعلومات والاتصالات"ICTs " لتنفيذ أعمال عدائية أو أعمال عدوانية، أو لتهديد السلام والأمن الدوليين، أو لنشر أسلحة معلوماتية أو تقنيات ذات صلة، وفيما يخص أوروبا، تفرض لائحتا المجلس الأوروبي 2012/36 و2012/264 قيوداً على تصدير المعدات والتقنيات وبعض المواد التي قد تُستخدم للمراقبة أو اعتراض الاتصالات عبر الإنترنت، أو الهاتف إلى سوريا وإيران على التوالي، ويمكن تبرير هذه القيود بموجب المادة 21 ب-2 من اتفاقية الجات لعام 1994، التي تسمح للأطراف المتعاقدة باتخاذ أي إجراء تعتبره ضرورياً لحماية مصالحها الأمنية الأساسية المتعلقة.

لقد تم اقتراح عدة إصلاحات في القانون الدولي العام لحماية حقوق الإنسان في الفضاء السيبراني بشكل أفضل، على سبيل المثال، اقترح القاضي "ستاين شجولبرغ"، رئيس مركز الفكر العالمي للسلام والعدالة في الفضاء السيبراني،

إنشاء المحكمة الجنائية الدولية للفضاء السيبراني "لمنع الجرائم السيبرانية الخطيرة والمنظمة على المستوى العالمي، وحماية السلام، وضمان ألا تمر أخطر الجرائم الدولية في الفضاء السيبراني دون عقاب، أي أن يتم ذلك من خلال مراقبة الاتصالات الإلكترونية خارج الحدود في التحقيقات الجنائية التي ستتطلب موافقة المحكمة أو مكتب المدعي العام في المحكمة، وكلما كان هناك سبب محتمل للاعتقاد بأن أي شخص مشتبه به في ارتكاب أو محاولة ارتكاب أي هجمات سيبرانية وجرائم سيبرانية أخرى سيخضع للمحاكمة الدولية" (Ramírez، A، و García-Segura، 2017، صفحة 369).

قد يؤدي تحسين آلية تقديم المساعدة القانونية المتبادلة"MLATs " استنادًا إلى معاهدات ثنائية أو متعددة الأطراف، والتي ستكون ملزمة للدول المعنية من خلال جعل الدول أكثر ثقة في استخدام هذه الآلية بدلًا من اللجوء إلى المراقبة السرية خارج الحدود لقمع الجرائم العابرة للارتفاقات الرقمية، وفي هذا الإطار لجأت أكثر من 70٪ من الدول إلى انتهاج إستراتيجية مكتب الأمم المتحدة لمكافحة الجرائم السيبرانية عبر الارتفاقات، وبذلك يتيح الإنترنت فرصًا غير مسبوقة للتعبير عن التعاون الجنائي العالمي، لكن هذه الفرصة تُضاعف الأضرار الناتجة عن استخدام المواد المحمية بحقوق الارتفاق، ومع سهولة تحميل وتوزيع الملفات، أصبح انتهاك حقوق الارتفاق الرقمي أكثر سهولة وتكرارًا، وهذا ما يجعل تعاون الدول وشركات المزودين بالانترنت ضروريًا للحد من الانتهاكات، لاسيما أن المزودين غالبًا ما يكونون الجهة الوحيدة القادرة على الوصول إلى المحتوى المخالف وتنفيذه أو اتخاذ الإجراءات المناسبة (Floridi، 2017، صفحة 374).

في ذات الإطار يعتبر تقييد الوصول إلى الانترنت انتهاكا للقانون الدولي لحقوق الإنسان، حيث أضحت الحقوق الرقمية رديفا لحقوق الإنسان في العالم المادي، ولذلك يثور الإشكال القانوني في هذا المجال عندما يرتبط ويختلط مفهوم الارتفاق الرقمي بالحق في الخصوصية وحرية التعبير، وبالتالي سيجد المشرع الدولي نفسه محاطا بعدة صعوبات تتعلق بتحديد القانون الواجب التطبيق في حالة ارتكاب الجرائم السيبرانية عبر نظام الارتفاق الرقمي (الصادق، 2022، صفحة 47).

ثانيا: إشكالية الموازنة بين الحماية الجنائية للخصوصية واستفاء الحق في ميراث الارتفاق الرقمي

يعد ضمان الحق في الخصوصية عبر الانترنت أمر ضروري لضمان ثقة الأفراد في ممارسة حقوقهم دون المساس بها أو انتهاكها (ابراهيم، 2026، صفحة 209)، فقد أعلنت الجمعية العالمية للخصوصية GPA في قرارها المتعلق بحماية المراقبة وحماية الخصوصية في 2024 عن التقدم التكنولوجي الحقوقي المرافق لعصرنا وفق تقنيات المراقبة وأنظمة تحديد المواقع، مما يستلزم أهمية بالغة لحماية البيانات الشخصية والخصوصية باعتبارها حقا أساسيا من حقوق الإنسان (نور، 2025، صفحة 502)، فإذا كانت الحماية الجنائية الموضوعية للحق في الخصوصية الرقمية تتمثل في تلك النصوص القانونية التي تتناول التجريم والعقاب المتعلق بالاعتداء أو المساس بهذا الحق، فان الحماية الإجرائية للحق في الخصوصية الرقمية يتمثل في تلك النصوص الجزائية، فضلا عن الضوابط والضمانات المقررة لضبط هذه الإجراءات وعدم التعسف في استعمالها من طرف السلطات المختصة (سعاد، 2026، صفحة 160)، فالحق في الخصوصية الرقمية يكون مكفول قانونا وقضاء، سواء في الصكوك الدولية وعلى رأسها الإعلان العامي لحقوق الإنسان، وكذلك العديد من الاتفاقيات الدولية والإقليمية والمؤتمرات (باسم، 2025، صفحة 878).

