مجلة جامعة طبرق للعلوم الاجتماعية والإنسانية
Tobruk University Journal of Social & Human Sciences
ISSN: 2789-5068
www.jshs.tu.edu.ly

التوقيع الرقمي وحجيته في الأثبات

إعداد

د . علي حسين كريم حسين
محاضر ورئيس قسم القانون الخاص - كلية القانون – جامعة طبرق

fwzkrymalghythy@gmail.com

الملخص:

هدفت الدراسة إلى التعرف على التوقيع الرقمي وحجيته في الإثبات وأوضحت الدراسة أن التوقيع الرقمي عبارة عن مجموعة من البيانات المرتبطة برسالة تضمن هوية الموقع وسلامة الرسالة، يهدف الكترونياً ضمان هوية المواطن لجعل المعاملات الإلكترونية سلسة وبسيطة وتم تقسيم الدراسة إلى عدد من المطالب ، وتناولت في المطلب الأول التوقيع الرقمي من حيث مفهومه وأهميته وصحته وتحدثنا في المطلب الثاني عن التوقيع الرقمي باستخدام نظام التشفير وفي المطلب الثالث حجية التوقيع الرقمي في الاثبات كما تضمن حجية التوقيع الرقمي (التصديق الإلكتروني) وعبء إثبات التوقيع الرقمي وتوصلت هذه الدراسة إلى بعض النتائج منها لا يكون المحرر الإلكتروني معداً للأثبات إلا إذا تدخل وسيط محل ثقة بإنشائه وإعداد إداه أمنة لتوقيعه وكذلك أوصت الدراسة بتعديل بعض نصوص الأثبات في القانون المدني من أجل منح الحجية القانونية للتوقيع الرقمي.

: Abstract.

The study aimed to identify the digital signature and its authenticity in proof The study showed that the digital signature is a set of data associated with a message that

guarantees the identity of the signatory and the integrity of the message, aims electronically to ensure the identity of the citizen to make electronic transactions smooth and simple The study was divided into a number of demands, and dealt with the first requirement of the digital signature in terms of its concept, importance and validity, and we talked in the second requirement about the digital signature using the encryption system and in the third requirement the authenticity of the digital signature in proof as Ensures authenticity of digital signature

مُقدّمة

تطورت العلاقات بين الأشخاص، وتعقدت المعاملات الناشئة بينهم، فكانت الحاجة ملحة إلى إثبات هوية كل طرف في أية معاملة من المعاملات التي يقومون بها، بذلك كان التوقيع هو الذي يميز هذه الأطراف على بعضها البعض بعد الترجمة الفعلية للتعبير عن إرادته.[1]

وقد مر التوقيع بمراحل عدة، فكان يتم عن طريق الختم. ومع بداية القرن السادس عشر أصبح التوقيع بخط اليد[2]، ثم توسع ليشمل بصمة الإصبع لما لها من قدرة على تحديد هوية الموقّع، نظراً لما أثبته العلم من قدرة بصمة الإصبع على تحقيق تلك الوظائف وعدم إمكانية التشابه بين البصمات حتى عند الإنسان نفسه. وفي الفترة الماضية دخلت البشرية مرحلة جديدة من التطور الفكري والمعرفي والتقني غير المسبوق حيث ظهر التوقيع الكتروني الذى غير المفاهيم الكلاسيكية للكتابة، فبدأت الدول تهتم به خصوصاً مع تزايد استخدامه يوماً بعد يوم عن طريق استخدام شبكة الإنترنت، وبذلك اختصر المسافات بين الدول والأفراد[3]، ولم يقتصر هذا التوقيع على شكلٍ واحدٍ وإنما اتخذ عدة أشكال بدءاً بالتوقيع عن طريق الرقم السري وانتهاءاً بالتوقيع الرقمي الذى أخذ حيزاً واسعاً في مجال المعاملات الكترونية ونال الاعتراف القانوني به

أهمية البحث:

مع ازدياد حجم تبادل البيانات والمعلومات الشخصية والمعاملات التجارية المهمة، أصبحت عملية حماية تلك البيانات العامة أحد أهم التحديات التي يسعى المتخصصون في هذا المجال إلى توفيرها، وتبين الدراسات وجود تزايد ملحوظ في عمليات اختراق تلك البيانات المهمة الأمر الذي أدى إلى صياغة طرق جديدة لحماية تلك المعلومات التي لا تقدر بثمن، ومن خلال تلك نشأ مفهوم التوقيع الرقمي.

أهداف البحث:

يهدف البحث إلى تسليط الضوء على التوقيع الرقمي، لما له من دورٍ كبيرٍ] في حماية البيانات والمعلومات.

إشكالية البحث:

تكمن إشكالية البحث في ما مدى الاعتراف بالتوقيع الرقمي ويمكن تقسيم تلك الاشكالات الى التالي:-

- ما مدى الحماية التقنية والقانونية والتوقيع الإلكتروني ؟
- هل حجية التوقيع الرقمي حجية كاملة ؟

منهج البحث:

والمنهج المتبع في هذا البحث المنهج الوصفي التحليلي للتوقيع الكتروني.

خطة البحث:

اشتمل البحث على ثلاث مطالب هي:-

المطلب الأول: المفهوم القانوني والفني للتوقيع الرقمي.

المطلب الثاني: التوقيع الرقمي باستخدام نظام التشفير.

المطلب الثالث: حجية التوقيع الرقمي في الإثبات.

المطلب الأول

المفهوم القانوني والفني للتوقيع الكتروني

التوقيع الرقمي عبارة عن بصمة رقمية أو علامة مميزة مرتبطة بمنظومة بيانات أخرى كل منها تنفرد بالمستند والشخص الذي وقع هذا المستند، وبذلك تكون طريقة اتصال مشفرة من أجل توثيق المعاملات التي تتم عبر الانترنت ويضمن سلامة البيانات الكترونية وتأمينها ضد أي اعتداء[4].

ويستخدم التوقيع الرقمي للتأكد من مصدر أي رسالة دون تعرضها لأي تغيير أثناء عملية النقل، ويمكن للمرسل استخدام المفتاح الخاص لتوقيع الوثيقة الكترونياً، أما فيما يتعلق بالمستقبل فيتم التحقق من صحة التوقيع عن طريق استخدام المفتاح العام المناسب لعملية التوقيع الرقمي التقليدية.[5]

وعرف المشرع الفرنسي التوقيع الرقمي وذلك بمقتضى التعديل الذي كان في(13 مارس 2000)، في المادة (4/1316)، بأنه التوقيع الذي ينتج عن أي وسيلة مقبولة موثوق بها لتحديد هوية الموقع وتكفل

اتصال التوقيع بالعمل أو المستند المرتبط به، وكذلك عرف قانون التوقيع الكتروني المصري التوقيع الرقمي في المادة (1فقرة ج)، بأنه: ما يوضع على محرر الكتروني ويتخذ شكل حروف أو أرقاماً أو رموز أو إشارات أو غيرها، ويكون له طابع منفرد يسمح بتحديد الشخص الموقع وتميزه عن غيره[6]، ويعتمد التوقيع الرقمي على فكرة أساسية مفادها تحويل رسالة المعلومات الكترونية من شكلها المعتاد كبيانات مقروءة إلى قيمة عددية لوغاريتمية، باستخدام نظام التشفير المحمل على جهاز الحاسوب بحيث لا يمكن لأحد معرفة ما تشير إليه هذه القيمة العددية من معان إلا غيرتها من صورتها الرقمية المشفرة إلى صورتها الأصلية كبيانات مقروءة وذلك باستخدام المفتاح العام[7]، فالتوقيع الكتروني اذا تحرك منفرداً أو مستقلاً عن شخص صاحبه داخل البيئة الكترونية فإنه يكون عرضة للسطو والتلاعب أكثر من التوقيع التقليدي، فإن التوقيع الرقمي يرد على دعامة مادية فإن أي تلاعب فيه يمكن كشفه بسهولة وذلك خلاف التوقيع الكتروني الذي يرد على دعائم غير مادية حيث يكون هذا التوقيع عرضة لتلاعبات لا يمكن كشفها[8]، ويعتبر التوقيع الرقمي من أهم صور التوقيع الكتروني، لما يتمتع به من قدرات فائقة على تحديد هوية أطراف العقد تحديداً ومميزات إضافية، لما يتمتع بدرجة عالية من الثقة والأمان في استخدامه وتطبيقه عند إبرام العقود[9]، ويعتمد التوقيع الرقمي على تكنولوجيا التشفير، وقد ظهر في هذا الخصوص نوعان من التشفير، أولهما: يسمى بالتشفير المتماثل، وثانيهما: بالتشفير غير المتماثل، وكلاهما آلية تتيح للمتعاقد أن يعبر عن إرادته تعبيراً آمناً من أي تلاعب أو تغيير، ويتم توثيق هذا التعبير وينسبه إلى نفسه وبالإضافة إلى ذلك يحتفظ به سراً حيث لا يطلع عليه سواه الا المتعاقد الاخر[10].

