# إشكالية إثبات الضرر السيبراني في ظل التحول الرقمي: دراسة قانونية وتحليلية

# The challenge of proving cyber damage in the context of digital transformation: a legal and analytical study



د/ دعاس كمال[1*]

[1] جامعة امحمد بوقرة بومرداس، الجزائر

k.daas@univ-boumerdes.dz

تاريخ الارسال: 2026/01/20 تاريخ القبول: 2026/06/03 تاريخ النشر: 2026/06/10

**ملخص:**

يعتبر إثبات الضرر السيبراني من أكثر الإشكالات القانونية تعقيدًا في ظل تطور الهجمات الإلكترونية وتنوعها، بحيث تواجه الضحية صعوبة في تحديد الجهة الفاعلة نظرًا لسهولة إخفاء الهوية في الفضاء الرقمي، وهو ما يثير مشكلة الإثبات أمام القضاء، خاصة في غياب إطار قانوني منظم وموحد للهجمات السيبرانية، بالتالي يعد تطوير القواعد القانونية والإجرائية ضرورة ملحة لمواكبة التحديات التي يفرضها الفضاء السيبراني.

**الكلمات المفتاحية:** *الضرر السيبراني؛ الرقمنة؛ الذكاء الاصطناعي؛ الهجمات السيبرانية؛ الإثبات الرقمي.*

**تصنيف جال:** *k00*

***Abstract***

*Proving cyber damage is one of the most complex legal challenges in light of the evolution and diversity of cyberattacks. Victims face difficulty identifying the perpetrator due to the ease with which identity can be concealed in the digital space. This raises the challenge of proving damage before the courts, especially in the absence of a unified legal framework for cyberattacks. Therefore, developing legal and procedural rules is an urgent necessity to keep pace with the challenges posed by cyberspace.*

***key words:*** *cyber damage; digitization ; artificial intelligence; cyberattacks; digital evidence.*

***JEL classification:*** *k00*

* د. دعاس كمال

**مقدّمة:**

مع تزايد الاعتماد على تقنيات الذكاء الاصطناعي في مختلف المجالات برزت إشكالات قانونية عميقة تتعلق بكيفية التعامل مع الأضرار التي تنشأ في الفضاء السيبراني نتيجة تدخل هذه التقنيات أو استعمالها، إذ أصبحت الأنظمة الذكية لا تقتصر على تنفيذ التعليمات البشرية بل تطورت إلى حد اتخاذ قرارات مسؤولة، خاصة ما يتعلق بإثبات الضرر وتحديد العلاقة السببية بين التصرف الآلي والنتيجة الضارة، وهذا ما يجعل من مهمة الإثبات تحديا حقيقيا، يتطلب أدوات قانونية وتقنية تتجاوز القوالب التقليدية المألوفة.

كما أن إثبات الضرر السيبراني يصطدم بجملة من الإشكالات من أبزها: صعوبة تتبع الأثر الرقمي، غياب السجلات الكافية أو الشفافة للعمليات التي تؤدي إلى الضرر، واحتمالية تدخل خوارزميات غير قابلة للفهم الكامل حتى من قبل مطوريها أنفسهم، ويزداد الأمر تعقيدا في ظل غياب تشريعات واضحة ومتكاملة تنظم آليات عبء الإثبات، وبالتالي يتطلب حلولا مبتكرة لضمان العدالة وحماية الحقوق في عصر رقمي متسارع.

**أسباب ودوافع اختيار الموضوع:** يكمن الدافع الأساسي في اختيار الموضوع في التوسع المتزايد في استخدام التكنولوجيا الرقمية التي أدت إلى ظهور أنماط جديدة من الأضرار والانتهاكات التي يصعب إثباتها بالوسائل التقليدية، بالإضافة إلى قلة الدراسات القانونية المتخصصة التي تعالج هذا الموضوع مقارنة بحجم المخاطر التي يفرزها.

انطلاقا مما تقدم سيتم التوسع في الموضوع، ومحاولة الإلمام بمختلف الأحكام والجوانب المتعلقة به، وذلك من خلال طرح الإشكالية التالية:

**إلى أي مدى يؤثر التطور الرقمي على إثبات الضرر الالكتروني في ظل الهجمات السيبرانية المعاصرة؟**

**المنهج المعتمد:** للإجابة على الإشكالية المطروحة أعلاه اعتمدنا المنهج الوصفي والتحليلي لبحث المعوقات القانونية المتصلة بإثبات الأضرار السيبرانية الناجمة عن التطور السريع للأجهزة الذكية.