يشير التعريف السائد بين الفقهاء القانونيين إلى أن" حق الميراث الوارد على الارتفاق الرقمي يتضمن جميع البيانات الإلكترونية للشخص المتوفى"، ويُعد هذا التعريف متوافقًا مع طبيعة البيانات الرقمية المتطابقة في الجودة والشكل، مما يستدعي أيضًا شمول البيانات المخزنة عبر وسائط تخزين الشخص المتوفى، كما أن الظل الرقمي، الذي أصبح أكثر فأكثر يمثل جزءًا من شخصية الإنسان، والذي لا يتجلى فقط من خلال حسابات البريد الإلكتروني أو الشبكات الاجتماعية، بل أيضًا عبر المحتوى المخزن محليًا، مثل الأقراص الصلبة، أقراصUSB ، بطاقاتSIM ، ذاكرة الهواتف الذكية، أو المحتوى المخزن على الإنترنت الذي يمكن أن ينتقل إلى ورثة المستخدم (Mackenrodt, 2018, p. 281)، ويشمل الحق في الميراث الرقمي كلمة المرور واسم المستخدم، كما يمكن أن تخضع البيانات المتصلة بالإنترنت وغير المتصلة بالإنترنت أيضًا لحقوق الملكية الفكرية، مثل حقوق الارتفاق الرقمي المتعلقة بالولوّج للصور والفيديوهات، وتكون علاقة ورثة المستخدم المتوفي مع مزودي الوصول والاستضافة عقدية بطبيعتها، على نفس النحو الذي تنطبق فيه العلاقة مع DENIC بخصوص الملكية وحق استخدام اسم نطاق معين (Iqbal, Debbabi, & Fung, 2020, p. 143).

يستند قانون الإرث الألماني إلى مبدأ الخلافة الشاملة "Universal Succession" ويشكل هذا المبدأ أحد الطرق الممكنة لتحديد انتقال الحقوق إلى الورثة، لكنه ليس مضمونًا بموجب المادة 14(1) الفقرة 1 البديل 2 من القانون الأساسي الألماني، ونظرًا لغياب أحكام قانونية محددة بشأن ميراث الارتفاق الرقمي، فإن البيانات المتصلة بالإنترنت من حسابات البريد الإلكتروني وحسابات الشبكات الاجتماعية، وكذلك العقود الأساسية لتلك الحسابات، تخضع أيضًا لهذا المبدأ، ومع ذلك، تمامًا كما قد يحتوي الإرث التناظري على مراكز قانونية غير قابلة للوراثة، كما قد تكون هناك أسباب أخرى لاستبعاد أجزاء من الميراث الرقمي القابل للانتقال إلى الورثة (Sarlet, 2022, p. 386).

تناولت الإجراءات أمام المحاكم الألمانية في ظل قرارات محكمة LG برلين 17 ديسمبر 2015، KGبرلين 31 مايو 2017، والمحكمة الاتحادية العليا 12 يوليو 2018 ، بعض الجوانب والمشكلات القانونية المتعلقة بالميراث الرقمي، ومع ذلك، تعتبر قرارات هذه المحاكم مهمة للأسئلة البارزة التي نوقشت في هذا السياق، فعلى سبيل المثال وفي إطار حيثيات إحدى القضايا الدولية المشهورة رفعت "أم" دعوى ضد شبكة Facebook" للحصول على وصول غير مقيد إلى كامل حساب ابنتها المستخدمة والبيانات المرتبطة بها ،وخاصة الرسائل المخزنة ضمن الحساب الالكتروني لابنتها، التي توفيت في 3 ديسمبر 2012 عن عمر يناهز 15 عامًا لأسباب غير معروفة بعد، بعد أن صدمها قطار مترو، وقد كانت المدعية تأمل في الحصول على معلومات من محتوى الاتصالات حول احتمال إعادة التحقيق في جريمة انتحار أو جريمة التحريض على الانتحار المتعلقة بابنتها، وكذلك ولدرء دعوى تعويضات رفعها سائق المترو، على الرغم من أن الابنة قد سلمت بيانات الوصول الخاصة بها لوالديها، لكن الأم لم تتمكن من الوصول إلى محتوى الاتصالات، وبعد أن أبلغ شخص ثالث Facebookبالوفاة، تم تحويل الحساب إلى وضع تذكاري بواسطة المزود، مما يعني أن الأصدقاء المسجلين فقط للمتوفاة استمروا في الوصول، وعند تسجيل دخول الوالدين، ظهرت إشعارات حول وضع الحساب التذكاري فقط، وتم رفض أي وصول إضافي (Ruggeri, 2022, p. 42).