والتشفير: هو عملية تحويل البيانات الكترونية الى رموز غير معروفة أو غير مفهومة يستحيل قراءتها أو معرفتها دون إعادتها إلى هيأتها الأصلية.[11]

أما التوقيع الرقمي: فهو كل ما يختم على المحرر الرقمي ويتخذ صوره حروفاً وارقاماً وغيرها، ويكون له طابع مميز يسمح بتحرير هوية الموقع ويميزه عن غيره.

وعرفه المشرع السعودي: بأنه بيانات الكترونية مدرجة في التعامل الكتروني أو المضافة إليه أو المرتبطة به، وتستخدم لإثبات هوية الموقع وموافقته على التعامل الكتروني واكتشاف أي تزوير أو تعديل على هذا التعامل بعد التوقيع عليه[12] وعند التوقيع على مستند أو على أي معلومات أخرى يبين الموقّع بدقة.

أولاً: حدود ما يريد التوقيع عليه، وبعد ذلك تتولى دالة البعثرة في برمجيات الموقع حساب نتيجة بعثرة تنفرد بها، وتحول برمجيات الموقع نتيجة البعثرة إلى توقيع رقمي باستخدام المفتاح المخصوص للموقع، وبذلك يتم التوقيع الرقمي الناتج عن ذلك توقيعاً تنفرد به المعلومات التي يجري التوقيع عليها، والمفتاح المخصوص الذي يستخدم في إنشاء التوقيع الرقمي[13].

ويمكن القول: بأن التوقيع الرقمي هو الوسيلة المادية لتوقيع المستندات الكترونية فإن التوقيع الرقمي يثبت هوية صاحبه أو حامله في العالم الكتروني وجميع التعاملات الكترونية ويتم ذلك من خلال تشفير المختصر الحسابي الناتج من عملية دالة الاختزال للمستند الكتروني (Hash) باستخدام المفتاح الخاص، وبذلك تكمن أهمية التوقيع الرقمي في إثبات هوية الشخص وإثبات موافقته على ما تم التوقيع عليه، ويضمن سلامة المستند الكتروني من أي تعديل بعد التوقيع الكتروني[14]، إذا يمكن بواسطة التوقيع الرقمي توقيع أي ملف وإرساله بواسطة البريد الكتروني ويكون مستقبل هذا البريد متأكداً من الشخص الذي أرسل هذه الملفات وذلك للتحقق من صحة التوقيع الرقمي، ليمكن استخدام التوقيع الرقمي في العقود وفي جميع المعاملات الحكومية الكترونية، ويكون ذلك بواسطة تشفير الملف بمفتاح خاص ويرسل عن طريق البريد الكتروني[15]، ومما تقدم تظهر العلاقة بين التوقيع الرقمي والتشفير وهو ختم رقمي مشفر يملك مفتاحه صاحب الختم ويعني بذلك تطابق المفتاح مع التوقيع الرقمي على الرسالة الكترونية أن مرسل الرسالة هو من أرسلها بالفعل، وليست مرسلة من قبل شخص آخر قام بكتابة عنوانك البريدي، لتبدو وكأنها مرسلة بإسمك، ويضمن التوقيع الرقمي عدم تعرض الرسالة لأي نوع من أنواع التعديل والتزوير[16].

ويرى الباحث: أن هناك فارقاً جلياً بين التوقيع الرقمي والتوقيع التقليدي، ففي الأخير يتم عير إمضاء اليد وحركتها وبذلك يكون التوقيع التقليدي توقيع ملموس. بينما التوقيع الرقمي يتم عبر وسيط يكون بصورة أكواد وحروف ورموز وأرقام، وعلى الرغم من الاختلاف في الوسيلة إلا أنهما يجتمعان في الوظيفة والغاية، وكذلك يرى الباحث: أن هناك تشابهاً بين التوقيع الرقمي والتوقيع السري حيث يجمع هذان التوقيعان في عدم معرفة الغير بهما، أي أن السرية هي عماد هذين التوقيعين، ومن جانبي أؤيد ما ذهب إليه أغلب الفقهاء في القول بأن التوقيع الكتروني الرقمي عن طريق شفرة المفتاحين، المفتاح العام، والمفتاح الخاص، حيث يحقق أعلى درجات السرية والسلامة والأمان والثقة في المعاملات، ويضمن تحديد هوية أطراف المعاملة حيث يميزهم عن غيرهم من الأشخاص، وبذلك يضمن عدم إمكان الدخول

على مضمون التوقيع أو المحرر الكتروني الذي يرتبط به، ويمكن بواسطته كشف أي تعديل أو تحريف في بيانات المحرر الكتروني الموقع الكترونياً[17]، وبذلك فإن التوقيع الرقمي يحقق أعلى درجات الثقة والأمان، وباستخدام التوقيع يتحقق الارتباط بين المستند الكتابي والتوقيع الوارد عليه، ويضمن سرية المعلومات التي تضمنتها المحررات الكترونية، حيث لا يمكن قراءة تلك المحررات لغير من أرسلت إليه، وباستخدام المفتاح العام للمرسل[18]، ولابد من الإشارة أخيراً إلى أن التوقيع الرقمي يجب تسجيله لدى الجهات المختصة بالتوثيق، وإصدار هذا التوقيع وجهات تقديم خدمات التوثيق من أجل ضمان تحقيق الأمان والثقة في التعامل بالتوقيع، وطبقاً لذلك أشار المشرع الأردني في (المادة 30)، من قانون المعاملات الكترونية إلى عملية توثيق التوقيع الكتروني، ويشترط أن يتم بإجراءات معتمدة ومقبولة تجارياً أو يتم الاتفاق عليها بين أطراف العلاقة[19].

أهمية التوقيع الرقمي:

يساعد التوقيع الرقمي على ضمان كون الموقع نفسه من يدعي حق هذا التوقيع، وبذلك يساعد التوقيع الرقمي على تحقيق أكبر قدر من الضمان والأمان وعدم تغيير المحتوى أو العبث به من لحظة التوقيع عليه رقمياً حيث يساعد التوقيع الرقمي على إثبات مصدر محتوى الموقع عليه أمام كافة الأطراف وعدم القدرة على الإنكار[20] وبالرغم من أن الرسائل تتضمن معلومات إلا أن هذه المعلومات قد تكون صحيحة وقد تكون خاطئة، بمعنى أن التوقيع الرقمي دليل صحة المرسل وليس صحة البيانات الموجودة بالرسائل، وبذلك يعتبر التوقيع الرقمي كامل الثقة والنزاهة، وبما أن عملية التشفير تخفي تخصيص مضمون الرسالة إلا أنه لا يمكن التغيير في تلك الرسالة الموقع عليها رقمياً[21] وبذلك فإن التوقيع الرقمي يحدد الشخص الذي وقع الوثيقة ويحدد التوقيع الرقمي (الوثيقة) التي تم توقيعها بشكل لا يحتمل التغيير[22]. فالتوقيع الرقمي يدل على هوية صاحبه وينفرد به الشخص الذي يستخدمه، وأن تكون معلومات إنشاء توقيع وطريقة استعماله تحت السيطرة التامة لصاحب التقويم، بذلك لا يطرأ أي تغيير على المعاملة الكترونية منذ وضع التوقيع عليها[23].

