ISSN:2509-0291
DOI
https://doi.org/10.63585/
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

جريمة الاعتداء على الوثائق الإلكترونية في القانون الموريتاني

The Crime of Assault on Electronic Documents under Mauritanian Law

الدكتورة المومنة محمد يسلم المصطفى
أستاذة بكلية الحقوق والعلوم السياسية، جامعة نواكشوط – موريتانيا
خبيرة قضائية معتمدة لدى المحاكم الموريتانية

ملخص:
تناول البحث تطور وسائل الاثبات من الوثيقة الورقية إلى الوثيقة الإلكترونية والتوقيع الإلكتروني نتيجة الثورة التكنولوجية، وقد اعترف المشرع الموريتاني في القانون رقم 022-2018 المتعلق بالمبادلات الإلكترونية بالوثيقة الإلكترونية ومنحها حجية في الاثبات، شريطة أن تتوفر على شروط الصحة والحفظ لكي تحظي بالحماية الجزائية.
وتتمثل شروط الصحة في وضوح المحتوى، سلامة البيانات من التعديل، ونسبتها إلى مصدرها عبر التوقيع الإلكتروني الذي عرفه القانون بأنه "بيان إلكتروني ملحق ببيانات أخرى للتعريف" وقد ساوى المشرع في المادة 84 بين التوقيع الإلكتروني المؤمن والتوقيع اليدوي.
أما شروط الحفظ فتتمثل في سهولة الوصول للبيانات، حفظها بنفس الشكل المرسل به دون تعديل، وحفظ بيانات المصدر والوجهة والتاريخ لمدة 5 سنوات وفق المادة 81. كما أجازت المادة 80 الاعتداد بالنسخ الإلكترونية إذا ثبتت مطابقتها.
كما تعرض البحث لصور الاعتداءات التي قد تطال الوثائق الإلكترونية وبين أركانها:
ـ الركن المادي: يتمثل في "إدخال أو تعديل أو تشويه أو محو أو حذف بيانات معلوماتية" بهدف إنتاج بيانات غير أصلية. وتشمل صورتين: صنع وثيقة مكذوبة أو تغيير محتوى وثيقة صحيحة، واشترطت المادة 13 حصول ضرر حتى تقوم الجريمة.
ـ الركن المعنوي المتمثل في القصد الجنائي العام والخاص، أي نية الجاني في تغيير الحقيقة واستعمال الوثيقة المزورة.
خلص البحث إلى أن المشرع الموريتاني قد وضع إطاراً قانونياً لحماية الوثائق الإلكترونية ومنحها قوة ثبوتية، مع تجريم الاعتداء عليها لضمان الثقة في المعاملات الإلكترونية، إلا أن فعالية هذه النصوص تبقي ترتبط بمدي مواكبتها للتطور التقني.
الكلمات المفتاحية: وثيقة إلكترونية، توقيع إلكتروني، جرائم إلكترونية، تزوير، القانون الموريتاني رقم 2018-022، القانون رقم 2016-007

Abstract
This research examines the evolution of means of proof from paper documents to electronic documents and electronic signatures as a result of the technological revolution. The Mauritanian legislator, in Law No. 2018-022 on Electronic Transactions, recognized the electronic document and granted it probative force, provided that it meets the conditions of validity and preservation in order to benefit from penal protection.
Validity conditions include: clarity of content, integrity of data against alteration, and attribution to its source through an electronic signature. The law defines it as "electronic data attached to other data for the purpose of identification". In

ISSN:2509-0291
DOI
https://doi.org/10.63585/
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

Article 84, the legislator equated a secure electronic signature with a handwritten signature.
Preservation conditions include: easy access to data, storing it in the same form in which it was sent without modification, and preserving data on the source, destination, and date for a period of 5 years in accordance with Article 81. Article 80 also allows electronic copies to be admitted as evidence if their conformity is proven.
The research also addressed the forms of assaults that may target electronic documents and explained their elements:
Material element: Consists of "introducing, modifying, distorting, erasing, or deleting computer data" with the aim of producing non-authentic data. It includes two forms: creating a false document or altering the content of a genuine document. Article 13 requires that harm occurs for the crime to be established.
Mental element: Consists of general and specific criminal intent, i.e., the perpetrator's intention to alter the truth and to use the forged document.
Conclusion: The study concludes that the Mauritanian legislator has established a legal framework to protect electronic documents and grant them probative force, while criminalizing assaults on them to ensure trust in electronic transactions. However, the effectiveness of these provisions remains linked to their ability to keep pace with technological developments.
Keywords: Electronic Document, Electronic Signature, Cybercrime, Forgery, Mauritanian Law No. 2018-022, Law No. 2016-007

المقدمة:

ظلت العلاقة بين الكتابة والدعامة الورقية علاقة وثيقة فترة طويلة من الزمن، إلا أن ظهور المعاملات التي تتم عن طريق وسائل التقنيات الحديثة وما تحمله من تسهيلات وسرعة في التعامل وتقريب للمسافة بين الأفراد، قد قلص من دور الوثيقة الورقية كأداة يعتمد عليها لاثبات معظم التصرفات القانونية، وقد أتاحت هذه التقنيات الجديدة وسائل إلكترونية يمكن الاعتماد عليها بدل الوسائل الورقية حيث أصبح بالإمكان الكتابة على جهاز الكمبيوتر، ونقل الرسائل من طرف إلى آخر عن طريق شبكات مفتوحة أو مغلقة، كما أنه أصبح من الممكن حمل المعلومة على أقراص مغناطيسية أو أقراص ضوئية مكتنزة، أو أقراص رقمية متعددة الوسائط، ونقلها بصفة يدوية من مكان إلى آخر، أو حفظها وتوثيقها بأوعية ضوئية أو إلكترونية مثل الميكروفيلم[1] والميكروفيش. إلا أن هذا الانتقال من العالم المادي إلى العالم الغير مادي حمل معه مفاهيم جديدة لم تكن معروفة في المعاملات والتي من أهم وسائل استقرارها وجود وسائل لاثباتها، يتعلق

1- الميكروفيلم هو عبارة على نتيجة لمعالجة آلية بالحاسب الإلكتروني ومن خصائصه أنه دليل مقرئي، لذا يمكن قراءة المعلومات من خلال عرضها علي الشاشة المتصلة بالجهاز كما يمكن الاحتفاظ بها، أما الاسطوانة الممغنطة فهي تتمثل في شكل قطعة معدنية دائرية الشكل يمكن شحنها مغناطيسيا بسهولة.