**الفرضية المعتمدة:** أن الضرر السيبراني لا يمكن التصدي له في ظل القواعد القانونية التقليدية مما يفرض تطوير آليات قانونية خاصة تتلائم وطبيعة هذا الضرر.

**أهداف المقال:** إن الهدف من دراسة هذه الإشكالية هو إبراز الصعوبات القانونية التي تعترض إثبات الضرر السيبراني في ظل القواعد التقليدية للإثبات مع تحليل مدى ملائمة القواعد القانونية الحالية لمواجهة هذا النوع المستحدث من الأضرار والكشف عن أوجه القصور التشريعي والعملي في هذا المجال.

ولمعالجة هذا الموضوع قسمنا الدراسة إلى مبحثين، حيث جاء المبحث الاول بعنوان التحديات القانونية لإثبات الضرر السيبراني الناتج عن التطور الرقمي، أما المبحث الثاني فجاء تحت عنوان وسائل الحماية القانونية للضرر السيبراني في ظل التطور الرقمي للأجهزة الذكية.

## 1. التحديات القانونية لإثبات الضرر السيبراني الناتج عن التطور الرقمي

يعتبر إثبات الضرر من الدعائم الأساسية للمسؤولية القانونية في فرعي القانون المدني والجنائي، غير أن التطور السريع في تقنيات المعلومات لا سيما في مجال البرمجيات قد أوجد تحديات جديدة أمام الفقه والقضاء أبرزها تعقيد عملية إثبات الضرر الناجم عن الأنشطة السيبرانية في البيئة الرقمية.

وبغية الإلمام بكافة الجوانب المرتبطة بصعوبة إثبات الضرر سنقوم بدراسة الإطار المفاهيمي للضرر السيبراني ، ثم سنتعرض بعد ذلك إلى تبيان صعوبة إثبات الضرر في ظل الهجومات السيبرانية.

### 2.1 الإطار المفاهيمي للضرر السيبراني:

شهد العالم في العقود الأخيرة تطورا تكنولوجيا هائلا أدى إلى تحول جذري في أنماط الحياة الاجتماعية والاقتصادية (الحميد، صفحة 2204)، والتي أصبحت اليوم تشكل صعوبات قانونية وأمنية متزايدة ينتج عنها أضرارا خطيرة عند سوء استعماله، فيمثل الأذى السيبراني تهديدا رقميا غير تقليدي يضر الأفراد والمنظمات (المنعم، التحديات القانونية أمام إثبات الضرر السيبراني في ظل تطور تقنيات الذكاء الاصطناعي، د.س.ن ، صفحة 3117).

يعتبر الضرر من الناحية اللغوية الضر ضد النفع، وهو إلحاق المفسدة بالغير، وهي كلمة شاملة لكل أوجه الأذى والإساءة للإنسان في نفسه أو عرضه أو شرفه أو اعتباره أو ماله أو عقله (عمر، 2020، صفحة 05).

أما من الناحية القانونية حسب المادة 124 من القانون المدني الجزائري فهو:"كل فعل أيا كان يرتكبه الشخص بخطئه ويسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض" (75-58، مؤرخ في 26 سبتمبر1975، الصادر في 30 سبتمبر 1975)، ومنه نستطيع أن نقول أن الضرر هو كل فعل يرتكبه الشخص عن طريق الخطأ، ويكون سببا لحدوث التعويض.

اصطلاحا الضرر هي كلمة مشتقة من استعمالاتها اللغوية، فيعرف بأنه الاخلال بمصلحة مشروعة للنفس أو للغير، تعديا أو تعسفا أو إهمال (أحمد م.، 1997، صفحة 97).

في حين أن كلمة السيبراني لغة هو مصطلح حديث مشتق من لفظ "Cyber" بالانجليزية، ولقد عرف قاموس أكسفورد كلمة "سيبراني" بأنها صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي (الله، 2020، صفحة 07).