التحقق من صحة التوقيع:

التحقق من صحة التوقيع الرقمي هو عملية تدقيق للتوقيع الرقمي وذلك بالرجوع الى الرسالة الأصلية وإلى مفتاح عمومي معين للتأكد فيما إذا كان ذلك التوقيع الرقمي قد أنشئ لتلك الرسالة ذاتها باستخدام المفتاح الخصوصي المقابل للمفتاح العمومي، ويتم التأكد من صحة التوقيع الرقمي بحساب نتيجة بعثرة

جديدة للرسالة الأصلية بواسطة دالة البعثرة التي استخدمت لإنشاء التوقيع الرقمي[24]، ومن ثم تقوم سلطة المصادقة أيضاً بتوقيع الشهادة الرقمية لتأكيد توقيتها أكثر والذي يمكن التأكد من صحته باستخدام المفتاح العام الخاص بسلطة المصادقة، والمعروف في شهادة أخرى من قبل السلطة مصادقة أخرى، ويمكن أن تكون على مستوى أعلى بالرتبة، ويمكن توثيق تلك الشهادة بواسطة المفتاح العام، وتمنع هذه الهرمية سلطات المصادقة مزيداً من الضمان والأمان والثقة، وبذلك فإن التوقيع الرقمي يفتح فرصاً عديدة في مجالات واسعة مثل تبادل البضائع، وطلب القروض، كتلك الأمور التي أصبح من الممكن ممارستها عبر الشبكة، وأصبح إجراء الصفقات التجارية أسرع وأسهل وأكثر أماناً وأقل تكلفة[25] ويعاقب بالحبس مدة لا تقل عن سنة وغرامة لا تقل عن ألف دينار ولا تزيد عن عشرة آلاف، كل من قام بتقليد عمل رقمي أو أدبي أو فني أو علمي أو أقام بقرصنة البرمجيات، علماً بأن نسخ البرمجيات يعد من أفعال التقليد [26] وبذلك يستلزم التوقيع الرقمي إيجاد جهة متخصصة ومحايدة يمكن عن طريقها التحقق من صحة التوقيع وذلك عن طريق الكاتب العدل الكتروني والذي شرعت الكثير من الدول في تنظيمه فيقوم هذا الكاتب الكتروني بإصدار شهادات رقمية تسمح بتوفير الثقة في جميع السندات الكترونية [27].

مزايا وعيوب التوقيع الرقمي:

1. التأكد من موثوقية المرسل بفضل وجود زوج من المفاتيح، عام وخاص حيث لا يمكن تزوير التوقيع الرقمي إلا في حال نسخ المفتاح الخاص للمرسل[28].
2. يسمح التوقيع الرقمي، نظراً لصعوبة اختراقه ودلالته على شخص صاحبه بإبرام الصفقات عن بعد عبر الوسائط الكترونية الأمر الذي يعمل على تطور التجارة عبر الدعامات الكترونية [29].
3. التوقيع الرقمي وسيلة مأمونة لتحديد هوية الشخص الذي قام بالتوقيع وذلك بعد اتباع إجراءات معينة يمكن التأكد للحاسب الآلي أن من قام بالتوقيع هو صاحب بطاقه السحب نفسه [30].
4. يؤدي التوقيع الرقمي إلى إقرار المعلومات التي تضمنها والمستند الكتروني، وخير مثال على ذلك بطاقات الائتمان البنكية حيث يحصل العميل على المبلغ المطلوب دون اللجوء إلى السحب اليدوي مما ينطوي عليه من إجراءات[31] ورغم مزايا التوقيع الرقمي إلا أنه لا يخلو من السلبيات التي تؤخذ عليه من سلبيات الرقم الكودي أو السري وذلك باحتمالية تعرضه للسرقة أو الضياع، لكن ذلك مردود عليه بأن التوقيع التقليدي عرضه للتزوير والتقليد[32] وذهب بعض الفقهاء في إطار الحديث عن سلبيات التوقيع إلى أن هذا التوقيع إذ ينشأ عن طريق الحاسب الآلي فإنه قد لا يكون معبراً عن هوية صاحبه وهذا الراي

من وجهة نظري تعوزه الدقة، وذلك أن التوقيع الرقمي يعتمد على شفرة معقدة لا يعرف مفتاحها إلا صاحب التوقيع، فإنه من المفترض أنه مجرد استعمال هذا التوقيع إنما يدل دلالة قاطعة على أن المستخدم هو صاحب التوقيع نفسه[33].

المطلب الثاني

التوقيع الرقمي باستخدام نظام التشفير

التشفير: هو أسلوب قديم استخدمه البشر منذ القدم وأول مجهود بشري للتشفير سجله التاريخ حدث قبل (4000 سنة)، فقد استخدم في الحضارات القديمة، لإخفاء المعلومات والمراسلات، مثل: الحضارة الفرعونية، والدولة الرومانية، ولكن التشفير كعلم مؤسس منظم يدين بولادته ونشأته للعلماء الرياضيين واللغويين العرب إبان العصر الذهبي للحضارة الإسلامية، ومن أشهرهم الفراهيدي والكندي. وقد ألف هؤلاء العلماء مفاهيم رياضية متقدمة، من أهمها، التوافيق والتباديل[34]، وبذلك فان نظام التشفير لا يعد حديث العهد بل كان موجوداً منذ العصور القديمة غير أن انتشار تقنيات التشفير بدأت تفرض نفسها بوصفها وسيلة لا غنى عنها في توفير أمن وسرية وسلامة السندات الكترونية فضلاً عن أن تقنيات التشفير تهدف الى التحقق من هوية الشخص الذي صدرت منه السندات والتأكد من إثبات صحتها وعدم تزويرها والتلاعب بها اثناء مرورها في وسائل الاتصالات[35] ، وبدأ استخدام التوقيع باستخدام نظام التشفير في المعاملات المصرفية حيث نجد البطاقات التي تحتوي على رقم سري يستطيع حاملها القيام بكافة العمليات المصرفية من خلال جهاز الصراف الالي، ثم تطور الامر الى استخدام هذا التوقيع كأسلوب موثق به في الرسائل المتبادلة رقمياً[36]، ويعتبر التوقيع في استخدام التشفير من أهم صور التوقيع الرقمي، وهو عبارة عن بيانات أو معلومات متصلة بمنظومة بيانات أخرى أو صياغة منظومة في صوره مشفرة، وبذلك يتم تحويل المحرر المكتوب باستخدام العمليات الحسابية من أسلوب كتابه عادية الى معادلة رياضية وتحويل التوقيع إلى أرقام، ولا يمكن لأحد أن يعيدها الى صيغتها المقروءة الا الشخص الذي لديه المعادلة الخاصة بها [37]، ويمكن تحديد مفهوم التشفير على أنه: عملية تحويل معلومات وبيانات عادية الى معلومات مشفرة غير مفهومة وذلك بغرض منع الأشخاص غير المصرح لهم من الاطلاع على المعلومات وفهم محتوى تلك الرسالة، وتتم عملية التشفير وفك الشفرة من خلال طريقة حسابية معقدة تستند الى صيغة رياضية تسمى خوارزميات [38].