لقد أوضحت المحكمة الاتحادية العليا أن الحق التعاقدي في الحصول على الوصول إلى حساب المستخدم المتوفى وجميع البيانات المحتواة فيه قابل للوراثة وفقًا لمبدأ الخلافة الشاملة المنصوص عليه في المادة 1922(1) من القانون المدني الألماني، ولا يشكل حماية الحقوق الشخصية للمتوفى بعد الوفاة، أو سرية الاتصالات، أو أحكام حماية البيانات، أو الحق العام للشخصية لصالح شركاء اتصال المتوفى أي عائق أمام الورثة في ممارسة هذا الحق، وبذلك، عارضت المحكمة الاتحادية العليا قرار KG برلين الذي ترك مسألة قابلية الوراثة مفتوحة صراحة، وأكدت ما ورد في حكم LG برلين، وعلى غرار الحالات السابقة، لم تحدد المحكمة الاتحادية العليا الشروط العامة لاستخدام"Facebook " ولا طبيعة عقد المستخدم كعائق أمام قابلية الوراثة للحق في الوصول إلى الحساب، وفي هذا الإطار لم تتضح بعد قواعد الحماية الجنائية وقابلية التحقيق القضائي الجنائي في استعمال حساب المستخدم، وبالموازاة مع ذلك اعتمد قضاة المحكمة على نظرية الالتزامات التعاقدية لمزود الشبكة الاجتماعية باعتبارها هي الجوهر القانوني في قضية الحال، كما أن المحتوى الذي أضافه المستخدمون هو الذي يحمل طابعًا شخصيًا، والالتزامات التعاقدية تظل مرتبطة فقط بالحساب ذاته (Ruggeri, 2022, p. 43).

اتباعًا للمحاكم الأدنى، قضت المحكمة الاتحادية العليا في ألمانيا بأن التفريق الصارم بين البيانات الشخصية من جهة والبيانات المرتبطة بالممتلكات من جهة أخرى، لا يكون ممكنًا عمليًا ولا متأصلًا في قانون الإرث الألماني، باعتبار أن هناك معاملة مختلفة للميراث الرقمي مقابل الميراث التناظري مما سيؤدي إلى نتائج غير مناسبة ولا يمكن تبريرها، وبما أن أصحاب الحقوق، عادة الأقرباء، قد يمارسون فقط حقوق دفاعية وحقوق إلغاء تجاه الأطراف الثالثة بدلًا من المطالبة بالوصول إلى الميراث الرقمي للمتوفى، كما أن حماية الحقوق الشخصية للمتوفى بعد الوفاة لا تمنع أيضًا الوراثة وفقًا للمحكمة الاتحادية العليا، والحماية الجنائية لسرية الاتصالات ستكون لصالح شركاء الاتصال للمتوفى، وهذا ما تمت مناقشته بشكل واسع على مستوى قواعد القانون الدولي (Sarlet, 2022, p. 383).

نظرًا لأن الكثير من معالجة البيانات يتم تنفيذها بواسطة كيانات خاصة، يجب على الدولة تنظيم هذه المعالجة لضمان حماية حقوق الأفراد وفقًا للالتزامات أو المعايير الدولية الملزمة للدولة، ولذلك يفرض قانون حماية البيانات في الاتحاد الأوروبي على كل من السلطات العامة والكيانات الخاصة التزامات مماثلة فيما يتعلق بمعالجة البيانات الشخصية، فعلى سبيل المثال، في يناير 2015، اعتبرت هيئة مفوض المعلومات في المملكة المتحدة"ICO " أن تحديث سياسة الخصوصية لشركة "غوغلGoogle" في مارس 2012 كان "غامضًا جدًا عند وصف كيفية استخدام البيانات الشخصية التي يتم جمعها من خدماتها ومنتجاتها على الويب"، ومنذ ذلك الحين، وافقت "غوغلGoogle" على تعديل سياسة الخصوصية الخاصة بها لتسهيل معرفة المستخدمين في المملكة المتحدة بكيفية جمع بياناتهم وما الغرض منها، ومن المرجح أن يتم تقليد هذا الإجراء في أماكن أخرى في جميع أنحاء الاتحاد الأوروبي، بسبب تأثير التكنولوجيا على النظام القانوني الحالي (Liu, 2021, p. 83).

يمس جمع البيانات الوصفية، أو البيانات التي تصف بيانات أخرى، مسائل الحق في الخصوصية والحق في حماية البيانات على حد سواء، من حيث إنفاذ القانون ومنع الجرائم، ويبدو أن المنطق القانوني هنا يكمن في أن جمع كل

البيانات الوصفية المتاحة وتخزينها وتحليلها عند الحاجة لأي منها فيما يتعلق بالتحقيق في جريمة أو منعها، يُعد فعالاً من حيث التكلفة وسهولة التنفيذ،كما يمكن ربط البيانات الوصفية معًا لتحديد المعلومات عن عادات وروتينات واتصالات ومكان تواجد موضوع البيانات وغيرها من المعلومات الشخصية(Ramírez, A, & García-Segura, 2017, p. 23) .

ثالثا: صعوبة إثبات المسؤولية الجنائية للروبوتات في حالة انتهاك قواعد الارتفاق الرقمي