اصطلاحا الكلمة " Cyber" مأخوذة من "Cyberneties" وهي كلمة تعود إلى اللغة اليونانية، وتعني" الحاكم" أو "الموجه" ولقد استخدمت لوصف علم التحكم في الأنظمة المعقدة، ثم تطورت لتستعمل في العصر الرقمي للإشارة إلى كل ما هو إلكتروني أو رقمي ومتصل بالحوسبة والاتصالات (المنعم، المرجع السابق، صفحة 3117).

وقد عرفه الاتحاد الدولي للاتصالات بأنه:" المجال المادي وغير المادي الذي يتكون وينتج من عناصر وهي: أجهزة الكمبيوتر، الشبكات، البرمجيات، الحوسبة، المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمو كل هذه العناصر (ITU, 2010, p. 12)."

كما عرفت الوكالة الفرنسية الفضاء السيبراني بأنه "فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية "، فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية مكونة من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين (OLIVIER, 2012, p. 19).

بعد التعرف على أهم المصطلحات المشكلة للضرر السيبراني وأبعاده العامة، يصبح من الضروري الانتقال إلى توضيح أنواعه لأن تنوع الهجمات والتهديدات في الفضاء السيبراني أدى إلى تعدد أشكال الضرر التي قد تطال المؤسسات والأفراد على حد سواء من بين هذه الأنواع نذكر مايلي:

- الضرر المالي:

هو ما يصيب الذمة المالية فيسبب لصاحبها خسارة مالية (سليمان، 1922، الصفحات 136-137)، سواء بصفة مباشرة أو غير مباشرة نتيجة للهجمات الالكترونية، مثل سرقة الأموال من الحسابات البنكية، أو الاحتيال باستخدام بطاقات الائتمان إضافة إلى تعطيل الأنظمة عن العمل وما يترتب عليه من خسائر تشغيلية كبيرة (المنعم، المرجع السابق، صفحة 3119).

- الضرر المعنوي(النفسي/الاجتماعي):

هو الضرر الناشئ عن الأضرار النفسية أو الاجتماعية التي لحقت بالمضرور، حيث يصاب الإنسان في شعوره أو عاطفته أو كرامته أو شرفه (القادر ا.، 2006، صفحة 180)، جراء لتسريب معلومات خاصة أو التشهير بهم مثل تسريب الصور أو المحادثات الشخصية، أو تشويه السمعة على وسائل التواصل الاجتماعي أو نشر معلومات حساسة دون إذن مسبق (أنور، 2007، صفحة 139).

- الضرر التقني(التشغيلي):

يظهر الضرر التقني في صورة تعطل أو تلف يصيب الأنظمة التقنية كأنظمة التشغيل أو قواعد البيانات أو الشبكات، مما يؤدي إلى إعاقة عمل المؤسسات أو الأفراد، وذلك من خلال هجمات مثل ادخال فيروسات تؤدي إلى فقدان البيانات (المنعم، المرجع السابق، صفحة 3120).

- الضرر القانوني:

هو الأذى أو المساس بحق أو مصلحة مشروعة تواجه الأفراد أو المؤسسات نتيجة لفشلهم في حماية البيانات، كأن تتعرض الشركات للغرامات بسبب تسريب بيانات المستخدمين .

- الضرر الأمني:

يعد الضرر الأمني من أخطر الأضرار، حيث يستهدف أمن الدولة أو مؤسساتها الحيوية من خلال هجمات الكترونية تخترق الأنظمة الحكومية أو العسكرية، أو تسرب وثائق سرية بهدف زعزعة الاستقرار الوطني(security) .

- الضرر الأخلاقي:

ينتج عن السلوكيات غير المشروعة التي تمارس عبر الانترنت، مثل الابتزاز الالكتروني، نشر المحتويات الضارة أو ممارسة التنمر الالكتروني، وهو ما يؤدي إلى تفشي ظواهر اجتماعية خطيرة وانحرافات سلوكية. (أيوب و البغدادي، 2022، صفحة 07)

**2.1 إشكالية إثبات الضرر في ظل الهجمات السيبرانية:**

أدى التطور السريع في تكنولوجيا المعلومات إلى ظهور حروب بنمط جديد، حيث أصبحت جزء جوهريا يعتمد عليها الأفراد والمؤسسات والدول إلا أن استعمال الذكاء الاصطناعي في المجال السيبراني أفرز نوعا جديدا من الجرائم المعقدة يطلق عليها "الجرائم السيبرانية المدعومة بالذكاء الاصطناعي.