وينقسم التوقيع باستخدام التشفير إلى نوعين:

أولاً: **التشفير المتماثل** وهو الذي يقوم على فكرة مفتاح واحد متبادل بين الطرفين يستخدم من المرسل، والهدف منه تشفير الرسالة، ويستعمل من المرسل إليه، ويقصد منه استعادة الرسالة في شكلها الواضح ويعمل في بيئة منعزلة، نظراً للمخاطر التي تحيط بعملية توزيع هذا المفتاح بين الطرفين وإمكانية تلقيه من الغير[39]، ويسمى أيضاً بالنظام السيمتري، وطريقة تشغيل النظام تعتمد على مفتاح موحد لإغلاق بيانات المحرر الكتروني وفتحها، ومفتاح الإغلاق والفتح عبارة عن معادلة رياضية يمثلها نظام معين تعمل على تحويل البيانات إلى نص رقمي ذو رموز غير مقروءة، ومن أكثر الأنظمة استخداماً. وآلية عمل (DES) ونظام (RC4) وآلية عمل هذين النظامين قائمة على تغيير تسلسل الأحرف[40]، وبعد أن يتم استقبال الرسالة يستخدم المستقبل نفس عبارة المرور، وذلك لفك النص المشفر حيث تقوم برمجيات التشفير مرة اخرى بترجمة عبارة المرور، وتشبك المفتاح الثنائي الذي يتولى إعادة النص المشفر إلى شكله الأصلي [41] وتكمن مساوئ هذا النوع من التشفير في ان المرسل إليه السند الكتروني الذي يأتيه من مصادر مختلفة يجب عليه امتلاك عدد من المفاتيح الخصوصية توازي عدد السندات الواردة من هذه المصادر، فضلاً عن ذلك أن استعمال المفتاح ذاته من قبل شخصين مختلفين قد يعرض السندات الكترونية الى الخطر الدائم في إمكانية انتقال المفتاح الخصوصي إلى الغير بشكل غير مشروع حينئذ يكون من الصعوبة تحديد حصول هذا الانتقال لا سيما إذا كان من منشئ السند الكتروني والمرسل إليه حائزين على المفتاح ذاته[42]

(**هذا الرسم يوضح عملية التشفير المتماثل**)

ثانياً: التشفير غير المتماثل يتم التوقيع في هذه الحالة باستخدام نوعين من مفاتيح التشفير، وهما: مفتاح خاص، حيث يستخدم التشفير رسالة البيانات، ويكون سراً لصاحبه بحيث لا يستطيع للغير العلم به. ومفتاح عام، يتم من خلاله فك شفرة الرسالة بحيث يمكن قراءتها ولكن لا يسمح المفتاح العام بالتعديل في محتوى الرسالة حيث أن عملية التعديل تتم من خلال المفتاح العام فقط[43]، ويتجنب هذا النوع من التشفير التبادل غير الآمن لمفتاح التشفير حيث يستخدم في التشفير غير المتماثل مفتاحان، أحدهما: خاص، والآخر عام. يتكون المفتاح الخاص من مجموعة من الرموز والأرقام التي يمكن تخزينها على بطاقه رقمية يتم الوصول إليها عن طريق الرقم الشخصي لصاحبه، وبذلك يكون هذا المفتاح معرفاً على طرف واحد فقط وهو المرسل[44] ومفتاح عام يتم من خلاله فك شفرة الرسالة بحيث يمكن قراءتها، ولكن لا يسمح المفتاح العام للتعديل في محتوى الرسالة حيث أن عملية التعديل تتم فقط من خلال المفتاح الخاص[45] وقد اخترع هذا النظام في الولايات المتحدة الأمريكية (عام 1976)، على أثر أبحاث قام بها كل من (Diffe - Hellman)، وقد لاقي هذا الاختراع ترحيباً واسعاً لفعاليته في توفير أمن وسرية بيانات المحرر الإلكتروني على شبكة التواصل الاجتماعي الحديثة (الانترنت) وطريقة تشغيل هذا النظام واقعية سهلة إلا أنها تحتاج إلى خبرة، ومهارة من الشخص القائم بالتشغيل وبذلك بحفظ ذاكره الحاسب الآلي حيث تجري عملية الإغلاق والفتح آلياً بعد تزويده ببيانات معينة. [46]

(**هذا الرسم يوضح عملية التشفير الغير التماثل**)

وغالباً ما يستخدم التشفير غير المتماثل في إبرام العقود الإلكترونية، لاعتماد المفتاحين، فالمفتاح العام يسمح لكل شخص مهتم في القيام بقراءة رسالة البيانات عبر الإنترنت ولكن دون أن يتمكن من إدخال أي تعديل عليه، ومفتاح خاص يمكن لصاحبه من وضع توقيعه على رسالة البيانات ثم يقوم

بإعادتها إلى مصدرها مرفقاً بها توقيعيه في ملف بحيث لا يمكن لمصدرها إجراء أي تعديل عليها[47] حيث أن عملية التعديل تتم من خلال المفتاح الخاص فقط [48] وعلى ذلك يكون المرسل إليه على علم بالمفتاح العام فقط وبمقتضى القانون الصادر في فرنسا عام (1990)، فقد سمح للمشروعات الصغيرة باستخدام التشفير بعد أن كان قاصراً على المجالات العسكرية والدبلوماسية والحكومية، كما خفض القانون الصادر في 26 يوليو من بعض القيود المتعلقة بالتشفير، كذلك القرار (98–101)، الصادر في(24–2–1998م)، قد وضع الضوابط المتعلقة باستخدامه [49] حيث أن المشرع المصري لم يتعرف بمقتضى القانون (رقم 15 لسنه 2004)، الخاص بتنظيم التوقيع الإلكتروني ولكنه نص على أن كل وسيلة الكترونية أياً كان شكلها أو طبيعية بحيث تكون توقيعاً الكترونياً طالما أن هذا الوسيلة تتسم بالطابع المنفرد الذي يسمح بتحديد هوية الشخص الموقع وتميزه عن غيره، وبذلك فإن المشرع المصري بإقراره لنظام التشفير يعد ذلك اعترافاً غير مباشر منه بالتوقيع الرقمي [50]، ويقوم التوقيع الرقمي أساساً على التشفير، وتعتبر المعاملات البنكية وكذلك التعاقد عبر شبكة الانترنت من أهم المعاملات التي يستخدم فيها التوقيع الرقمي، وفيما يتعلق بالمعاملات البنكية يمكن للعميل عن طريق البطاقة البنكية وهي أحد اشكال التوقيع الرقمي أن يقوم بكل العمليات البنكية كالاستعلام عن حساب أو صرف جزء من رصيده وذلك بإدخال الرقم السري الخاص والذي يعتبر بمثابة التوقيع الإلكتروني الرقمي، ولهذه البطاقات أنواع عديدة أشهرها بطاقات السحب الآلي وبطاقات الوفاء والائتمان والشيكات،[51] فالإجراءات التي يقوم بها حامل البطاقة من إدخال البطاقة في الجهاز وما يليها من إجراءات الرقم السري وأيضاً تحديد المبلغ، جميعها تمثل المحور الإلكتروني المطلوب والمقيد والمحفوظ في الأشرطة والاسطوانات الممغنطة في ذاكرة الحاسوب لدى المصرف والتي يمكن الرجوع إليها متى ما تطلب الأمر، وبذلك يتم تحديد جميع الأوامر التي طلبها العميل بما في ذلك دخول البطاقة في الجهاز وتعزيز ذلك برقم سري،[52] وبالرغم من أن هناك مزايا عملية وقانونية يمنحها نظام تقنية التشفير غير المتماثل بالمفتاح العمومي إذ أن كل مستخدم لشبكة الانترنت لا يستخدم سوى مفتاح أو رمز سري واحد في تشفير السندات التي يرغب بإرسالها أو التي يرغب في فك تشفيرها إلا أن هناك صعوبات تواجه هذا النوع من التشفير تكمن في مدى ضمان المفتاح العمومي واستخدامه من قبل الحائز على المفتاح الخاص[53]، وهنا يستلزم الأمر وجود شخص أو جهة محايدة موثوق بها تقوم بدور الوسيط في تسليم المفتاح العام من المرسل الى المرسل إليه

كما تقوم بإصدار شهادات رقمية تحدد هوية المتعاملين وصحة المعاملات التي تضمنتها هذه الرسالة وتلك الجهة هي الكاتب العدل الإلكتروني[54].