تشير كل من أحدث التقنيات الرقمية والقانون الدولي إلى أن الجدال أمام القاضي الدولي باعتبار أن الروبوت يجب أن يُعتبر ''مذنبًا'' سيكون بلا معنى، ولذلك تتطلب الأنظمة القانونية عناصر نفسية محددة، مثل الوعي أو الإرادة الحرة، كشرط مسبق لتحديد المسؤولية الجنائية، فعلى سبيل المثال وباستقراء قواعد الركن المعنوي للجريمة، لا يُحاسب الأطفال الصغار على سلوكهم نظرًا لنقص النضج العاطفي والفكري لديهم، وبالمثل، لا يُحاسب الأفراد المصابون بأمراض نفسية شديدة على أفعالهم بسبب عدم قدرتهم على فهم ما يقومون به بالكامل (Sellers & Maxeiner, London, p. 47)، وفي مثال معاصر يتعلق"بقضية الروبوت روبي CX30" تشير بعض الأبحاث القانونية الدولية إلى أن الاعتراف بالمسؤولية الجنائية لروبوت روبّي CX30 سيجعل جميع الأسباب التي تقوم عليها مشروعية العقاب في القانون الجنائي الحديث، مثل نظرية الانتقام أو الوقاية الخاصة والعامة، بلا معنى، وقد تساءل بعض الفقه الدولي في هذا الإطار حول ما إذا كان يمكن لروبوت روبّي سداد دينه للمجتمع؟ وهل يمكن للمجتمع الدولي تصحيح الطابع الأخلاقي للآلة المستقلة بحيث تفهم تمامًا سبب عدم وجوب تكرار الفعل الشرير؟ وما الجدوى من معاقبة روبّي لإقناع البشر أو الروبوتات الأخرى بعدم ارتكاب مخالفات مماثلة؟.

يدّعي دعاة أطروحة ''عدم المسؤولية الجديدة'' أنه حتى في هذه الحالات، لن يتم توتير الرؤية القانونية التقليدية، فمن جهة، ينطبق نموذج المسؤولية في حالات المشاركة على الفرد الذي يرسل أو يُفَعِّلُ روبوتًا من أجل ارتكاب جريمة، حتى ولو ''قرر'' الروبوت الانحراف عن تلك الخطة وارتكب نوعًا آخر من الجرائم، وعلى الرغم من عدم القدرة على التنبؤ بسلوك الآلة أو احتمال عطلها، فإن مستخدم هذا الروبوت سيُحاسب على الجريمة الإضافية في معظم الأنظمة القانونية نظرًا للخطة الأصلية للمستخدم، ومن جهة أخرى، عندما لا يكون لدى البشر نية لارتكاب خطأ، لكن الروبوت الذي يستخدمونه يرتكب هذا الخطأ، يحاسب الأفراد على أساس الإهمال أو عدم العناية الواجبة، أي لأن ''طرفًا معقولًا'' فشل في الوقاية من الضرر ''المتوقع''، وفي نهاية المطاف، ومن منظور النظرية القانونية التقليدية، تشبه الحداثة المزعومة في جميع هذه الحالات مسؤولية مالك أو حافظ حيوان الذي يكون معروفا أو مفترض أن يكون خطيرًا على البشر (Liu, 2021, p. 86).

مع ذلك، ومن خلال رسم تشابه بين سياسات المسؤولية الصارمة التقليدية للأضرار الناجمة عن الحيوانات، ومسؤولية البشر عن سلوك الروبوتات، تعترف أطروحة عدم المسؤولية الجديدة بأننا أمام نوع جديد من المسؤولية البشرية عن أفعال الآخرين، وبما أن الروبوتات، مثل الحيوانات، تتصرف، فإن الضرر الناتج عن هذه الروبوتات لا يمكن إدراجه ضمن النظرية التقليدية لقواعد المسؤولية الصارمة للأنشطة الخطرة، مثل المسؤولية عن المنتجات المعيبة أو نقص المعلومات، وعلى الرغم من أن تصميم وإنتاج واستخدام بعض تطبيقات الروبوتات يمكن اعتباره "خطيرًا"، مثل الأسلحة القتالية غير

المأهولة المستقلة أو شبه المستقلة، فإن العديد من التطبيقات الأخرى بالكاد يمكن رؤيتها ضمن هذه الفئة، وبالتالي يمكن التفكير في آلات لم تُصمَّم أو تُستخدم لارتكاب أي جريمة، مثل روبوتات الجراحة" da Vinci "أو المركبات المائية غير المأهولة (UUVs) التي تقوم بإصلاحات على منصات النفط في البحر الكاريبي، وما توحي به هذه الأمثلة هو أننا نتعامل مع مصدر جديد للوكالة الأخلاقية، حيث يمكن للروبوتات اتخاذ أفعال يمكن تصنيفها أخلاقيًا على أنها جيدة أو سيئة متطرفة، تمامًا كما يحدث مع الحيوانات والأطفال، وبالطبع البالغين (Bolton-King, 2022, p. 154).

بعد الأشكال التقليدية للمسؤولية بدون خطأ عن سلوك الحيوانات والأطفال والموظفين، يُجبر دعاة أطروحة عدم المسؤولية الجديدة على الاعتراف بأن الأنظمة القانونية ستُحاسب البشر على ما "يختار" الروبوت المستقل القيام به، وأن التشبيهات مع أنواع أخرى من المسؤولية الصارمة لا تكفي لمعالجة حداثة تكنولوجيا الروبوتات، ولذلك ينبغي كذلك النظر في الطرق التي توفر بها الأنظمة القانونية حدودًا لمثل هذه القواعد الصارمة للمسؤولية، فلم تعد الروبوتات المزودة بالذكاء الاصطناعي الخارق مجرد حلم أو خيال علمي، بل أصبحت حقيقة علمية تحظى بتطبيقات عدة تحاكي الذكاء البشري (وليد، 2024، صفحة 331).