أشار تقرير لمؤسسة "جارتنر للأبحاث" بأن الذكاء الاصطناعي يمكن أن يستخدم من قبل المتسللين لأغراض خبيثة كاختراق الشبكات، انتحال الهوية هجمات حجب الخدمة وغيرها من الأفعال التي تندرج تحت بند الجرائم السيبرانية (القادر د.، 2025، صفحة 02).

في كثير من الحالات لا يكون هنالك تدخل مباشر من الإنسان عند تنفيذ الجريمة، بل يتم تنفيذها بواسطة برمجيات ذكية تتخذ قراراتها بناء على معطيات وتعلم ذاتي، هذا الطابع "شبه المستقل" يجعل من الصعب قانونا إسناد الجريمة إلى شخص معين لا سيما عند عدم وضوح العلاقة بين فعل الذكاء الاصطناعي ونية الفاعل البشري، مما يعقد الركن المعنوي للجريمة (وسيلة، 2023، صفحة 08).

يظهر جليا أن تعقيد الركن المعنوي للجريمة يؤدي إلى غياب القصد الجنائي لأن هذا الأخير هو انصراف الإرادة نحو تحقيق وضع اجرامي مع العلم بحقيقته الواقعية وبماهية الاجرام (المنعم، المرجع السابق، صفحة 3125)، فالمسؤولية الجنائية في القواعد العامة تعتمد على توافر القصد الجنائي إلى جانب الركن الرمادي (محمود، 2017، صفحة 138)، لكن في حالات الجرائم المدعومة بالذكاء الاصطناعي قد لا يكون هناك قصد إجرامي واضح، لا من جانب المبرمج، ولا من جانب المشغل، إضافة إلى ذلك فإن العلاقة السببية بين الفعل والفاعل تصبح غير واضحة، لأن عبء إثبات هذه العلاقة تقع على عاتق الشخص الذي يدعي وقوع الضرر هذه القاعدة القانونية التي وضعها المشرع لا تتناسب مع طبيعة تقنيات الذكاء الاصطناعي، وبالتالي يصعب إثباتها (جهان و حشماوي، 2021، صفحة 21).

لذلك ومع التطور التكنولوجي المتسارع أصبح من الصعب جمع الأدلة الرقمية نتيجة اعتماد المهاجمون على أساليب متطورة للغاية، بما في ذلك الخوارزميات الذكية التي يمكنها التكيف مع الهجمات أو حتى إخفاء أدلة الهجوم بشكل ديناميكي.

كما يمكن للمهاجمين استعمال تقنيات التشفير المتقدمة التي يصعب من خلالها تحديد هويتهم وتتبع مساراتهم، كما يمكنهم إخفاء هويتهم عبر شبكات افتراضية خاصة.

## 2. الحماية القانونية للضرر السيبراني في ظل التطور الرقمي للأجهزة الذكية.

بفضل الثورة الرقمية المتسارعة صار الذكاء الاصطناعي أحد أبرز التحولات التكنولوجية التي تؤثر بشكل جوهري في جميع جوانب الحياة، وعلى رأسها تلك المتصلة بالضرر السيبراني فهو يطرح إشكالات قانونية معقدة تتعلق بصعوبة تحديد المسؤولية، إلا أن الإطار القانوني الحالي لا يزال يعتمد على مفاهيم المسؤولية التقليدية ولا يواكب الطبيعة الديناميكية للذكاء الاصطناعي، و عليه فإن تطوير هذا الإطار أصبح ضرورة قانونية ملحة سواء من خلال استحداث تشريعات جديدة وهذا ما سنتناوله في المطلب الأول، وتشجيع الابتكار التكنولوجي من ناحية أخرى، وكذا تفعيل أدوات الإثبات الإلكتروني والرقمي في المطلب الثاني.

### 1.2 تعزيز البنية القانونية والتشريعية:

يعد تعزيز البنية التشريعية والقانونية من الركائز الأساسية لتحقيق الحكم الراشد وضمان سيادة القانون فهو يهدف إلى تطوير المنظومة القانونية بما يتماشى مع متطلبات العصر، من خلال تحديث القوانين، وتحسين آليات تطبيقها، وتعزيز الشفافية والمساءلة كما يساهم في خلق بيئة قانونية مستقرة تشجع على الاستثمار وتحمي حقوق الأفراد والمؤسسات مما يدعم التنمية الاقتصادية والاجتماعية بشكل مستدام.