المطلب الثالث

حجية التوقيع الرقمي في الإثبات

اعتمدت التسريحات الجديدة مؤخراً من قبل الدول الأعضاء في الاتحاد الأوروبي ضمن ما يسمى: قاعدة المسائل التشريعية المتعلقة بالتجارة الإلكترونية فقد أقرت التوقيع الرقمي وأكدت على أهميته ومنحه قيمة قانونية مساوية للإمضاء أو التوقيع الخطي، فقد أصدرت اللجنة الأوروبية المهتمة والمعنية بالإشراف على تقنين هذا المشروع وعرض توجيهات تتعلق بالإطار المشترك للتوقيع الرقمي [55]هدفه ما يلي:

1. منع الدول الأعضاء من رفض منح التوقيع الرقمي مفعولاً قانونياً لمجرد تنفيذه إلكترونياً.
2. ضمان حرية سير خدمات التصديق والمصادقات في قلب الاتحاد الأوروبي، وبموجب ذلك تمنح المصادقات الصفة القانونية اللازمة إذا تضمنت البيانات هوية مورد خدمة التصديق اسم حامل اللقب وصلاحياته النوعية، توقيع نظام التحقيق مدة الصلاحية، التوقيع الرقمي لمقدم خدمة المصادقة، الكود الذي يحدد هوية المصادقة.[56]

أولا: حجية التوقيع الرقمي(التصديق الإلكتروني)

التوقيع الرقمي: هو الصورة العملية للتوقيع الإلكتروني المتقدم أو المحمي وذلك في التشريعات التي ميزت بين التوقيع الإلكتروني المتقدم والبسيط، وهناك بعض التشريعات التي وضعت شروطاً معينة للاعتداد بالتوقيع توافرت فقط في التوقيع الرقمي، وبذلك نال التوقيع الإلكتروني المتقدم في جميع التشريعات حجية في الإثبات مماثلة لتلك التي تقررت للتوقيعات الخطية التقليدية في قوانين الإثبات[57]، وذلك بعد استيفاء شروط معينة، كما أصدرت العديد من الدول التي تعترف بحجية التوقيع الإلكتروني وتساوي بينه وبين التوقيع اليدوي طالما توافرت الشروط الخاصة بتوثيق هذا التوقيع، من هذه الدول: ألمانيا، حيث أصدرت القانون الفدرالي (في 13 – 6 – 1997م)،[58] ليطبق في أول أغسطس (سنة 1997م)، بتنظيم التوقيع الرقمي، وكذلك إيطالية التي أصدرت التشريعين: تشريع التوقيع في (15 – 3 – 1997م)، والنشر بشأن شهادة التوثيق في (15– 3– 1999م)، وفي إسبانيا هناك قانون(59/ 2003) بشأن التوقيع الذي يحدد ثلاثة أنواع من العلامات .

أولاً : بساطة البيانات التي يمكن أن تستخدم لتحديد الموقع أصالة.

ثانياً: وثيقة تضمن سلامة ونزاهة ذلك باستخدام (DSCF) أمن جهاز إنشاء التوقيع.

ثالثا: معترف بها (شهاده تمنح بعد التحقق من هوية الموقع والتوقيع)[59] وقد حرص المشرع الليبي على إخفاء الحجية على المستندات الرقمية في الإثبات وذلك في نص المادة(97/ 2) من قانون المصارف رقم واحد لسنة (2005)، على أنه يُعتد بالمستندات والتوقيعات الإلكترونية التي تتم في إطار المعاملات المصرفية وما يتصل بها من مُعاملات أخرى، وتكون بها الحجية في إثبات ما تضمنه من بيانات،[60] وقد تبين لنا أن التوقيع الإلكتروني يقوم على استخدام تكنولوجيا الحاسب الآلي والإنترنت وغيرهما من وسائل الاتصال الحديثة، لذا فهو يتخذ شكل بيانات إلكترونية تنفذ عن طريق مجموعه من الإجراءات والخطوات التكنولوجية، وبذلك يتخذ التوقيع عدة أشكال وصور، وقد يمثل هذا التوقيع رمزاً أو رقماً أو حرفاً، وفي النهاية تعتمد على تكنولوجيا التشفير والتكوين والتقويم وغيرها، فإن هذا التوقيع لا ينتج أي حجية قانونية إلا بعد التوثيق[61] فالقانون المصري نص على أن التوقيع الإلكتروني في نطاق المعاملات المدنية والتجارية والإدارية له ذات الحجية المقررة لتوقيع في أحكام قانون إثبات في المواد المدنية والتجارية[62]، متى استوفت الشروط المنصوص عليها في هنا القانون وفقا للضوابط الفنية والتقنية[63] التي تحددها اللائحة التنفيذية لهذا القانون، ويرى بعض الفقهاء أن حجية التوقيع الإلكتروني يتفق مع مبادئ الإثبات في الشريعة الإسلامية، فجميع وسائل الإثبات في الشريعة الإسلامية هدفها إظهار الحق وتحقيق العدل بين الأطراف، وبالتالي يجوز اللجوء لأية وسيلة مشروعة تثبت الحق سواء أكانت تقليدية أم حديثة إلكترونية وكذلك الإثبات في الشريعة الإسلامية لا يشترط الكتابة على ورق او استخدام مواد معينه بل يجوز الكتابة على الحجر والعظام والشجر، ويجوز الكتابة على أي دعائم عادية أو الكترونياً وبالتالي يقبل الفقه الإسلامي الإثبات بالفاكس أو التليكس،[64] فآلية التوقيع الرقمي التي تعتمد على تقنيات التشفير ووجود طرف ثالث معتمد موثوق فيه ومحايد يتولى إصدار شهادات التصديق الإلكتروني التي تكشف عن صحة التوقيع الرقمي من عدمه وبذلك تجعله في كل مرحلة من مراحله يزداد موثوقية ويحقق أعلى مستويات الأمان الأمر الذي جعل المشرعين يمنحونه ليس فقط حجية مساوية لحجية التوقيع الخطي المقررة في الإثبات، وإنما قرينة قانونية على صحته وسلامته،[65] في الصورة المنسوخة على الورق الإلكتروني الأصلي، تعد حجية على الجميع بالقدر الذي تكون فيه مطابقة لأصل هذا المحرر وذلك ما دام المحرر الإلكتروني الأصلي التوقيع الإلكتروني موجودين على الدعامة الإلكترونية وهي وسيلة مادية

تستخدم لتخزين وتداول المعلومات والبيانات الإلكترونية [66]، وبذلك فإن القانون قد جعل قرينة مفادها أن التوقيع الإلكتروني متى استوفى شروطاً معينة أمكن الاعتداد بهذا التوقيع الإلكتروني وفي القانون الأردني للمعاملات الإلكترونية إذ تبين أن إجراءات التوثيق المستخدمة معتمدة ومقبولة تجارياً أو اتفق عليها بين الأطراف، فيعتبر التوقيع الإلكتروني موثقاً إذا تضمن التالي:

- يتميز بشكل فريد لارتباطه بالشخص صاحب العلاقة.
- يعتبر كافٍ للتعريف بصاحبه.
- تم إنشاؤه بوسائل خاصة بالشحن وتحت سيطرته.

ارتباطه بالسجل الذي يتعلق به بصورة لا تسمح بإجراء أي تعديل على القيد بعد توقيعه،[67] ويكون السجل الإلكتروني والرسائل الإلكترونية لآثار القانونية نفسها المعترف بها للأوراق العرفية مع مراعاة ما يلي:

- الطريقة التي تم بها إنشاء أو حفظ السجل أو العقد أو الرسالة الإلكترونية.
- الطريقة التي تم بها التوقيع.
- الطريقة التي استعملت للمحافظة على سلامة المعلومات التي تضمنها العقد أو الرسالة والسجل.
- الطريقة التي حددت من خلالها هوية المنشئ وبذلك فإن هناك التزامات على جهات التوثيق الإلكتروني وهي التوقيع الإلكتروني الرقمي حيث يتم بواسطة برنامج كمبيوتر خاص لهذه الغاية أو باستعماله فإن الشخص يكون قد وقع على إرساله تماماً كما يوقع يدويا في عالم الأوراق والوثائق الورقية. [68]

إن التوقيع الرقمي مرتبط جوهرياً بالتشفير بحيث لا يكون قادراً على قراءتها إلا الشخص المستقبل وحده[69] ويكون مقدم خدمات التوثيق مسؤولاً عن الضمانات الآتية:

- صحة المعلومات المصادقة التي تضمنتها الشهادة في تاريخ تسليمها.
- العلاقة بين صاحب الشهادة ومنظومة التدقيق في التوقيع الخاص به.
- استقلال صاحب الشهادة بمسك منظومة إنشاء توقيع مطابقاً للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية للقانون على أن تكون متكاملة مع منظومة التدقيق لمعرفة الشهادة في وقت تسليمها،[70] وهنا بعض الواجبات التي تقع على عاتق الموقع، وهي: ممارسة عناية معقولة لتفادي استخدام أداة

توقيعية استخداماً من غير مأذون وأن يخطر الأشخاص المعنيين بدون تأخير غير مبرر، وأن يمارس عناية معقولة لضمان واكتمال كل ما يقدمه من بيانات دقيقة وما يقدمه من بيانات وتصريحات جوهرية ذات صلة بالشهادة طيلة فترة سريانها وذلك في الحالات التي تستلزم فيها أداة التوقيع استخدام شهادة.[71]

إذن التوقيع في التوثيق الإلكتروني أصبح الآن حقيقة لا يستقيم معنى المحرر الإلكتروني الا بها، ومن أوضح التشريعات العربية تجسيداً لهذه الحقيقة قانون المعاملات الإلكترونية الأردنية في مادة (32/ ب) التي نفت أي قيمة قانونية للمحرر الإلكتروني بعنصريه إذا لم يكن موثقاً [72].