على العموم، من غير المحتمل أن نجد استعارة أو تشبيهًا واحدًا يمكنه استيعاب القضايا المتعلقة بالجيل القادم من الروبوتات في مجالات القانون الجنائي الدولي والعقود، ومن المحتمل جدًا أن تختلف المسؤولية وفقًا لأنواع التطبيقات المختلفة التي يتم التعامل معها، ومع ذلك، يمكن الجدال ضد أطروحة "عدم المسؤولية الجديدة"، والطرح بأن الروبوتات ستحتاج إلى إطار معياري خاص بها، يفتح الطريق أمام أنواع جديدة من المسؤولية القانونية الضعيفة والقوية عن سلوك الروبوتات المفتوح، وقد ذهب الاتجاه الحديث إلى القول بأن الهدف الأساسي من إيقاع الجزاء على مستخدم أو مبرمج الروبوت كفيل بتحقيق نظام العدالة الجنائية (مصطفى، 2025، صفحة 331).

تعتبر أطروحة عدم المسؤولية الجديدة من بين القواعد القانونية الحديثة المتعلقة بمسؤولية البشر عن سلوك الروبوتات، ويظهر ذلك من خلال النصوص القانونية التقليدية التي قد تصلح لمواجهة بعض المظاهر الإجرامية للروبوت كأحد تطبيقات الذكاء الاصطناعي، ويكون ذلك عن طريق مساءلة المبرمج والمستخدم، ولكن هذه المساءلة قد تقف عاجزة عندما تقع الجريمة من طرف الروبوت ذاته في ظل نظرية التعليم الذاتي العميق (بطور، 2023، صفحة 226).

بالاقتران مع مفاهيم قانونية مثل السببية، والتوقع المعقول، وتقسيم المسؤولية، يُعتبر مبدأ المسؤولية معيارًا عامًا ومرموقًا وعمليًا، يحدد القيود العملية لتصميم وبناء واستخدام الروبوتات، ويحدد من سيكون مسؤولًا عن السلوك المستقل لكل آلة في جميع المجالات القانونية، وعلى الرغم من وجود هذا الإطار المشترك، تبقى هناك فروق جوهرية مطروحة ، ففي القانون الجنائي الدولي، تنطوي المسؤولية في الغالب على اللوم، بحيث أنه بمجرد أن تُدين المحاكم المتهمين تثبت المسؤولية الجنائية، وعلى النقيض، في القانون المدني، لا تتضمن المسؤولية دائمًا اللوم، بل تمثل واجبًا للتعويض على أساس قواعد المسؤولية المطلقة الموضّحة أعلاه (Bolton-King, 2022, p. 97).

علاوة على ذلك، عند التعامل مع أنواع جديدة من المسؤولية عن سلوك الروبوتات، وفي هذا الإطار يركز المحامون الجنائيون غالبًا على الضرر أو الأضرار التي تسببها هذه الآلات، وعلى العكس من ذلك ، لا يلزم في القانون المدني أن

يحدث خطأ ما، إذ أن اهتمام القانون المدني يمتد أيضًا إلى كيفية استفادة البشر من الروبوتات في إبرام العقود أو تأسيس الحقوق والالتزامات بينهم، في سيناريوهات "رابح-رابح"، ويمكن بذلك تتبع النقاش الحالي المطروح حول الأوتوماتا الإدراكية على شكل وكلاء برمجيين في إطار الملاحظة التأسيسية، وبالتالي فان عدم سن تشريع دولي منظم أو إجراء تعديلات للقواعد القانونية ذات الصلة بالمسؤولية الجنائية الدولية حتى تواكب تكنولوجيا الروبوتات، يعني وجود فراغ تشريعي دولي إزاء قواعد المسؤولية الجنائية وما تسببه أضرار الروبوتات (نادر، 2024، صفحة 18).

تستند مثل هذه الفروقات الجوهرية بين القانون الجنائي الدولي والقانون المدني إلى سمة مشتركة في مجال القانون وتقسيم قواعد المسؤولية، التي لا تشمل بالضرورة الاستخدامات الجنائية للروبوتات، بل الشروط والبنود التي تعتمد على اتفاق طواعي بين الأفراد، والذي ستنفذه المحكمة (Sellers & Maxeiner, London, p. 49)، ففي بعض الأحيان، سيكون لإزالة الروبوتات قانونيًا أو إبادتها من الفضاء السيبراني أسوأ حتى من قاعدة "الثلاثة تحذيرات" المعمول بها حاليًا في مجال الجرائم الحاسوبية، وفي الحالة الأخيرة، وكجزء من نظام تدريجي ينتهي بفصل المستخدم عن الإنترنت بعد ثلاثة تحذيرات لانتهاك حقوق الارتفاق، مما يُبعد البشر مؤقتًا عن الإنترنت، أما في حالة الروبوتات، فيمكننا إعادة صياغة ما كتبه الفقيه" دوستويفسكي" في فلسفة الجريمة والعقاب، حيث رأى" أنه إذا كان البشر يملك ضميرًا، فسوف يعاني من خطأ الروبوت، وسيكون ذلك عقابًا بالإضافة إلى السجن" (Sellers & Maxeiner, London, p. 50).