على أساس ذلك أصبح تعديل النصوص القانونية في العصر الرقمي ضرورة ملحة من أجل حماية حقوق الأفراد لذا سنتطرق إلى أهم القوانين التي يجب تعديلها.

- تعديل قانون العقوبات والإجراءات الجزائية:

وذلك بإدخال نص قانوني يجرم استعمال الأنظمة الذكية في: تنفيذ هجمات إلكترونية، توليد محتوى مزيف، تصنيف الجرائم التي تتم باستخدام الذكاء الاصطناعي «كجرائم مشددة العقوبة " نظرا لتعقيد كشفها وخطورتها (مصطفى، 2024، الصفحات 1-3).

تعديل قانون حماية البيانات الخاصة:

وذلك من خلال النص على الحق في التفسير: أي إلزام الجهات التي تستخدم أنظمة الذكاء الاصطناعي باتخاذ قرارات كفيلة لتوضيح كيفية اتخاذ القرار، توسيع مفهوم "البيانات الحساسة" ليشمل البيانات التي يمكن للذكاء الاصطناعي استخلاصها، مثل الحالة النفسية، إلزام الشركات والمطورين بالحصول على موافقة صريحة عند استخدام الذكاء الاصطناعي (المنعم، المرجع السابق ، صفحة 3132).

- تعديل القانون المدني نظام المسؤولية المدنية:

استحداث مادة تنص على المسؤولية عن الأضرار الناتجة عن الأنظمة الذكية حتى بدون وجود خطأ بشري مباشر، بالإضافة إلى اعتماد مبدأ "المسؤولية التضامنية" والمطور والمشغل، والمستخدم النهائي، وفقا لنسبة مساهمته في الضرر (فكري، 2024، الصفحات 451-474).

- تعديل قانون التجارة الإلكترونية:

من خلال ادخال مفهوم "الوكلاء الأذكياء" في نظام العقود الالكترونية، والاعتراف بشرعية العقود التي يبرمها نظام الذكاء الاصطناعي بالنيابة عن شخص طبيعي، مع اشتراط الشفافية في التعامل بالأنظمة الالكترونية عند التعاقد، وابلاغ المستهلك بذلك (المنعم، المرجع السابق، صفحة 3133).

- ادخال تشريعات جديدة غير موجودة :

مثل قانون خاص يعالج الإشكالات الناتجة عن إدخال الأنظمة الذكية في التعاملات يشمل قواعد المسائلة، التسجيل الإلزامي لبعض الأنظمة عالية الخطورة، التزامات مطوري الذكاء الاصطناعي، وآليات الرقابة والتفتيش (صلاح، 2024، صفحة 62).

- تعديل قانون العمل :

النص على حق الموظف في معرفة ما إذا كان يخضع لتقييم إلكتروني، وضع حدود على قرارات الفصل أو الترقية التي تعتمد كليا على أنظمة الذكاء الاصطناعي، وضع برامج إعادة تأهيل وتدريب للموظفين المهددين بالإحلال نتيجة الأخطاء الالكترونية الشائعة (المنعم، المرجع السابق، صفحة 3133).

بالإضافة إلى تعديل النصوص القانونية وجب على المشرع استحداث نظام قانوني خاص بالأجهزة الذكية لأن وجود قانون خاص بالذكاء الاصطناعي أصبح ضرورة ملحة في العصر الحالي، نظراً للتطور السريع لهذه التكنولوجيا وتأثيرها المتزايد على مختلف مناحي الحياة. وهو ما يعكس الضرورة الملحة لسنّ قانون ينظم استخدام وتطوير الذكاء الاصطناعي، من خلال مراعاة هذه النقاط:

- حماية حقوق الإنسان :

من خلال ضمان عدم استخدام الذكاء الاصطناعي في انتهاك الخصوصية، التمييز العنصري أو الجندري، أو التلاعب بالمعلومات، حماية الأفراد من الأضرار الناتجة عن قرارات آلية غير عادلة أو غير شفافة (مثل أنظمة القبول الجامعي أو القروض البنكية المعتمدة على الذكاء الاصطناعي)

- تعزيز الشفافية والمساءلة :

من المهم وجود قوانين تفرض الشفافية في كيفية اتخاذ أنظمة الذكاء الاصطناعي لقراراتها، وتحديد الجهة المسؤولة قانونياً عن الأضرار أو الأخطاء التي قد تنتج عن استخدام الذكاء الاصطناعي (المطور، المستخدم، الشركة؟).