كذلك في حالة عدم توثيق السجل الإلكتروني أو التوقيع الإلكتروني فلا يعتد بهما ولا يترتب على أي منهما أي حجية في القانون[73]، هناك حكم صادر من محكمة النقض الفرنسية بتاريخ (30- 9- 2010م)، حيث نقضت فيه الحكم الصادر من محكمة الاستئناف (ديجون) الذي اعترفت بالرسالة الإلكترونية بحجيتها كدليل كامل في الإثبات حيث قررت أي محكمة النقض في تعقيبها على هذا الحكم أن التوقيع ضروري في نسبة تصرف القانون إلى من يحتج عليه، فضلاً عن أنه يكشف عن رضا الطرفين بالالتزامات التي تنتج عن هذا التصرف، ثم اردفت نفس المحكمة موضحة متطلبات التوقيع الإلكتروني فقالت: إن التوقيع في الشكل الإلكتروني هو عبارة عن استعمال اجراء دقيق وموثوق به في تحديد هوية صاحبه من خلال ضمان ارتباط التوقيع بالتصرف الذي يرتبط به ارتباطاً لا ينفك، وصحة هذا الاجراء ودقته والثقة فيه هي عملية مفترضة افتراضاً يقبل إثبات العكس إذا كان التوقيع الإلكتروني دالاً على شخصية الموقع ومرتبة لسلامة التصرف الذي يرتبط به وناشئاً في ظل الشروط والضوابط الفنية المنصوص عليها في المرسوم الصادر عن مجلس الدولة[74] .

ثانياً: عبء إثبات حجية التوقيع الرقمي.

كما هو معروف فإن التوقيع يعتبر عنصر جوهري للإثبات، وهو الحجة القانونية للورقة المكتوبة وبها إلزامية القاضي، ولكن التوقيع الرقمي يختلف كلياً عن التوقيع التقليدي، ولذلك يجب تأمين البيانات والمحافظة عليها وعلى سريتها وخصوصيتها والحفاظ على خصوصية صاحب البيانات، وبدون هذه الضمانات لا يمكن المحافظة على الإنجازات في العالم الرقمي،[75] وبالرجوع إلى المشروع اللبناني الجديد المعدل لقانون أصول المحاكمات المدنية المتعلق بالإثبات يعتبر السند الإلكتروني مقبولاً في الإثبات بالمقدار نفسه لقبول الكتابة القائمة على سند ورقي ما دام يتوافر فيه شرطان وهما:

- إمكانية تحديد هوية الشخص الذي أصدره.

▪ كون السند قد نظم وحفظ وفق شروط من شأنها ضمان محتواه ومصداقيته[76]. وتعد القرينة القانونية إعفاء استثنائي من عبء الإثبات الذي تقضي به القواعد العامة للإثبات التي من خلالها يفترض أن يكون المشرع أمراً معيناً يترتب عليه نقل عبء الإثبات من طرف إلى آخر[77] وهنا يجب أن نفرق بين أمرين، أولهما: حالة كون التوقيع الإلكتروني صادر من مقدم الخدمة، وثانيهما: كون التوقيع الإلكتروني صادر من طرف ثالث وهو الموثق، فالأخير هو توقيع الإلكتروني ذو حجية كاملة، وبالتالي يقع على المتضرر منه عبء إثبات اعتماد التوقيع على شهادة إلكترونية لم تستوف الشروط القانونية المطلوبة. أما التوقيع الإلكتروني الصادر من مقدم الخدمة فإن عبء الإثبات يقع على عاتق مقدم خدمات التصديق الإلكتروني[78] وكذلك يتمتع المحرر الورقي الإلكتروني المصحوب بتوقيع الكتروني مؤمن بقرينة قانونية مفادها صحة التوقيع وسلامة البيانات المدونة به، ويترتب عليه إعفاء من يتمسك بالمحرر من عبء إثبات صحته وسلامته المادية، أما المحرر الرسمي فهو حجة في ذاته لوجود قرينة صحة التوقيع، وفي حالة حدوث نزاع في صحة هذا المحرر فليس على من يتمسك به إقامة الدليل على صحته وبذلك يقع عبء نقضه على الخصم الذي ينازع فيه، ولا يمكن تحقيق ذلك إلا من خلال الطعن بالتزوير[79]،ويجب على مقدم خدمات التصديق، ومدير المواقع الإلكترونية استعمال وسائل موثوق بها، لإصدار وتسليم وحفظ الشهادات، واتخاذ الوسائل اللازمة لحمايتها من التزوير[80]، وأن عبء إثبات حجية التوقع الرقمي مرهون بالسياسة التشريعية التي يتبناها المشرعون، فإذا كان المشرع قد اتجه إلى تخفيف عبء الاثبات على من يحتج بالتوقيع الرقمي لاعتبارات معينة نعتقد أن من أهمها: تعدد عناصر التأمين والأمان في التوقيع الرقمي بإقرار قرينة قانونية بسيطة مفترضاً فيها صحة التوقيع الإلكتروني المتقدم وبذلك فإن عبء الإثبات عدم صحة التوقيع الإلكتروني المتقدم ودحض حجيته يكون مرتبطاً بقدرة المدعى عليه وليس المدعي المتمسك بالتوقيع، على إثبات ذلك الأمر[81].

الخاتمة

الحمد الله الذي بنعمته تمم الصالحات حمداً كثيراً طيباً مباركاً فيه، لإتمام هذه الدراسة التي تناولناها تحت عنوان: التوقيع الرقمي وحجيته في الاثبات والذي يعد من أبرز الموضوعات القانونية حيث يعتبر التوقيع الرقمي من أبرز صور التوقيعات، وقد هدفت الدراسة إلى تسليط الضوء على التوقيع الرقمي، لما له من أهمية كبيرة ففي المطلب الأول تعرضت الدراسة: للمفهوم الفني والقانوني للتوقيع الرقمي. كما

تحدثت عن أهمية التوقيع الرقمي ومزاياه والمطلب الثاني: تعرضنا من خلاله لنظام التشفير وبذلك يعتبر التوقيع الرقمي من أكثر التوقيعات استخداما، كما تطرقنا في المطلب الثالث إلى حجية التوقيع الرقمي في الإثبات باعتباره يحقق أعلى مستويات الأمان والثقة، الأمر الذي جعل له حجية مساوية لحجية بعض التوقيعات التي لها دور كبير في الإثبات.

نتائج البحث:

1. أن المحرر الإلكتروني المعد للأثبات لا يكون له أثر قانوني ألا إذا كان محفوظ.
2. لا يكون المحرر الإلكتروني معداً للإثبات إلا إذا تدخل وسيط محل ثقة بإنشائه وإعداد كأداة آمنة لتوقيعه.
3. يتمتع التوقيع بحجية قانونية تساوي ما للكتابة التقليدية والسندات التقليدية والتواقيع التقليدية من قوة الاثبات متى كانت مستوفية للشروط القانونية الخاصة بها.
4. دلة الكتابة الورقية كأداة من أجل إبرام العقد أو حجيته.