ISSN:2509-0291
DOI
https://doi.org/10.63585/
مجلة القانون والأعمال الدولية
Revue internationale du droit des affaires
www.Droitetentreprise.com
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

الأمر بالوثائق الإلكترونية والتوقيع الإلكتروني[2]، كأدوات لاثبات العلاقات الناشئة في البيئة الإلكترونية، بعد أن كانت المعاملات القانونية تتم عن طريق الوثائق الورقية والتوقيعات اليدوية مما يشكل تطورا كبيرا في وسائل الاثبات والتي تلعب دورا هاما في اثبات الحقوق وتحمل الالتزامات.[3]

وقد رحبت معظم التشريعات بهذا التغيير الحاصل في مجال التسجيلات الإلكترونية فقد اعترف المشرع الموريتاني في صياغته للقانون رقم 2018-022 المعلق بالمبادلات الإلكترونية بوضوح بالوثيقة الإلكترونية ومنحها قوة ثبوتية في الاثبات وعرفها ضمن الفقرة العاشرة من المادة الأولى من بأنها "مجموعة البيانات المسجلة أو المخزنة في الذاكرة على أية دعامة سواء بواسطة نظام معلوماتي أو آلية مماثلة والتي تمكن قراءتها أو إدراكها من قبل شخص أو من قبل ذلك النظام أو تلك الآلة، ويستهدف كذلك أي عرض أو إخراج مطبوع أو أي معالجة أخرى لتلك البيانات.

وهذا الاعتراف بالوثائق الإلكترونية تتضمنه بعض الشروط التي يجب أن تتوفر في الوثيقة من أجل أن تحظى بالحماية القانونية (المطلب الأول) قبل التعرض إلى الأفعال غير المشروعة المسلطة عليها (المطلب الثاني).

المطلب الأول: الوثيقة الإلكترونية المستوجبة للحماية الجزائية

إن التطور المذهل الذي شهده الميدان المعلوماتي وما وفره من إمكانيات لم تكن متوفرة في السابق والتي تضمن سلامة المعالجة الالكترونية من أي تدخل غير مشروع من الغير، أدى إلى تجنب عدة صعوبات عانت منها الوثيقة الإلكترونية في شكلها الورقي، غير أن هذه الأهمية لفضائل المعلوماتية، فإنه لا يمكن إنكار مخاطرها على الوثيقة

ولتجاوز هذه المخاوف من مخاطر التكنولوجيا التي يمكن أن تطال الوثيقة المخزنة إلكترونيا، سارعت كافة التشاريع إلى وضع برامج حمائية صارمة، ولم يكن المشرع الموريتاني في منأى عن هذه الحركة التشريعية، فقد أقر بضرورة أن تتوفر الوثيقة الإلكترونية على بعض الشروط للازمة لمنحها الحماية الجزائية، وهي أساسا شروط تتعلق بصحة الوثيقة الالكترونية (الفقرة الأولى) وشروط تتعلق بحفظ الوثيقة الالكترونية (الفقرة الثانية)

الفقرة الأولى: شروط صحة الوثيقة الإلكترونية

إن مفهوم الحفظ يقتضي أن يتم حفظ الكتب بشكل سليم ودائم، ولا يتم ذلك إلا إذا استكملت الوثيقة شكلها النهائي، وذلك بعد احتوائها كافة الشروط القانونية المطلوبة لصحتها. ومن ضمن تلك الشروط أن يكون الكتب ذا محتوي يمكن فهمه، مما يضمن

---

2 لا يمكن الحديث عن التّعامل الإلكتروني بدون الاعتراف بالوثيقة الإلكترونية والإمضاء الإلكتروني، وذلك ما يمثّل أسس التّعامل الإلكتروني في أيّ مجال. وفعلا كان أوّل ما شغل المشرعين هو التّقنين في هذا المجال وهو بالفعل ما سار عليه المشرع الموريتاني حيث أصدر القانون رقم 022 ـ 2018 ليعترف بالوثيقة الإلكترونية والتوقيع الإلكتروني.

3 لكن ومع ذلك. **ثار خلافا كبير بشأن مفعول الرسائل الإلكترونية الناتجة عن التعامل الإلكتروني ومدى صحتها وقابليتها للتنفيذ، ففي البداية لم يعترف رجال القانون بهذه الوسائل الحديثة في المعاملات، حيث كان الاعتقاد السائد أن تكون الوثيقة في شكل ورقي ملموس، وقد تأسست الأنظمة القانونية في مادة الاثبات على هذا المبدأ، إلا أنه وفي ظل التقدم العلمي الهائل وبلوغه درجة كبيرة من المعرفة والإتقان في هذا الجانب كما سبق وأن وضحنا، بين ضرورة الاعتراف بالوثيقة الإلكترونية والتي ربما تضمن درجة عالية من الدقة والوضوح، تفوق الكتائب الورقية، التي تكون عادة أكثر عرضة للتدليس بأيسر السبل، لذلك جاءت المبادرة من لجنة الأمم المتحدة للقانون التجاري الدولي سنة 1985 عندما طلبت من الدول الأعضاء والمنظمات الدولية إعادة صياغة الجوانب القانونية الخاصة بالتسجيلات الإلكترونية والمعلوماتية لغاية استعمال الوسائل الإلكترونية**

نظر في: **علي كحلون، العقد الإلكتروني**، م. ق. ت، ديسمبر 2001.

ISSN:2509-0291
DOI
https://doi.org/10.63585/
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

تحقيقه لغاية جعل المراسلة الإلكترونية مفهومه أمام العدالة ومقبولة كوسيلة اثبات[4]، ولا يمكن أن يتحقق ذلك إلا إذا تم حفظها بطريقة تضمن عدم قابليتها لأي تعديل أو تشويه في محتواها، وشرط الحفظ لا يجب أن يكون مجرد دليل فقط على وجود المعاملة، بل يكون دالا بعد ذلك على سلامة محتوى الوثيقة، وفي هذا الإطار اشترط القانون أن يأمن الحفظ الاطلاع على محتوى بيانات أخري تمكن من التعرف على هوية مصدر ووجهة رسالة البيانات، وكذلك تاريخ وساعة الإرسال والاستلام إن كانت موجودة، ولضمان ذلك ظهر مصطلح جديد على شبكة المعلومات الدولية، يسمى بـ"**سلامة بيانات المحرر الإلكتروني" ويقصد به** خلو البيانات التي يتضمنها المحرر الإلكتروني من أي تعديل، أو تحريف سواء بالحذف أو بالإضافة، وذلك أثناء نشأته، أو نقله، أو إرساله، أو حفظه، أو استرجاعه، بصرف النظر عن ما إذا كان التعديل عن قصد أو من غير قصد.