- دعم الابتكار مع تقليل المخاطر:

القانون الجيد لا يجب أن يعيق الابتكار، بل يوجهه نحو الاستخدام الآمن والمسؤول، كما يمكن أن يخلق بيئة موثوقة تُشجّع المستثمرين والمطورين على العمل ضمن إطار قانوني واضح.

- تنظيم استخدام الذكاء الاصطناعي في القطاعات الحساسة:

تتمثل القطاعات الحساسة خاصة في الرعاية الصحية، الأمن، العدالة، التعليم، حيث قد يؤدي سوء استخدامه إلى عواقب وخيمة على الأفراد والمجتمع. مثلاً، لا يجوز الاعتماد على AI في تشخيص طبي بدون إشراف بشري مختص.

### 2.2 تطوير آليات الإثبات الرقمي:

يعد استحداث آليات للإثبات الرقمي من الركائز الأساسية في عصر التحول الرقمي، حيث أصبح من الضروري إيجاد وسائل موثوقة وآمنة لإثبات الهوية، الحقوق، أو صحة البيانات في البيئات الرقمية ومن بين هذه الآليات نذكر :

- إقرار التوقيع الإلكتروني والتوثيق الرقمي كأدلة قضائية:

استند الفقه والقضاء لمنح الإثبات الإلكتروني الحجية القانونية الثبوتية على التفسير والاعتراف به أمام المحاكم إلى التوقيع الالكتروني، فذلك يسمح بتسريع الإجراءات القانونية ويقلل من الحاجة إلى الأوراق التقليدية، كما يمكن الاعتماد على تقنيات التوثيق الرقمي (فاطمة، 2020، صفحة 688).

- استخدام تقنيات البلوك تشين لتوثيق الأدلة الرقمية:

البلوك تشين هي شبكة معلومات تحتوي على مجموعة من الأجهزة التي تسمح بحفظ المعلومات وتوثيق البيانات بطريقة تمنع التعديل أو التلاعب بها بعد تسجيلها، وهو ما يضمن للمحاكم عدم التعرض للتغير أو التزوير، ما يعزز من مصداقية الإجراءات القانونية (عبير و علواني، 2023، الصفحات 9-10).

- استخدام الذكاء الاصطناعي في تحليل الأدلة:

يمكن استخدام تقنية الذكاء الاصطناعي في فحص الأدلة الرقمية بشكل أسرع وأكثر دقة، مثل التعرف على العبث في الصور والفيديوهات، أو التحقق من صحة الوثائق بالإضافة إلى ذلك أنه يساعد في تحديد وجود أي هجوم سيبراني أو تلاعب في المعلومات الرقمية المقدمة للمحكمة. (محمد، 2023، الصفحات 143-166)

- تطوير آليات للتحقق من صحة الأدلة الرقمية:

يجب وضع تقنيات وآليات تمكن المحاكم من التحقق من صحة الأدلة الرقمية مثل التحقق من هويات الأطراف المرسلة والتأكد من أن البيانات الواردة لم يتم التلاعب بها أو تعديلها (المنعم، المرجع السابق، صفحة 3135).

- تدريب القضاة والمحامين على التعامل مع الأدلة الرقمية:

مع استمرار تطور التكنولوجيا، من المتوقع أن تتطور أيضا معايير قبول الدليل الإلكتروني في المحاكم، لذا يجب على الأنظمة القضائية تحديث ومواكبة التطورات الحاصلة في جميع الأدلة، فضلا عن تعزيز تدريب القضاة والمحامين في هذا المجال واشراكهم ضمن دورات تدريبية عالية المستوى (أحمد هـ.، 1989، صفحة 123).

## 3.الخاتمة:

ما جرى تقديمه من تحديات قضائية أمام إثبات الضرر الإلكتروني في ظل تطور تقنيات الذكاء الاصطناعي، يبين أن النظام الحقوقي في العديد من البلدان يواجه عسرا في مواكبة هذا التطور السريع، فوجود ثغرات في التشريعات الحالية يعيق المتضررين من الحصول على تعويض عادل، ويؤدي إلى صعوبة تحديد المسؤولية القضائية بدقة في الحوادث المتعلقة بالأمن السيبراني، لذا وجب على المشرعين والجهات القانونية تطوير تشريعات مرنة وفعالة، تواكب تطور تقنيات الذكاء الاصطناعي وتضمن صون الحقوق القانونية للأفراد والمؤسسات.