توصيات:

1. نوصي مقدمي خدمات التصديق بالاهتمام التشريعي وتوفير القدرات الفنية والتكنولوجية والمالية التي يتطلبها مجال عملهم.
2. تعديل بعض نصوص الإثبات في القانون المدني من أجل منح الحجية القانونية للتوقيع الرقمي.
3. عقد ندوات ودورات تدريبية من أجل إعداد كوادر قضائية تمتلك وعياً معلوماتياً لمواكبة المتغيرات والمستجدات على القواعد القانونية.

الهوامش:

1. د. أيمن علي حسين الحوثي، التوقيع الالكتروني بين النظرية والتطبيق، دار الفكر الجامعية الاسكندرية– 2011 ، ص1.
2. د. أحمد عبدالكريم موسى– حجية التوقيع الإلكتروني في الإثبات دراسة في التشريع العماني– مجلة البحوث القانونية والاقتصادية والشرعية– جامعة المنصورة– العدد 65– المجلد الأول– أبريل 2010، ص237.
3. د. ثروت عبدالحميد، التوقيع الإلكتروني، ماهية مخاطرة وكيفية مواجهتها في الإثبات، دار الجامعة الجديدة 2007، ص16.
4. د. صفاء فتوح جمعة– الإطار القانوني والفني للتحول الرقمي في المنظمات الحكومية– دار الفكر والقانون للنشر والتوزيع، جامعة المنصورة، 2022، ص284.

5. د. يوسف حسن يوسف، التجارة الإلكترونية وأبعادها القانونية الدولية، الطبعة الأولى، المركز القومي للصادرات القانونية، 2011، ص214.
6. الصالحين محمد العيش، الكتابة الرقمية طريق للتعبير عن الإرادة ودليلاً للإثبات، الطبعة الأولى، منشأة المعارف الاسكندرية 2008، ص174.
7. محمد عامر كريم، إثبات العقد المبرم عن طريق الانترنت، رسالة ماجستير، جامعة الاسكندرية، 2015، ص110.
8. نور خالد عبدالمحسن– حجية المحررات والتوقيع الإلكتروني في الإثبات عبر شبكة الإنترنت– رسالة ماجستير، جامعة عين شمس، ص76.
9. أيمن علي حسين الحوثي، التوقيع الإلكتروني بين النظرية والتطبيق، مرجع سابق، ص45.
10. د. مصطفي أبو مندور موسى– مفهوم المحرر الإلكتروني المعد للإثبات– مجلة الحوث القانونية والاقتصادية والشرعية، دار الفكر العربي، جامعة المنصورة، العدد (60) المجلد الثاني، أغسطس 2016، ص752.
11. الفقرة(5) من المادة الأولى من القانون الليبي رقم (5) لسنة 2022، بشأن مكافحة الجرائم الإلكترونية، ص3.
12. د. قدري عبدالفتاح الشهادي، قانون التوقيع الإلكتروني ولائحته التنفيذية والتجارة الإلكترونية في التشريع المصري– دار النهضة العربية، القاهرة 2008، ص491.
13. قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية الامم المتحدة نيويورك 2002ص39.
14. د. فرحان نزال، د. سامر خليل – التوقيع الرقمي وحجيته في الإثبات في قانون المعاملات الإماراتي والأسباني– مجلة البحوث القانونية والاقتصادية والشرعية، دار الفكر العربي، جامعة المنصورة، العدد(67) الجزء الأول (المجلد الثاني) ديسمبر 2018، ص567.
15. أمير فرج يوسف – الجديد في التوقيع الإلكتروني، الطبعة الأولى، مكتبة الوفاء القانونية، الاسكندرية 2011، ص83.
16. أمير فرج يوسف – التوقيع الإلكتروني– دار المطبوعات الجامعية، 2008، ص70.
17. د. ممدوح محمد مبروك – مدى حجية التوقيع الإلكتروني في الإثبات، دراسة مقارنة بالفقه الإسلامي، دار النهضة العربية، القاهرة، 2008، ص20.
18. خالد ممدوح إبراهيم– التوقيع الإلكتروني – الدار الجامعية 2010، ص92.
19. يوسف أحمد النوافله – الإثبات الإلكتروني– رسالة ماجستير، جامعة الاسكندرية، سنة 2020، ص62.
20. أمير فرج يوسف – الجديد في التوقيع الإلكتروني، مرجع سابق، ص94.
21. أيمن على حسين الحوثي، التوقيع الإلكتروني بين النظرية والتطبيق، مرجع سابق، ص74.
22. د. يوسف حسن يوسف، التجارة الإلكترونية وأبعادها القانونية الدولية، مرجع سابق، ص89.
23. المادة (10) من القانون الليبي رقم (6) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، العدد رقم (1)، ص28.
24. أمير فرج يوسف – التوقيع الإلكتروني–مرجع سابق، ص 62.
25. د. صفاء فتوح– الإطار القانوني والفني للتحول الرقمي في المنظمات الحكومية، مرجع سابق، ص500.
26. المادة (25) من القانون الليبي رقم (5) لسنة 2022 بشأن مكافحة المعاملات الإلكترونية، العدد رقم (1) ص 12.
27. د. عباس العبودي–تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجارها– منشورات الحلبي الحقوقية، ص234.
28. صفاء فتوح– الإطار القانوني والفني للتحول الرقمي في المنظمات الحكومية، مرجع سابق، ص499.
29. نور خالد عبدالمحسن– حجية المحررات والتوقيع، مرجع سابق، ص86.

30. عبد الفتاح بيومي حجازي– التوقيع الإلكتروني في النظم القانونية المقارنة– الطبعة الأولى، دار الفكر الجامعي، 2005، ص27.
31. نور خالد عبدالمحسن– حجية المحررات والتوقيع، مرجع سابق، ص86.
32. عبد الفتاح بيومي حجازي– التوقيع الإلكتروني في النظم القانونية المقارنة– مرجع سابق، ص28.
33. صفاء فتوح– الإطار القانوني والفني للتحول الرقمي في المنظمات الحكومية، مرجع سابق، ص500.
34. خالد ممدوح إبراهيم– التوقيع الإلكتروني – الدار الجامعية 2010، ص149.
35. د. عباس العبودي–تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجارها– مرجع سابق، ص230.
36. الصالحين محمد العيش، الكتابة الرقمية، مرجع سابق، ص177.
37. د. ثروت عبدالحميد– التوقيع الإلكتروني ومدى حجته في الإثبات– البعة الثانية، مكتبة الجلاء، 2003، ص50.
38. د. خالد ممدوح – التوقيع الإلكتروني– مرجع سابق، ص151.
39. أيمن على حسين الحوثي، التوقيع الإلكتروني بين النظرية والتطبيق، مرجع سابق، ص45.
40. عيسى غسان– القواعد الخاصة بالتوقيع الإلكتروني، مرجع سابق ص67.
41. الصالحين محمد العيش، الكتابة الرقمية، مرجع سابق، ص178.
42. د. عباس العبودي–تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجارها، مرجع سابق، ص232.
43. محمد عامر كريم، إثبات العقد المبرم عن طريق الإنترنت، مرجع سابق، ص111.
44. الصالحين محمد العيش، الكتابة الرقمية، مرجع سابق، ص178.
45. نور خالد عبدالمحسن– حجية المحررات والتوقيع، مرجع سابق، ص77.
46. عسى غسان– القواعد الخاصة بالتوقيع الإلكتروني، مرجع سابق، ص69.
47. أيمن على حسين الحوثي، التوقيع الإلكتروني بين النظرية والتطبيق، مرجع سابق، ص45.
48. د. محمد أبو زيد– تحديث قانون لإثبات مكانة المحررات الإلكترونية بين الأدلة الكتابية– دار النهضة العربية، 2004، ص174.
49. عبد الفتاح بيومي حجازي– التوقيع الإلكتروني في النظم القانونية المقارنة– مرجع سابق، ص32.
50. نور خالد عبدالمحسن– حجية المحررات والتوقيع، مرجع سابق، ص77.
51. محمد عامر كريم، إثبات العقد المبرم عن طريق الانترنت، مرجع سابق، ص111.
52. أيمن على حسين الحوثي، التوقيع الإلكتروني بين النظرية والتطبيق، مرجع سابق، ص45.
53. د. عباس العبودي– تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجارها، مرجع سابق، ص232.
54. الصالحين محمد العيش، الكتابة الرقمية، مرجع سابق، ص178.
55. د. فرحان نزال، د. سامر خليل – التوقيع الرقمي وحجيته في الإثبات– مرجع سابق، ص593.
56. أمير فرج يوسف– الجديد في التوقيع الإلكتروني، مرجع سابق، ص120.
57. محمد محمد سادات– حجية المحررات الموقعة إلكترونياً في الإثبات_ دار الجامعة الجديدة، 2011، ص143.
58. د. عطا عبد العاطي السنباطي – الإثبات في العقود الإلكترونية، دار النهضة العربية، سنة 2008، ص225.
59. د. فرحان نزال، د. سامر خليل – التوقيع الرقمي وحجيته في الإثبات– مرجع سابق، ص594.
60. الصالحين محمد العيش، الكتابة الرقمية، مرجع سابق، ص197.
61. أمير فرج يوسف– الجديد في التوقيع الإلكتروني– مرجع سابق، ص197.