كذلك من بين شروط صحة الوثيقة بالإضافة إلى وضوح مفهومها صحة نسبتها إلى محررها، بحيث يكون ملزما بمحتوياتها لذلك استحدث التوقيع الإلكتروني كوسيلة للتعريف بهوية مصدر الوثيقة الإلكترونية، كما يفترض شرط حفظ الوثيقة كذلك أن يتم حفظها على حامل يؤمن قراءتها والرجوع إليها متى اقتضت الحاجة إلى ذلك.

عليه، وانطلاقا من الأهمية التي يعطيها القانون الموريتاني لنظام الاثبات، فقد منح الوثائق للإلكترونية مكانة متميزة حيث اعتبرها دليل اثبات كامل، وكذلك يحظى التوقيع الإلكتروني بأهمية بالغة صلب هذا النظام، ويعرف التوقيع الإلكتروني بأنه العلامة التي يضعها المتعاقد على الوثيقة تحت أية صورة كانت للدلالة على هويته وعلى موافقته على ما تتضمنه الوثيقة[5]، وقد دقق البعض هذا المفهوم بأنه تسجيل شخصي معروف يعبر به من صدر عنه للدالة على هويته وموافقته على محتوي الوثيقة[6].

ويعتمد التوقيع الإلكتروني على وظيفتين الأولى عضوية تتمثل في تحديد هوية الشخص الموقع، طالما كانت العلامة الموضوعة هي علامة شخصية ومعلومة نسبتها للشخص، أما الثانية فتتعلق بالتعبير عن إرادة واضحة واطلاعه على محتوى الوثيقة وموافقته على مضمونها، مما يعني الحضور المادي للشخص المعني[7].

وفي هذا الإطار وضع الاتحاد الأوربي معايير عامة للتوقيع الإلكتروني، بتاريخ 30 نوفمبر 1999، أعتمد الاعتراف بالتوقيع الإلكتروني بكل أشكاله، وعدم اشتراط المصادقة المسبقة وترك الحرية للأطراف المتعاقدة وضمان صلتهم بمضمون الوثيقة، كما تحدث كذلك عن التوقيع الإلكتروني المتقدم أو المدعم، للدلالة على الإمضاءات المؤمنة وشهادات المصادقة الإلكترونية[8].

وقد اعتمدت أغلب التشاريع في العالم إطارا قانونيا للتوقيع الإلكتروني، من ذلك ما ذهب إليه المشرع الموريتاني الذي جعله شرطا من الشروط اللازمة لصحة الوثيقة الإلكترونية، وعرفه بأنه "بيان على شكل إلكتروني ملحق أو مربوط منطقيا ببيانات

4 ـ Roger Garraud, traite théorique et pratique de droit pénal français ,tom 3 43p

5ـ **علي كحلون**، التجارة الإلكترونية، م. ق. ت، فيفري 2000، ص 39.

6ـ **عز الدين الحناشي**، إدارة الاثبات من النظرة التقليدية إلى التجارة الإلكترونية، م. ق. ت، عددـ 1999، ص 119.

7ـ **عمر الطيب**، الكتب الإلكتروني، م. ق. ت، أكتوبر 2001، ص 441.

8 ـ **عبد الفتاح أبيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 146.

ISSN:2509-0291
DOI
https://doi.org/10.63585/
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

إلكترونية أخري ويستخدم كطريقة للتعريف[9]"، كما أنه أنشأ هيئة مختصة بالإمضاءات الإلكترونية حدد مهامها وضوابطها ضمن شروط يضبطها القانون[10].

وعليه فالتوقيع الإلكتروني لا يمكن أن يعتد به إلا إذ اعتمد على منوال تعريف موثوق به يضمن صلة الإمضاء المذكور بالوثيقة الإلكترونية المرتبطة به، ويقر علماء الإعلاميّة ورجال القانون على حدّ السّواء كذلك، أنّ ضمان الصّلة بين الإمضاء وصاحبه لا يمكن أن يتحقّق من الوجهة الواقعيّة إلا بتدخّل طرف ثالث يسمي بمزوّد خدمات المصادقة الإلكترونية[11].

تدقيق هنا هل مزود الخدمات هو منظوم موثوق بها كما أن الإمضاء لا يمكن أن يعتدّ به إلاّ إذا اعتمد على منوال تعريف موثوق به، وقد قدّمنا أنّ الطّرق في الإمضاء يمكن أن تتعدّد،

وقد اختلفت المواقف حول مدى مصداقية الإمضاء الإلكتروني، حيث يري البعض أن الإمضاء الإلكتروني لا يرقي إلى مرتبة الإمضاء اليدوي، بينها ذهب رأي آخر إلى اعتبار التوقيع الإلكتروني تقنية تستجيب للسلامة القانونية، ويمكن اعتباره طريقة من طرق تعريف المتعاقدين وبالتالي لا يمكن حصر العنصر المادي في وصف معين أو شكل خاص[12].

ما يلاحظ هو أن أغلب التشريعات إن لم تكن كلها قد منحت القوة الثبوتية للتوقيع الإلكتروني، كما عليه الحال في التوقيع اليدوي.

من ذلك ما نص وهو ما سار عليه المشرع الموريتاني صلب المادة 84 على أنه ودون المساس بالأحكام المعمول بها، فإن التوقيع الإلكتروني المؤمن المنشأ بواسطة نظام لإنشاء التوقيع الآمن والذي يستطيع الموقع حفظه تحت رقابته الحصرية والذي يعتمد تدقيقه على إفادة مؤهلة يقبل كتوقيع مثل التوقيع اليدوي.

ويتخذ التوقيع الإلكتروني عدة تطبيقات، منها الرقم السري المعتمد في البطاقات البنكية وكذلك الإمضاء البيو متري المعتمد على بصمات اليد أو قزحية العين، ويبقي أهمها وأكثرها شيوعا الإمضاءات المعتمدة على وسائل التشفير[13].

---

9 ـ الفقرة 19 من المادة 1 من القانون الموريتاني رقم 022 ـ 2018، الصادر بتاريخ 12 جويلية 2018 المتعلق بالمبادلات والتجارة الإلكترونية.