وبالتالي، فإن الشخصية القانونية المستقلة للروبوتات وغيرها من الوكلاء الاصطناعيين لا تقتصر ببساطة على الشخصية القانونية التابعة لأشخاص اصطناعيين آخرين مثل الحكومات أو المنظمات أو الشركات، التي تُختزل مسؤوليتهم في النهاية إلى تجمع من البشر كمصدر وحيد ذي صلة لأفعالهم من أجل معالجة الثورات الروبوتية، والتمردات، والمصادرات، والمقاومة، والسرقات، وما إلى ذلك، ولكن، إذا قبلنا أن مسؤولية الوكيل، أي النية الإجرامية (mens rea)، ستكون متأصلة في عقلية صناعية للآلة وقادرة على قدر من التعاطف أو نوع من الاستقلالية التي تمكّنها من اتخاذ أفعال مقصودة، ومن المرجح جدًا أن يتغير معنى المفاهيم القانونية التقليدية مثل السرقة، والتمرد، أو القتل، في الواقع، إلى ما قد يكون عليه معنى هذه المفاهيم القانونية الذي لا يزال معتمدًا على خيال كتاب الخيال العلمي، وليس على التحليل القانوني العلمي من قبل الخبراء القانونيين، وفي هذا الإطار ابتكر البرلمان الأوروبي على ضوء القانون المدني للروبوتات في 2017 نظرية جديدة تتعلق بالنائب الإنسان المسؤول عن تعويض من يصابون بالأضرار بسبب تشغيل الروبوتات، مستندين في ذلك على خطأ يجب إثباته على النائب، الذي يمكن أن يكون صانع الروبوت أو مالكه أو مشغله أو الذي يستخدمه (نادر، 2024، صفحة 91).

سيطرح السؤال مستقبلا حول مدى كون المحامي الآلي مؤيدًا لتقليد القانون الطبيعي عند استعمال الارتفاقات الرقمية، بحيث تُنظر القواعد على أنها التزامات موضوعية يُعد انتهاكها خرقًا لطبيعة الوكيل الاصطناعي؟، أم سيكون الروبوت، بالعكس، نوعًا من الواقعية القانونية، بحيث تعتمد القواعد في تصميمه على كيفية تأثير هذه الآلات حول فهم البشر للعالم، ومعرفتهم وبيئتهم؟، وماذا عن المواقف المؤسسية للمحامين الآليين الذين، على عكس زملائهم المهتمين باتباع درس "كلسن Kelsen "في العقيدة الخالصة للقانون، والذين يركزون على الآليات الجوهرية للنظام الروبوتي

الجديد؟...، في نهاية المطاف، لا أحد يعرف إلى أين يمكن أن تصل هذه السيناريوهات، من خلال رسم خط فاصل بين قوة الخيال العلمي وحدود التحليل القانوني العلمي، ومن المحتمل أن تكون الشخصية القانونية المستقلة للروبوتات خارج جدول الأعمال في المستقبل المنظور، ونظرًا لأن هذه الآلات تفتقر إلى مكونات نفسية محددة، مثل الوعي الذاتي والنوايا الشبيهة بالبشر، فإن الروبوتات تعتبر مرشحة جيدة لأنواع جديدة من المساءلة في مجال العدالة الدولية الجنائية، بدلاً من الشخصية القانونية الكاملة التي تتحمل كل من المسؤولية المدنية والجنائية للوكيل الأخلاقي، وفي هذا الإطار اختلفت وجهات النظر لدى القانونيين في تحديد أهلية الروبوتات، ما بين مثبت لها بشكل كامل، وما بين مقرر لبعضها (الأحمد، 2025، صفحة 358).

الخاتمة:

إن المفهوم التقليدي لحقوق الارتفاق لم يعد ينسجم مع تطورات الحياة والثورة المعلوماتية المعاصرة، باعتبار أن صور حقوق الارتفاق لم ترد على سبيل الحصر في التشريعات الدولية عموما، وبالتالي يمكن التوّسع في مفهومها بما يتناسب مع تطورات الحياة والاستخدامات البشرية، خاصة إذا ما لاحظنا أن هناك صور مستحدثة تمتد إلى الأشياء غير العقارية كحقوق الارتفاقات الرقمية والذكاء الاصطناعي والبرامج والتطبيقات وغيرها...

تشير الأبحاث ضمن فلسفة التكنولوجيا وسوسيولوجيا القانون إلى أن الهدف من القانون الدولي للارتفاقات الرقمية هو تنظيم عملية الولوّج الدولي إلى منصات البحث وتداول البيانات الرقمية، وبذلك تتم الموازنة بين ممارسة حقوق الإنسان في البيئة الرقمية والخضوع لمقتضيات اتفاقية بودابست، على أساس الامتثال للمعايير القانونية الدولية، وتحديد الاختصاص القضائي الدولي المناسب لمعاقبة مرتكبي الجرائم السيبرانية.

تختلف التشريعات الدولية بشكل كبير فيما يتعلق بالعناصر الأساسية لنظام الحماية الجنائية لقواعد الارتفاقات الرقمية، ولذلك تعتمد كل دولة على حق الفرد في الخصوصية، إلا أن معنى الخصوصية وأصول هذا الحق يمكن أن تختلف من بلد إلى آخر، ونتيجة لذلك، تختلف السياسات والقوانين المنظمة للحق في الخصوصية وحدود حمايتها الجنائية، ومع ازدياد استخدام التكنولوجيا في مجال العلاقات العامة، سيظل الحق في الخصوصية عبر المنصات الرقمية مسألة مهمة لدى كل من الفقه والقضاء الدوليين، وفي هذا الإطار يتحتم على المشرع الدولي سن اتفاقية جنائية عالمية موّحدة لمواجهة مختلف الجرائم السيبرانية المرتكبة عبر الارتفاقات الرقمية.