إن ضمان حماية الأفراد من الأضرار السيبرانية يتطلب تعاونا دوليا مستمرا، وتحديثا دائما للأنظمة القانونية بما يكفل تحقيق العدالة وحفظ الحقوق في ظل التكنولوجيا الحديثة.

فيما يلي بعض **النتائج** المتعلقة بالموضوع:

- أظهر البحث أن الضرر السيبراني يتميز بطابع خاص تقني يصعب مقارنته مع الضرر التقليدي.
- القواعد القانونية التقليدية للإثبات في إطار المسؤولية المدنية غير كافية لوحدها لمواجهة هذا النوع من الأضرار الالكترونية.
- أظهر البحث عدم وجود تعريف قانوني دقيق وموحد للضرر السيبراني.
- الإثبات الرقمي يصطدم بصعوبات وتحديات عملية تتعلق بسرعة زوال الدليل وإمكانية التلاعب به بمختلف الوسائل الرقمية.
- التحول الرقمي يفرض نفسه على القضاء مما يتطلب خبرة تقنية وقانونية متخصصة.
- الحماية القانونية الحالية للحقوق الرقمية لا تزال جزئية ولا ترقى إلى حجم المخاطر السيبرانية المتزايدة.
- يمكن أن يطرح الطابع العابر للحدود للضرر السيبراني إشكالات عدة تتعلق بالقانون الواجب التطبيق في المنازعات وكذا الاختصاص القضائي.
- غياب أجهزة تتفاعل في تقييم الأضرار السيبرانية يزيد من تعقيد تسويتها قضائيا.
- ضعف الوعي القانوني للأفراد والمؤسسات بخصوص موضوع مخاطر الضرر السيبراني وطرق إثباته.

- صعوبة إثبات العلاقة السببية بين الفعل السيبراني الضار والضرر الناتج عنه خاصة عند تعدد الفاعلين أو استخدام تقنيات إخفاء الهوية.
- التأخر النسبي للتشريعات الوطنية في تنظيم هذا النوع من الأضرار مقارنة بالسرعة الكبيرة للتطور التكنولوجي.

**التوصيات:**

- ضرورة استحداث قوانين وطنية جديدة وشاملة تواكب العصر الرقمي.
- ضرورة عمل نظام قانوني موحد للمسؤولية القانونية الناشئة عن استخدام أنظمة الذكاء الاصطناعي.
- تعزيز التعاون الدولي بين الدول من خلال إبرام العديد من الاتفاقيات الدولية التي من شأنها مكافحة الفساد الإلكتروني.
- إنشاء مؤسسات وطنية رقابية للتحقق من صحة الأدلة الرقمية للإثبات الإلكتروني.
- العمل على استحداث تشريعات متخصصة في الذكاء الاصطناعي.
- تطوير آليات فعالة لجمع الأدلة الرقمية في القضايا المتعلقة بالضرر السيبراني وتلك المتعلقة بالأمن السيبراني عامة.
- ضرورة إقرار تعريف تشريعي واضح للضرر السيبراني.
- تطوير قواعد الإثبات القانونية بما يسمح بالاعتراف الصريح بالأدلة الرقمية واعتماد حجيتها.
- ضمان تكوين خاص للقضاة في المجال التقني والقانوني.
- توعية الأفراد والمؤسسات بمخاطر الفضاء الرقمي وسبل الحماية القانونية المتاحة.
- تشجيع البحث العلمي في مجال الجرائم والأضرار السيبرانية لمواكبة التحول الرقمي.

## 4.قائمة المراجع: (الخط: Sakkal Majalla حجم: 18 حجم سميك).


- ,58-75أمر رقم مؤرخ في 26 سبتمبر1975، الصادر في 30 سبتمبر 1975 .(يتضمن القانون المدني الجزائري .ج.ر.ج.د عدد *78*.
- ITU. (2010). cyber crime legislation. *toolkit for the international télécommunication union* . geneva.
- kkkk. (5555). *uuuu.*
- OLIVIER, K. (2012). *introduction a la cyler stratégie.* paris.