10 المادة 90 من القانون 2018 ـ 022 من القانون السابق التي تنص على أنه " **تنشأ بالطرق المحدد بالطرق التنظيمية، سلطة تصديق لغرض تحديد السياسة الموريتانية في مجال التصديق والعمل على تطبيقها. خاصة بواسطة الاعتماد ورقابة مقدمي خدمات التصديق المؤهلين"**

وقدد حدد القانون الشروط التي يجب أن تتوفر لدي مقدم خدامات التصديق الإلكتروني، وذلك ضمن المادة 92 من القانون المذكور، كما أكدت المادة 93 مسؤولية مقدم وثيقة مؤهلة للجمهور عن الأضرار الناتجة لأي كيان أو شخص طبيعي أو معنوي يثق بشكل معقول في تلك الإفادة فيما يخص:

ـ صحة كافة المعلومات الواردة في الإفادة المؤهلة عند التاريخ الذي سلمت فيه، واحتواء هذه الإفادة على كافة البيانات المطلوبة للإفادة المؤهلة.

ـ التأكد بأن الموقع المعرف في الإفادة كان يمتلك عند تسليم الإفادة. البيانات المتعلقة بإنشاء التوقيع المتطابقة للبيانات المتعلقة بتدقيق التوقيع المسلمة أو المبينة في الإفادة.

ـ التأكد من البيانات المتعلقة بإنشاء التوقيع وتلك المتعلقة بتدقيق التوقيع يمكن استخدامها بشكل تكميلي، في حالة إنشاء مقدم خدمة التصديق لهذين النوعين من البيانات. إلا إذ أثبت مقدم خدمة التصديق أنه لم يرتكب أية إهمال.

11 عرفت الفقرة 17 من القانون الموريتاني رقم 022 ـ 2018، مقدم خدمات التصديق الإلكتروني بأنه" إي شخص يصدر إفادات إلكترونية أو يقدم خدمات أخري في مجال التوقيع الإلكتروني"

12 ـ **علي كحلون**، التجارة الإلكترونية، م. ق. ت، فيفري لسنة 2000، ص 40.

13 **طه بن محمد ناصر الشابي**، مرجع سابق، ص 104 .

التشفير هو ووسيلة تقنية تمكن من تحويل النص الإلكتروني إلى رموز مبهمة يعسر معرفة فحواها إلا من قبل المرسلة إليه اعتماد على طريقة فنية لتفكيك رموزها قصد إدراك مضمونها.

تتخذ الإمضاءات المعتمدة على وسائل التشفير نوعين، التّشفير التّماثلي والتّشفير اللاتماثلي ويعتمد التّشفير التّماثلي

ISSN:2509-0291
DOI
https://doi.org/10.63585/
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

من ذلك ما تعتمده المؤسسات البنكية في البطاقات الذكية لسحب الأموال مع تمكينها لحرفائها ما يسمي بالرمز السري وهو عبارة عن أربعة أرقام وبمجرد إدخال البطاقة مع تضمين الرمز السري في الموزع المالي يعد من قبيل الإمضاء الإلكتروني المعادل للإمضاء اليدوي يتمكن بموجبه الحريف من سحب المبلغ المطلوب[14].

الفقرة الثانية: شروط حفظ الوثيقة

يتطلب استقرار المعاملات ضرورة وجود وسائل لاثباتها، فكلما ارتقي المجتمع كلما وجدت وسائل جديدة يتم من خلالها عقد تلك المعاملات والاتفاق على كافة بنودها وتوضيح حقوق أطرافها ووجباته، ومسؤوليات كل طرف اتجاه الطرف الآخر، ومع انتشار التجارة الإلكترونية، ووسائل التواصل الحديثة اكتسبت الوثيقة الإلكترونية أهمية كبيرة كوسيلة لإتمام المعاملات.

إذ أن الوثيقة الإلكترونية في تعريفها هي عبارة عن سلاسل من الأرقام والمفاتيح التي يفهمها جهاز البرمجة المعلوماتية ويخرجها في حلتها النهائية عبارة عن نص مكتوب مضمن في وعاء إلكتروني[15]، فهي على العكس من الوثيقة الورقية العادية غير ملموسة، بمعنى أنها تكون ذات استعمال مباشر كالإنترنت أو استعمال غير مباشر كالأقراص الضوئية المكتنزة، وبالتالي فهي مجموعة بيانات مجسدة ضوئيا ومخزنة ماديا على أقراص معلوماتية أو أوعية مغناطيسية أو ضوئية، تكون محفوظة ضمن حوامل إلكترونية تؤمن قراءتها عند الرجوع إليها، وهو ما يعني معالجة البيانات على الحاسوب وتحويلها عبر الشبكات ونقل البيانات الإلكترونية على الحوامل المغناطيسي.

عليه، فالتعامل الإلكتروني يحمل معنيين: المعني الأول هو ما يعرف بمعالجة البيانات الإلكترونية، بمعني استعمال وسائل الاتصال الحديثة في تخزين المعلومة ومعالجتها، وهذه المعالجة أصبحت اليوم لا تطرح إشكال كبير باعتبار أن هذه التقنية أصبحت مستعملة في أغلب المؤسسات.

أما المستوي الثاني فهو تبادل المعطيات الإلكترونية، أي نقل المعلومة من مكان لآخر، وذلك عن طريق وسائل الاتصال الحديثة، أي الربط بين عدة حواسيب في أماكن مختلفة[16].