62. محمد محمد سادات– حجية المحررات الموقعة إلكترونياً في الإثبات– مرجع سابق، ص144.
63. عبد الفتاح بيومي حجازي– التوقيع الإلكتروني في النظم القانونية المقارنة– مرجع سابق، ص404.
64. محمد عامر كريم، إثبات العقد المبرم عن طريق الإنترنت، مرجع سابق، ص127.
65. محمد سادات– حجية المحررات الموقعة إلكترونياً في الإثبات– مرجع سابق، ص147.
66. المادة (18) من القانون الليبي رقم (6) لسنة 2022م، بشأن المعاملات الإلكترونية.
67. المادة(31) من قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2001.
68. المادة(19) من القانون الليبي رقم (6) لسنة 2022م، بشأن المعاملات الإلكترونية.
69. د. فرحان نزال، د. سامر خليل – التوقيع الرقمي وحجيته في الإثبات– مرجع سابق، ص594.
70. المادة (37) من القانون الليبي رقم (6) لسنة 2022م، بشأن المعاملات الإلكترونية.
71. د. فرحان نزال، د. سامر خليل – التوقيع الرقمي وحجيته في الإثبات– مرجع سابق، ص597.
72. مصطفى أبو مندور– مفهوم المحرر الإلكتروني عند الإثبات– مرجع سابق، ص 786.
73. أمير فرج يوسف– الجديد في التوقيع الإلكتروني– مرجع سابق، ص105.
74. مصطفى أبو مندور– مفهوم المحرر الإلكتروني عند لإثبات– مرجع سابق، ص 787.
75. د. فرحان نزال، د. سامر خليل – التوقيع الرقمي وحجيته في الاثبات– مرجع سابق، ص603.
76. أمير فرج يوسف– الجديد في التوقيع الإلكتروني– مرجع سابق، ص113.
77. محمد محمد سادات– حجية المحررات الموقعة إلكترونياً في لإثبات– مرجع سابق، ص132.
78. المادة (17) من قانون المعاملات من قانون المعاملات الإلكترونية الأردني، رقم 15 لسنة 2015، ص 7.
79. صفاء فتوح– الإطار القانوني والفني للتحول الرقمي في المنظمات الحكومية، مرجع سابق، ص495.
80. المادة (33) من القانون الليبي رقم (6) لسنة 2022م، بشأن المعاملات الإلكترونية.
81. محمد سادات– حجية المحررات الموقعة إلكترونياً في الإثبات– مرجع سابق، ص154

قائمة المراجع

أولا: **الكتب القانونية**:

1. د. أيمن على حسين الحوثي، التوقيع الإلكتروني بين النظرية والتطبيق، دار الفكر الجامعية الاسكندرية– 2011.
2. أمير فرج يوسف – التوقيع الإلكتروني– دار المطبوعات الجامعية، 2008.
3. أمير فرج يوسف – الجديد في التوقيع الإلكتروني، الطبعة الأولى، مكتبة الوفاء القانونية، الاسكندرية، 2011.
4. الصالحين محمد العيش، الكتابة الرقمية طريق للتعبير عن الإرادة ودليلاً للإثبات، الطبعة الأولى، منشأة المعارف، الاسكندرية، 2008.
5. د. ثروت عبدالحميد – التوقيع الإلكتروني– ماهية مخاطرة ومدى حجيته في الإثبات– دار الجامعة الجديدة، 2007.
6. خالد ممدوح إبراهيم– التوقيع الإلكتروني – الدار الجامعية، 2010 .
7. د. ثروت عبدالحميد، التوقيع الإلكتروني، ماهية مخاطرة وكيفية مواجهتها في الإثبات، دار الجامعة الجديدة، 2007.

8. د. صفاء فتوح جمعة– الإطار القانوني والفني للتحول الرقمي في المنظمات الحكومية– دار الفكر والقانون للنشر والتوزيع، جامعة المنصورة، 2022.
9. د. عباس العبودي–تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجارها– منشورات الحلبي الحقوقية، بدون سنة نشر.
10. عبد الفتاح بيومي حجازي– التوقيع الإلكتروني في النظم القانونية المقارنة– الطبعة الأولى، دار الفكر الجامعي، 2005.
11. د. عطا عبد العاطي السنباطي– الإثبات في العقود الإلكترونية– دار النهضة العربية، سنة 2008.
12. عيسى غسان رضى– القواعد الخاصة بالتوقيع الإلكتروني– دار الثقافة للنشر والتوزيع– الطبعة الثانية، 2012.
13. قدري عبدالفتاح– قانون التوقيع الإلكتروني ولائحته التنفيذية والتجارة الإلكترونية– دار النهضة العربية، القاهرة، 2008.

14. محمد أبوزيد– تحديث قانون لإثبات مكانة المحررات الإلكترونية بين الأدلة الكتابية– دار النهضة العربية، 2004.
15. محمد سادات– حجية المحررات الموقعة إلكترونياً في الإثبات_ دار الجامعة الجديدة، 2011.
16. د. ممدوح محمد مبروك – مدى حجية التوقيع الإلكتروني في الإثبات دراسة مقارنة بالفقه الإسلامي، دار النهضة العربية، القاهرة، 2008 .
17. د. يوسف حسن يوسف، التجارة الإلكترونية وأبعادها القانونية الدولية، الطبعة الأولى، المركز القومي للإصدرات القانونية، 2011 .

ثانيا: الرسائل العلمية

1. محمد عامر كريم، إثبات العقد المبرم عن طريق الانترنت، رسالة ماجستير، جامعة الاسكندرية، 2015.
2. نور خالد عبدالمحسن– حجية المحررات والتوقيع الإلكتروني في الإثبات عبر شبكة الإنترنت– رسالة ماجستير جامعة عين شمس .
3. يوسف أحمد النوافله – الإثبات الإلكتروني– رسالة ماجستير، جامعة الإسكندرية، سنة 2010 .

ثالثا: المجلات القانونية:

1. د. أحمد عبدالكريم موسى– حجية التوقيع الإلكتروني في الإثبات، دراسة في التشريع العماني– مجلة البحوث القانونية والاقتصادية والشرعية– جامعة المنصورة– العدد 65– المجلد الأول– أبريل 2010.
2. د. فرحان نزال، د. سامر خليل – التوقيع الرقمي وحجيته في الإثبات في قانون المعاملات الإماراتي والأسباني– مجلة البحوث القانونية والاقتصادية والشرعية، دار الفكر العربي، جامعة المنصورة، العدد(67) الجزء الأول (المجلد الثاني) ديسمبر، 2018.
3. د. مصطفي أبو مندور موسى– مفهوم المحرر الإلكتروني المعد للإثبات– مجلة البحوث القانونية والاقتصادية والشرعية، دار الفكر العربي، جامعة المنصورة، العدد (60) المجلد الثاني، أغسطس 2016.