- security, g. c. (s.d.). *world economic forum.* Récupéré sur https://www.weform.org/reports/global
- أحمد, م .(1997) .*الضرر في الفقه الاسلامي* .مصر: دار ابن عفان للنشر والتوزيع.
- أحمد, ه .(1989) .*حجية المخرجات الكمبيوترية في الإثبات الجنائي* .مصر: دار النهضة العربية.
- القادر, ا. ع .(2006) .*مصادر الحق الشخصي في القانون المدني* . عمان: دار الثقافة للنشر والتوزيع.
- القادر, د. ع .(2025) .الحروب السيبرانية في ظل القانون الدولي الإنساني .*المجلة الجزائرية للحقوق والعلوم* .
- الله, ا. ر .(2020) .الجرائة السيبرانية .*المجلة الالكترونية الشاملة متعددة التخصصات*.
- المنعم, ا. م .(s.d.) .*المرجع السابق* .
- المنعم, ا. م .(s.d.) .*المرجع السابق* .
- المنعم, ا. م .(s.d.) .*المرجع السابق* .
- المنعم, ا. م .(s.d.) .*المرجع السابق* .
- المنعم, ا. م .(s.d.) .*المرجع السابق* .
- المنعم, ا. م .(s.d.) .*المرجع السابق* .
- المنعم, ا. م .(s.d.) .*المرجع السابق* .
- المنعم, ا. م .(s.d.) .*المرجع السابق* .
- المنعم, ا. م) .د.س.ن .( التحديات القانونية أمام إثبات الضرر السيبراني في ظل تطور تقنيات الذكاء الاصطناعي .*المجلة القانونية* .3117 ,
- أنور, س .(2007) .*مصادر الالتزام في القانون المدني الأردني* .القاهرة: دار الثقافة للنشر والتوزيع.
- أيوب, ع. ا & .,البغدادي, أ .(2022) .الأخلاق والأمن السيبراني .*مجلة بنها للعلوم الإنسانية*.
- جيهان, ن & .,حشماوي, أ .(2021) .أثر القصد الجنائي في تحديد المسؤولية الجزائية .سعيدة, كلية الحقوق والعلوم السياسية, الجزائر.
- سليمان, م .(1922) .*الوافي في شرح القانون المدني* .القاهرة.
- صلاح, ش. م .(2024) .المسؤولية المدنية الناشئة عن استخدام الذكاء الاصطناعي .*مجلة العلوم القانونية والاقتصادية* .
- عبير, خ & .,علواني, ن .(2023) .دور تقنية البلوك تشين في التعاملات التجارية . قالمة, كلية الحقوق والعلوم السياسية , الجزائر.
- عمر, ر .(2020) .التعويض عن الضرر في الشريعة الاسلامية والقانون المدني الجزائري .*مذكرة لنيل شهادة الماستر في العلوم الاسلامية* .المسيلة, الجزائر.

- فاطمة, ب .(2020) .حجية التوقيع الالكتروني استنادا إلى القواعد العامة للإثبات وضرورة التدخل التشريعي .*مجلة الدراسات الحقوقية* .
- فكري, أ. ع .(2024) .المسؤولية الجنائية عن أعمال الذكاء الاصطناعي . *مجلة العلوم القانونية والاقتصادية* .
- محمد, ا. ن .(2023) .دور الذكاء الاصطناعي في دعم نظام العدالة وتحليل الأدلة الرقمية . *المجلة السعودية للدراسات القانونية* .
- محمود, ا. ر .(2017) .*القصد الجنائي في الجرائم المتعلقة بالانترنت والمعلوماتية* . مركز الدراسات العربية للنشر والتوزيع.
- مصطفى, ا. م .(2024) .ضرورة التدخل التشريعي لمواجهة مخاطر الذكاء الاصطناعي ومعالجة تطوره لحماية القيم الإنسانية في المجتمع المصري .*مجلة القانون*.
- وسيلة, س .(2023) .الذكاء الاصطناعي وتحديات الممارسة الأخلاقية .*مجلة نماء للاقتصاد والتجارة*.
- يزيد صالح الحميد. (بلا تاريخ). الجرائم السيبرانية في القانون الجنائي. *المجلة القانونية*، 2204.