وفي نفس السياق تثير عملية نقل المعلومة عدة إشكاليات تمثلت في نوعية نقلها لأنها قد تتعرض أثناء عملية نقلها إلى الإتلاف أو التخريب، لذلك وضع المشرع عدة ضوابط

على مفتاح واحد، سواء في التّشفير أو فكّ التّشفير. لكنّ هذه الطّريقة تتطلّب إحالة المفتاح بين الأطراف بطريقة يجب أن تضمن سلامته. ويعتمد التّشفير اللاتماثلي على مفتاحين مترابطين، المفتاح الخاصّ ولا يمكن أن يعلمه إلا المعني بالأمر والمفتاح العام وهو معلوم من طرف جميع المتعاملين، حيث يتمّ تشفير الوثيقة بواسطة المفتاح الخاص، فتصبح غير مقروءة، وترسل على الشّبكة، فإذا فتحت للمرسل إليه بواسطة المفتاح العام المعلوم لديه، فيعلم حينئذ أن المراسلة جاءت فعلا من الباعث المعني دون الآخر. وتمكّن هذه الطّريقة من التّعريف بالباعث واستثباته، لكنّها لا تضمن سريّة وسلامة الوثيقة لأنّه يمكن لأي طرف أن يطّلع عليها فيغيّر محتواها. لذلك اتّجه التّطبيق إلى استعمال طريقة التّشفير المزدو وهو أن تشفّر الرّسالة أوّلا بواسطة المفتاح السّري للمرسل، وهو ما يضمن التّعريف بالباعث، وثانيا بواسطة المفتاح العام للمرسل إليه، وهو ما يضمن سريتها، حيث أن فتحها لا يمكن أن يتحقّق إلاّ بواسطة المفتاح الخاصّ الذّي لا يمكن أن يعلمه إلا المرسل إليه. وإذا ما وصلت المراسلة إلى المرسل إليه فكّ التّشفير الأوّل بواسطة المفتاح العام للباعث، فيتعرّف على المرسل، وفكّ المستوى الثّاني بواسطة مفتاحه الخاص، فيتعرّف على محتوى الرّسالة. وإذا كان الغرض هو تقرير سلامة الوثيقة من التّغيير، دون سريّة المعلومة، وفي نفس الوقت التّحقّق من هويّة المراسل، فيمكن الاستعمال المزدوج لمنظومة الإمضاء ومنظومة، ورغم أن هذه الطّرق تبدو معقّدة من حيث تكوينها، فإنّها سهلة الاستعمال، لأنّها في نهاية الأمر لا تعدو أن تكون سوى برمجيات، تؤدّي المطلوب بمجرّد تطبيقها على الجهاز. نظر في: **علي كحلون، العقد الإلكتروني**، ص، وما بعدها 44 **وما بعدها.**

14 **طه بن محمد الناصر الشابي،** التدليس الإلكتروني، مرجع سابق، ص، 105.

15 **طه بن محمد الناصر الشابي،** التدليس الإلكتروني، مرجع سابق، ص 102.

16 ـ **كحلون**، التجارة الإلكترونية، مرجع سابق. ص42.

Volume 11 issue 4
N:65 August 2026
ISSN:2509-0291
DOI
https://doi.org/10.63585/

تتعلق بكيفية إعدادها وحفظها وكذلك التعرف على الأطراف المتعاقدة، كل ذلك من أجل أن تضمن الوثيقة الإلكترونية مصداقيتها.

وإذا كان من المسلم به أن المشرع قد منح الوثيقة الإلكترونية الحجية القانونية اللازمة كوسيلة اثبات شأنها شأن المحررات التقليدية واعتبراها أدلة كتابية مهما كانت دعامتها، إلا أن هذه الحجية مبنية على توافر مجموعة من الشروط، اللازمة لصحتها والتي بدونها لا يمكن أن تعتمد كدليل قانوني في أي نزاع.

من خلال قراءة النص القانوني المتعلقة بالوثيقة نجد أن المشرع قد ربط بين حجية الوثيقة ومسألة حفظها، إذ حدد المشرع وظائف السند الإلكتروني، وحدد وظائف الحامل الإلكتروني صلب المادة 81 ـ[17] من نفس القانون وهي:

1ـ المعلومات التي تشملها رسالة البيات يجب أن يكون النفاذ إليها سهلا، وأن تكون مقروءة ومفهومة من أجل الرجوع إليها لاحقا.

2 ـ يجب حفظ رسالة البيانات بالشكل الذي أنشئت أو أرسلت أو استقبلت به، أو على شكل يمكن اثبات عدم قابليته للتعديل أو التشويه في محتواه، وأن الوثيقة المرسلة وتلك المحفوظة متطابقتان تماما.

3 ـ يجب حفظ المعلومات التي تمكن من تحديد مصدر ووجهة رسالة البيانات، وكذا تبين تاريخ وساعة الإرسال أوالاستلام إذا كانت موجودة.

ومدة الحفظ تكون خمس سنوات حسب أحكام هذه المادة.

بالنسبة للوسائل المعتمدة في حفظ الوثيقة الالكترونية، فقد اشترط المشرع ضرورة توفر حوامل الكترونية تتحمل عملية الحفظ، والحوامل الإلكترونية هي عبارة عن أوعية حديثة لحفظ

إن الغاية الأساسية للمشرع في إيجاد السبل الكفيلة بحفظ الوثيقة الالكترونية، إنما هي أساس اعتبار الوثيقة الالكترونية "كتبا قانونيا" يمكن الاحتجاج به أمام المحاكم[18]. إذ أن النصوص التشريعية وانطلاقا من مبدأ ضرورة أن تكون نصوصا مواكبة للتطورات التكنولوجية، اتجهت كافة التشاريع ومن بينها المشرع الموريتاني إلى اعتبار الوثيقة الالكترونية التي تتوفر فيها كافة شروط الحفظ حجة قانونية يمكن الاعتماد عليها، هذا إضافة إلى الاعتراف بالنسخ المستخرجة من بعض التّطبيقات الإلكترونية، فيعطيها الحجّية المناسبة، ولأن كان الأصل في العالم الإلكتروني له مدلول خاص، ومن الصعب التّفريق بين أصل الحجّة ونسختها، ولا يعدّ ذلك إلاّ من قبيل الأمور الاصطناعيّة. لكنّ المشرّع أدمج مفهوم النسخة بمقتضي المادة 80 من القانون 022 ـ 2018، التي تنص على أنه تجوز النسخة المبرمة بطريقة إلكترونية أو أي استنساخ آخر له نفس الحجية إذا تم اثبات مطابقتها من قبل الهيئات المعتمدة للتصديق، وعند الاقتضاء يلزم مؤدي التصديق إلى إعطاء نسخة مطابقة.

17ـ المادة 81 من الفصل الثاني من القانون رقم 2018 ـ 022 المتعلق بالمبادلات والتجارة الإلكترونية.