ونظرًا لتفاعل المؤسسات الجنائية الدولية أكثر مع المستخدمين أصحاب المصلحة عبر الإنترنت ومنصات التواصل الاجتماعي، أصبح من الضروري على صناع القرار في إطار قواعد العدالة الدولية الجنائية أن يأخذوا بعين الاعتبار الجوانب القانونية لتفسير الجريمة السيبرانية وطرائق التحقيق فيها، بالإضافة إلى تقنين قواعد الارتفاقات الرقمية وكيفية تفسيرها في البيئة السيبرانية، فقد أدى غياب المعايير القانونية الكافية للخصوصية الرقمية إلى تبلور عدة تشريعات دولية غير قادرة على مواكبة ومكافحة الكم الهائل من الجرائم السيبرانية المعاصرة.

قائمة المراجع والمصادر

أولا: المراجع باللغة الأجنبية

Alaydrus, L. V. (2012). Pemanfaatan Spektrum Digital Dividend Dengan Pendekatan Model Easement. InComTech , 3 (2).
Alhajj, R., & Glässer, U. (2013). Mining Social Networks and Security Informatics. London: Springer.
Bolton-King, R. M. (2022). Privacy, Security And Forensics in The Internet of Things (IoT). Switzerland: Springer .
Callanan, T. T. (2015). Self- and Co-regulation in Cybercrime, Cybersecurity and National Security. New York : Springer.
Chen, T. M., Jarvis, L., & Macdonald, S. (2014). Cyberterrorism Understanding, Assessment, and Response. London: Springer .
Floridi, M. T. (2017). The Responsibilities of Online Service Providers. Switzerland: Springer International Publishing.
Giovanella, R. C. (2015). Balancing Copyright Law in the Digital Age Comparative Perspectives. New York: Springer .
Heintze, H.-J., & Thielborger, P. (2016). From Cold War to Cyber War The Evolution of the International Law. Switzerland: Springer International Publishing.
Hert, S. G. (2015). Reforming European Data Protection Law. New York: Springer .
Iorliam, A. (2019). Cybersecurity in Nigeria. Nigeria: Springer.
Iqbal, F., Debbabi, M., & Fung, B. C. (2020). Machine Learning for Authorship Attribution. Switzerland: Springer Nature.
Kittichaisaree, K. (2017). Public International Law of Cyberspace. Switzerland : Springer International Publishing .
Leslie, D. A. (2014). Legal Principles for Combatting Cyberlaundering. Switzerland: Springer International Publishing .
Liu, S. (2021). Rights Limitation in Digital Age Reform of Fair Use in Copyright Law. Singapore: Intellectual Property Publishing House.
Mackenrodt, M. B.-O. (2018). Personal Data in Competition,Consumer Protection and Intellectual Property Law Towards a Holistic Approach. Germany: Springer Nature.
O'Reilly, W. (2025). Easements as an Option for API Access. The Student Journal of Information Privacy Law , 3 (1).
Ramírez, M., A, L., & García-Segura. (2017). Cyberspace Risks and Benefits for Society, Security and Development. Switzerland: Springer International Publishing.
Ruggeri, L. B. (2022). Investigating and Preventing Crime in the Digital Era New Safeguards, New Rights. Switzerland: Springer .
Rybski, M. Z. (2021). European Constitutional Courts towards Data Retention Laws. Switzerland: Springer Nature .
Sarlet, M. A. (2022). Personality and Data Protection Rights on the Internet Brazilian and German Approaches. Switzerland: Springer Nature.

Sellers, M., & Maxeiner, J. (London). Human Law and Computer Law:Comparative Perspectives. 2013: Springer.

Taddeo, M., & Floridi, L. (2017). The Responsibilities of Online Service Providers. Switzerland: Springer International Publishing .

Viano, E. C. (2017). Cybercrime, Organized Crime,and Societal Responses International Approaches. Switzerland : Springer International Publishing .

Ziccardi, G. (2013). Resistance, Liberation Technology and Human Rights in the Digital Age. Netherlands: Springer.

ثانيا: المراجع باللغة العربية

ابراهيم ,ل .ن .(2026) .آثر الذكاء الاصطناعي على الحقوق المدنية والسياسية الحق في الخصوصية وحرية التعبير أنموذجا .*مجلة دراسات اقليمية* .(67)

الطباخ ,ش .(2014) .*الموسوعة الشاملة في الدفوع المدنية* .القاهرة :دار العدالة للنشر والتوزيع .

الأحمد ,م .ع .(2025) .المسؤولية الجنائية المترتبة على تقنيات الذكاء الاصناعي الروبوتات نموذجا دراسة فقهية مقارنة بقانون الجزء الكويتي .*مجلة الشريعة والدراسات الاسلامية* .(143) *40* ,

الجيلالي ,ع .(2009) .*المدخل للعلوم القانونية نظرية الحق* .الجزائر :برتي للنشر.

العطوي ,ف .م .(2013) .*الاشكالات التي يثيرها التعاون الدولي في المواد الجنائية* .القاهرة :دار النهضة العربية.

العمل عن بعد كأسلوب حديث لتنظيم العمل–المفهوم والخصوصية–*الدراسات القانونية المقارنة* 1863–1831

باسم ,غ .ع .(2025) .التنظيم الدولي لحماية الحق في الخصوصية الرقمية .*مجلة الفارابي للعلوم الانسانية* .(6) *8* ,

بحص ,ص .ح .(2025) .المسؤولية الجنائية الدولية عن استخدام الذكاء الاصطناعي في النزاع المسلح .*مجلة جامعة البيان للدراسات والبحوث القانونية* , *4*(3).

بطور ,ا .ا .(2023) .مدى مسؤولية الروبوت الطبي جنائيا كأحد تطبيقات الذكاء الاصطناعي دراسة تحليلية تأصيلية .*المجلة القانونية* .(1) *16* ,

بلحيمر ,ع .(2017) .تمييز ارتفاق المرور عن حق المرور .*مذكرة ماجستير* .الجزائر :كلية الحقوق جامعة الجزائر.