18 حيث أصبح من الهين التعرف على هوية المتعاقدين والحيلولة دون إنكارهم للمراسلات المتبادلة بينهم، وذلك لضمان سلامة أوفر مما كان عليه الحال بالنسبة للوثيقة الورقية التي من الصعب أن تسلم كما هو معلوم من التزوير والتدليس وكذلك تقليد التوقيع المتضمن بها. وهذا التحول التدريجي من الوثيقة الورقية إلى الوثيقة الإلكترونية صاحبه جدل واسع حول مدي قبول هذه الوثائق في مادة الاثبات مما أثار خلافا على مستوي الفقه والقضاء، فقد أنكر العمل القضائي على الكتائب الإلكترونية في بداية ظهورها أي قيمة ثبوتية، واتجه الفقه إلى اعتبارها قرينة من جملة القرائن. نظر في: **زهير إسكندر**، التشريع التونسي والتكنلوجيا الجديدة للمعلومات، م. ق. ت، الصادرة بديسمبر 2005 ص 50.

وقد ظل هذا الجدل قائما حتى أخذ المشرع بزمام الأمور، إذ جعل المشرع الوثيقة الإلكترونية بمقتضي المادة 77 من القانون رقم، 022 - 2018 المتعلق بالمبادلات والتجارة الإلكترونية في مرتبة الكتب الرسمي المادة 77 من القانون رقم 2018-022:" "يقبل المكتوب بالطريقة الإلكترونية دليل بنفس درجة المكتوب على دعامة ورقية ويمتلك نفس القوة الثبوتية، شريطة تمكينه من التعريف القانوني على الشخص الصادر عنه، وأن يكون تم إعداده وحفظه ضمن الشروط الكفيلة بسلامته.

ISSN:2509-0291
DOI
https://doi.org/10.63585/
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

المطلب الثاني: صور الاعتداء على الوثيقة الالكترونية

إن الهدف من تجريم الاعتداءات المسلطة على الوثيقة الإلكترونية، يتمثل في صيانة حقيقة الوثيقة وحمايتها من كل أشكال الاعتداء. وهذه الحماية الجزائية تضمن توفر الثقة في الوثيقة الإلكترونية، التي أصبحت يعتمد عليها في حفظ واثبات حقوق الأفراد، خاصة في ظل أنتشار المعلوماتية واكتساحها كافة المجالات، حيث أصبحت تجري من خلالها الكثير من العمليات ذات الآثار القانونية الهامة[19] .

يتمثل الاعتداء الذي يمكن أن يطال الوثيقة الالكترونية أساسا في جريمة التدليس، وهو ما نص عليه المشرع الموريتاني صلب المادة 12 من القسم الثالث من الفرع الثاني من القسم الثاني من الفصل الثاني من القانون 2016-007 التي جاء بها **"كل من قام عن قصد وبدون حق بإدخال أو تشويه أو محو أو حذف بيانات معلوماتية منتجا بيانات غير أصلية بهدف أن تأخذ البيانات المنتجة بعين الاعتبار أو تستخدم لأغراض قانونية كما لو كانت أصلية سواء كانت أم لا مقروأة ومفهومة بشكل مباشر بالحبس من سنتين إلى خمس سنوات وبغرامة من 500.000 إلى 2.000.000 أوقية أو بإحدى هاتين العقوبتين...".**

عليه فجريمة التزوير الواقعة على الوثيقة الالكترونية تتعلق بإدخال تغيير بأي شكل كان على محتوي وثائق معلوماتية أو إلكترونية أصلها صحيح. وكغيرها من الجرائم تتكون جريمة التدليس المعلوماتي من ركن مادي (الفقرة الأولى) وركن معنوي (الفقرة الثانية).

الفقرة الأولى: الركن المادي

الركن المادي في جريمة التدليس يعني وقوع نشاط الإجرامي من شأنه تغيير الحقيقة في محرر بطريقة ما، نص عليه القانون وأن يكون من شأن هذا التغيير إلحاق الضرر بالغير أو احتمال حدوثه. فيشترط لقيام جريمة التدليس المعلوماتي توفر عنصرين يتمثل العنصر الأول في تغيير الحقيقة أي الفعل المجرم (أولا) ويتمثل العنصر الثاني في حصول النتيجة الإجرامية "ضرر" (ثانيا)

أولا: صور الأفعال المجرمة

تتمثل أساسا صور الأفعال المجرمة في **" إدخال أو تشويه أو محو أو حذف بيانات معلوماتية"** حسب المادة 12 من القانون الموريتاني، فالحذف أو التشويه أو الحذف كما ذهب إلى ذلك المشرع إنما في الحقيقة كلها أفعال لإبدال الحقيقة المضمنة بالوثيقة بحقيقة أخري مغايرة لها تماما أو إبدال جزء منها بأخرى بالتالي فإن تغيير الحقيقة هو إبدالها بما يخالفها وإذا لم يكن هناك تغيير لا يمكن الحديث عن وجود جريمة تدليس[20]، والمقصود بتغيير الحقيقة هو تغيير الحقيقة النسبية وليس تغييرا للحقيقة الواقعية المطلقة[21].

وبما أن تغيير الحقيقة هو أحد العناصر الجوهرية اللازم توفرها لقيام جريمة التدليس يجب أن يكون حاصلا في محرر مكتوب أو علي البيانات والمعطيات المخزنة والمبرمجة في الحاسوب ويجب أن تصدر من شخص معين وذلك بالطرق المحددة قانونا[22].

19 **عبد الفتاح أبيومي حجازي**، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 152.
20 **عبد الفتاح بيومي حجازي**، "الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت"، مرجع سابق، ص 16.
21 **عبد الفتاح بيومي حجازي**، المرجع السابق، ص 17.
22 **محمد علي العريان**، مرجع سابق، ص 138.

ISSN:2509-0291
DOI
https://doi.org/10.63585/
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

ويعتبر المحرر في مضمونه الكتابة المركبة من حروف أو علامات تدل على معنى أو فكرة معينة مع إمكانية القراءة البصرية لمحتواه وهو ما تفترضه نصوص التزوير التقليدية[23].

وبالتمعن في النص التشريعي نلاحظ أن المشرع كان أوسع من حيث تحديده لأفعال التدليس التي يمكن أن تسلط على الوثيقة الالكترونية وهو ما نتبين من خلال صور الأفعال التالي:

أ: صنع وثيقة مكذوبة

يتمثل في صنع أو خلق محرر بأكمله ونسبته لغير محرره وذلك لخدمة غرض غير شرعي للجاني ويتم نسبتها لغير محررها بطابع وإمضاء مدلس ومزور لكي يستمد منه قيمته القانونية[24] ويتم الصنع الالكتروني من خلال إدخال المصطنع ما يريد من معلومات أو بيانات إلى الحاسب الآلي، ومن ثم ينسب صدورها إلى شخص ما أو جهة ما، ثم يستخرجها من الحاسب الآلي بوصفها منسوبة إلى ذلك الشخص أو تلك الجهة.

ولذلك يعد تزييف العملة الورقية باستخدام الماسح الضوئي والحاسب الآلي من طرق الاصطناع كما هي من طرق التقليد، لأن الاصطناع هو إيجاد محرر بأكمله ونسبه إلى غيره، ولا توجد صعوبة في إدخال عناصر المحرر المراد تزويره إلى الحاسب الآلي سواء عن طريق الماسح الضوئي، أو عن طريق لوحة المفاتيح، بل وعن طريق استدعاء المعلومات من الإنترنت ثم صياغتها في هيئة المحرر المزور الذي يطلبه الجاني ويطبعه ويستخدمه حسب رغبته.[25]

كما تجدر الإشارة إلى أن صنع الوثيقة الالكترونية يمكن أن يكون إما بصنع وثيقة غير موجودة من أصلها أو صنع وثيقة مخالفة لأصلها والحالة الأولي تجسد الخلق الفعلي للسند الالكتروني ذلك أن الموظف يقوم بتحديد جميع عناصر الوثيقة المكذوبة دون أن يكون لها وجود في الحقيقة في حين الحالة الثانية والمتمثلة في صنع وثيقة مخالفة لأصلها يكون فيها الموظف عالما بحقيقة الأمر وبحقيقة الوثيقة الأصلية ورغم ذلك يقوم بصنع وثيقة جديدة مخالفة تماما للتنصيصات الأصلية.

ويعتبر صنع الوثيقة الالكترونية في جريمة في حد ذاته مستقلة عن جريمة تغيير الحقيقة.

ب: أفعال تغيير محتوى الوثيقة

نصت المادة 12 على أنه **"كل من قام عن قصد وبدون حق، بإدخال أو تعديل أو تشويه أو محو أو حذف بيانات معلوماتية..."**.

نلاحظ في هذا الإطار أن المشرع حدد الأفعال التزوير التي يمكن أن تطال الوثيقة الالكترونية.

وتغيير المحررات قد يكون إما بالإدخال معطيات جديدة أو الحذف بعض المعطيات أو تعديلها وتحدث الإضافة بزيادة كلمة إلى اسم ورد في المحرر أو إلى الإمضاء أو بزيادة رقم المبلغ المكتوب في المحرر أو في التاريخ أو بزيادة كلمات في مكان خال في المحرر[26].

فالتغيير المعاقب عليه يجب أن يمس بالبيانات الأساسية للوثيقة وهو ما دأب عليه فقه القضاء فيما يتعلق بالمحررات حيث اعتبرت محكمة التعقيب التونسية في احدي قراراتها

---

23 **مصطفي السعيد مصطفي،** " قانون العقوبات "، القسم العام، دار النهضة العربية، 2000، ص 100.

24 **عبد الفتاح بيومي حجازي**، مرجع سابق، ص 200.

25 ـ **عبد الفتاح بيومي حجازي**، نفس المرجع السابق، ص 201.

26 : **فوزية عبد الستار**، "شرح قانون العقوبات القسم الخاص"، مرجع سابق، ص 100.

ISSN:2509-0291
DOI
https://doi.org/10.63585/
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

[27] حيث اعتبرت أن التزوير "هو تعمد تغيير الحقيقة في أمر جوهري بإحدى الطرق". وفي مناسبة ثانية واعتبرت أنه لا نزاع في أنه من الأركان الأساسية التي تقوم عليها جناية الزور قصد الجاني عن سوء نية تغيير الحقيقة في أمر جوهري" [28].
وتعتبر البيانات الجوهرية البيانات التي لها قيمة قانونية وهي كل تنصيص يراه الأطراف والقانون عنصرا جوهريا للوثيقة الالكترونية[29].

ثانيا: حصول الضرر

يعتبر الضرر عنصرا أساسيا لقيامة الجريمة بشكل عام، عدي الجرائم الشكلية التي تقوم في الكثير من صورها بمجرد وقوع الفعل الغير مشروع بغض النظر عن حصول ضرر من جراءه أم لا.
ونظرا لأهمية عنصر الضرر في جريمة الاعتداء على الوثيقة الإلكترونية، ذهب البعض إلى اعتباره ركنا مستقلا، قائما بذاته عن الركن المادي، بينما يري جانب آخر أنه عنصر من عناصر الركن المادي لجريمة تدليس الوثائق الإلكترونية، نظر لارتباطه بالوثيقة.

فاشترط المشرع لقيام الركن المادي في جريمة التدليس الإلكتروني حصول الضرر وهو ما نص عليه صراحة إذا جاء بالمادة 13 من القانون رقم 07-2016 أنه: " كل من يتسبب عن قصد وبدون حق، في إلحاق ضرر بأملاك الغير، بواسطة: إدخال أو تشويه أو محو أو حذف بيانات معلوماتية، أي شكل من أشكال المساس بسير نظام معلوماتي".
يتضح من خلال النص أن المشرع اشترط حصول ضرر ناتج عن فعل التزوير الذي لحق بالوثائق الإلكترونية، مما يجعل جريمة التدليس الإلكتروني من الجرائم المادية، حيث أنه إذا لم ينتج عن فعل التدليس أي ضرر فلا تمكن مساءلة الفاعل.
بمعني أن الضرر هو الأثر المترتب عن تغيير الحقيقة بإحدى الطرق القانونية في الوثيقة الإلكترونية، فلا يخضع فعل تغير الحقيقة في الوثيقة لنصوص القانون الجنائي باعتباره تزويرا إلا نتج عنه ضررا يمس بحقوق الغير، سواء كان ضررا عام يمس المجتمع ككل، أو ضرر خاصا يمس بمصلحة فرد بعينه.