تحسين ,ب .ع .(2025) .حقوق الانسان والحريات العامة في عصر الذكاء الاصطناعي دراسة نقدية بين التشريع العراقي والمواثيق الدولية .*مجلة آداب الفراهيدي* .(9) *8* ,

جعفر ,ع .م .(2025) .دور القضاء الاداري في حماية الحقوق الرقمية للافراد دراسة تجاوزات السلطة الادارية في عصر التكنولوجيا في ضوء أحكام القضاء الاداري العراقي .*مجلة العلوم القانونية والسياسية* .(1) *14* ,

حسين ,أ .س .(2011) .*الاحتيال الالكتروني الأسباب والحلول* .(Vol. 1)عمان :دار الجنادرية للنشر والتوزيع

حيدري ,س .ص .(2025) .الاطار القانونية لحماية الأمن السيبراني في العراق دراسة تحليلية في ضوء التشريعات الوطنية والمعايير الدولية .*مجلة دراسات البصرة* .(62)

خنفوسي ,ع .ا .(2019) .*مدخل الى قانون الملكية الفكرية* .عمان الاردن :مركز الكتاب الاكاديمي.

ريكان ,ص .ج .(2025) .مبدأ اسناد المسؤولية الدولية عن أعمال العدوان التي تتم من خلال الهجمات السيبرانية في اطار القانون الدولي .*مجلة القادسية للقانون والعلوم السياسية* .(2) *16* ,

زهراء ,ه .م .(2025) .تحديات حماية الخصوصية في الفضاء السيبراني دراسة في القانون العراقي .*مجلة المستقبل للدراسات القانونية* .(1) *1* ,

سبتي ,ع .ا .(2021) .الارتفاقات الادارية في مجال البريد والاتصالات الالكترونية وفقا للقانون الجزائري .*حوليات جامعة الجزائر* .(3) *35* ,

سعاد ,ر .ح .(2026) .الحماية الجنائية للحق في الخصوصية الرقمية في التشريع العراقي والقانون المصري والاماراتي دراسة مقارنة .*مجلة القانون للدراسات والبحوث القانونية* .(32) *19* ,

سعد ,ع .ن .(2025) .القصور التشريعي في مواجهة جرائم الذكاء الاصطناعي دراسة مقارنة .*مجلة دراسات البصرة* .(64)

سكينة ,ع .ك .(2026) .الضمانات الدستورية والقانونية للحقوق الرقمية للمواطن .*مجلة جامعة تكريت* .(3) *10* ,

عمر ,ح .ب .(2025) .*القضاء العقاري في ضوء أحدث القرارات الصادرة عن المحكمة العليا ومجلس الدولة ومحكمة التنازع* .الجزائر :دار بلقيس.

عمرو شكري القبطان. (2025). *جرائم أمن الفضاء السيبراني دراسة في اسباب براءة مقدمي الخدمات من المساهمة في ارتكابها*. القاهرة: الدار المصرية اللبنانية

عواد ,ع .ا .(2025) .سياسات مكافحة الارهاب السيبراني نماذج مختارة .*مجلة الفكر القيادي للبحوث والدراسات* .(6)*2* ,

كاسيزي ,ا .(2015) .*القانون الجنائي الدولي* .لبنان :مكتبة صادر ناشرون.

كحلون ,ع .(2015) .*التعليق على مجلة الحقوق العينية وقانون التحيين* .(Vol. 3)تونس :مجمع الاطرش للكتاب المختص.

كوثر ,ف .ج .(2026) .الحماية القانونية للهوية الرقمية دراسة تحليلية مقارنة .*مجلة مركز بابل للدراسات الانسانية* .(1)*16* ,

لوجين نزار ذنون ,و .ن.(.s.d) .

مُحَمَّد ,خ .س .(2025) .تحديات استخدام الذكاء الاصطناعي وفق قواعد القانون الدولي الانساني التقليدي.(92)*22* .

مُحَمَّد ,ح .ه .(2020) .*المواطنة العالمية البيئة الرقمية* .القاهرة :الدار المصرية اللبنانية.

مصطفى ,ج .ج .(2025) .المسؤولية الجنائية الناتجة عن استخدام الروبوتات الانسالة .*مجلة جامعة البيان* .(1)*4* ,

مطير ,ذ .ا &.,علي مطشر ,ع .ا .(2023) .الارتفاقات الالكترونية .*مجلة كلية الامام الكاظم* .(4)*7* ,

نادر ,ق .ر .(2024) .*القانون والذكاء الاصطناعي المسؤولية المدنية عن اضرار الروبوتات ذات الذكاء الاصناعي دراسة مقارنة* .عمان الاردن :دار المعتز للنشر والتوزيع.

نور ,م .م .(2025) .الحماية الدولية للخصوصية الرقمية في اطار الذكاء الاصطناعي .*مجلة الفارابي للعلوم الانسانية* .(3)*8* ,

وليد ,ا .م .(2024) .اشكالية تطبيق أحكام المسؤولية الجنائية عن أفعال الروبوتات المزودة بالذكاء الاصطناعي .*مجلة طبنة للدراسات العلمية والاكاديمية* , *7*(1).

يوسف ,ي .ع .(2025) .أثر التهديدات الرقمية على حقوق الإنسان .*المجلة العراقية للبحوث الانسانية والاجتماعية والعلمية* .(19)