الفقرة الثانية: الركن المعنوي

لا يمكن بأي حال من الأحوال إدانة أي أحد الأفعال الإجرامية الصادرة عن الأفراد بصورة قاطعة، ما لم يكن ذلك الفعل مشروطا بوجود الركن الثاني من أركان الجريمة، ألا وهو الركن المعنوي المتمثل هنا في القصد الجنائي، فكل جريمة تتطلب القصد الجنائي من أجل ضمان اكتمال الإدانة.
فالركن المعنوي أو الركن القصدي للجريمة يعد أهم الأركان في جريمة التدليس، وقد اشترط المشرع الموريتاني ضرورة توفر هذا الركن في جريمة تدليس الوثيقة الالكترونية.
إذ أقر صلب المادة 12 من قانون 07-2016 أن يكون الاعتداء على الوثيقة الالكترونية والذي جاء به" **كل من قام عن قصد وبدون حق..."، كما أقر ذلك أيضا صلب المادة 13 من ذات القانون والتي وردت على الصياغة التالية أن " كل من يتسبب عن قصد وبدون حق...".**

---

27 قرار تعقيبي جزائي عدد 3834 مؤرخ في 10_3_1965 نشريه محكمة التعقيب 1965 ص 88.
28 قرار تعقيبي جزائي عدد 5737 مؤرخ في 11-7-1981 نشريه محكمة التعقيب 1981 ص 143.
29 **منية بن ترادیت غمارسة**، "الجرائم المعلوماتية"، مرجع سابق، ص 89.

ISSN:2509-0291
DOI
https://doi.org/10.63585/
Volume 11 issue 4
N:65 August 2026
جامعة الحسن الأول سطات
كلية العلوم القانونية و السياسية
مختبر البحث قانون الأعمال

نلاحظ في هذا الإطار أن ركن القصد ركنا أساسي في جريمة التزوير الالكتروني في القانون الموريتاني أي أن تتوجه إرادة الجاني العمدية إلى ارتكاب الجريمة مع العلم بارتكابها، بالإضافة إلى القصد الجنائي الخاص، حيث لا بد أن تتوافر لدى الجاني نية استعمال الوثيقة محل التزوير فيما زورت من أجله وبه يتحقق القصد لقيام التزوير وانصراف إرادة الجاني إلى ارتكاب الفعل المـادي المكون له مع علمه بذلك.
ويجب أن يقترن القصد الجنائي العام والذي يتمثل في نية الجاني لتحقيق نتيجة إجرامية للقصد الجنائي الخاص أي الهدف الذي يسعي الجاني لتحقيقه من جراء جريمته والذي يتمثل في جريمة التدليس الالكتروني بتغيير الحقيقة وإحداث ضرر للشخص المستهدف بالتدليس.

الخاتمة:

من خلال ما سبق خلص البحث إلى جملة من الاستنتاجات نجملها في اللآتي:

ـ الاعتراف القانوني بالوثيقة الإلكترونية

لقد اعترف المشرع الموريتاني في القانون رقم 022-2018 المتعلق بالمبادلات الإلكترونية بالوثيقة الإلكترونية ومنحها نفس الحجية القانونية للوثيقة الورقية في الاثبات مما يمثل نقلة نوعية في نظام الاثبات الموريتاني.

لكي تتمتع الوثيقة الإلكترونية بالحماية الجزائية وضع المشرع مجموعة من الشروط تتمثل في:

ـ صحة وضوح المحتوى، سلامة البيانات من التعديل، ونسبتها إلى مصدرها عبر التوقيع الإلكتروني وساوى المشرع في المادة 84 بين التوقيع الإلكتروني المؤمن والتوقيع اليدوي.

ـ شروط الحفظ سهولة الوصول للبيانات، حفظها دون تعديل، وحفظ بيانات المصدر والوجهة والتاريخ لمدة 5 سنوات وفق المادة 81 وأجازت المادة 80 الاعتداد بالنسخ الإلكترونية إذا ثبتت مطابقته.

تجريم الاعتداء على الوثائق الإلكترونية

نص القانون رقم 007-2016 المتعلق بالجريمة السيبرانية على تجريم أي اعتداء على الوثائق الإلكترونية وتقوم الجريمة على ركنين:

ـ الركن المادي "إدخال أو تعديل أو تشويه أو محو أو حذف بيانات معلوماتية" بهدف إنتاج بيانات غير أصلية ويشمل صورتين، صنع وثيقة مكذوبة أو تغيير محتوى وثيقة صحيحة واشترطت المادة 13 حصول ضرر لقيام الجريمة.

ـ الركن المعنوي القصد الجنائي العام والخاص، أي علم الجاني وتعمد تغيير الحقيقة واستعمال الوثيقة المزورة.

ـ تشديد العقوبة وتوسيع نطاق المسؤولية، كما أقر المسؤولية الجنائية للشخص المعنوي عن هذه الجرائم.

ـ أهمية التوقيع الإلكتروني

أصبح التوقيع الإلكتروني الوسيلة الأساسية لاثبات نسبة الوثيقة لمصدرها. ويعتمد على وظيفتين تحديد هوية الموقع، والتعبير عن الرضا بمحتوى الوثيقة.

وفي الأخير خلص البحث إلى أن المشرع الموريتاني وضع إطاراً قانونياً متكاملاً لحماية الوثائق الإلكترونية وضمان الثقة في المعاملات الإلكترونية، إلا أن فعالية هذه النصوص تبقى مرتبطة بمدى قدرتها على مواكبة التطور التقني السريع في مجال الجريمة السيبرانية، وبتوفير الآليات التقنية والقضائية لتطبيقها.

❖ **المراجع:**

الكتب:

عبد الفتاح بيومي، "مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي دراسة متعمقة في القانون المعلوماتي"، دار شتات لنشر والبرمجيات الإسكندرية، سنة 2007

منية ترديت غمارسة، جرائم المعلوماتية، في القانون التونسي، القانون المقارن، والقانون الدولي، تونس 2015.

مصطفي السعيد مصطفي، " قانون العقوبات " القسم العام، دار النهضة العربية، 2000، ص 100.

محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، القاهرة 2004

محمود نجيب حسني، شرح قانون العقوبات القسم العام، الطبعة السادسة، دار النهضة العربية، القاهرة، مصر، 1989

المقالات:

علي كحلون، العقد الإلكتروني، م. ق. ت، ديسمبر 2001

طه بن محمد الناصر الشابي، التدليس الإلكتروني، مجلة القضاء والتشريع، أكتوبر 2005.

علي كحلون، التجارة الإلكترونية، م. ق. ت، فيفري 2000.

عز الدين الحناشي، إدارة الاثبات من النظرة التقليدية إلى التجارة الإلكترونية، م. ق. ت، عدد 1999.

عمر الطيب، الكتب الإلكتروني، م. ق. ت، أكتوبر 2001.

زهير إسكندر، التشريع التونسي والتكنلوجيا الجديدة للمعلومات، م. ق. ت، الصادرة بديسمبر 2005.

Roger Garraud, traite théorique et pratique de droit pénal français, ـ tom