التوقيع الإلكتروني ودوره القانوني
في المعاملات التجارية الإلكترونية

دكتور/ أحمد رجب عبد الخالق قرشم

مقدمة: –

تمهيد وتقسيم:

مع دخول عصر المعاملات الإلكترونية، وخاصة التجارية منها أصبح الاعتراف بالتوقيع الإلكتروني قانوناً وتطبيقه عملياً أمراً في غاية الأهمية، لأنه أصبح أداة التعاملات المستقبلية في التعاملات الإلكترونية بين الناس والهيئات الاقتصادية، حيث سهلت لهم تبادل المعلومات مع ضمان توثيقها مما أضفى ضمانة شرعية على تبادل المستندات والمعاملات التجارية، خصوصاً في ظل صدور التشريعات الوطنية والدولية التي اهتمت بوضع تشريعات تنظم منظومة التوقيع الإلكتروني.

والتوقيع التقليدي كان ومازال يعتبر الطريقة المعاملات من خلال توقيعه على الوثائق، كما يشير التوقيع على المستند إلى نية الموقَع فيما يتعلق بتلك الوثائق، ومع ظهور عصر التعاملات الإلكترونية، أصبح التوقيع الإلكتروني يعتمد عليه بشكل أساسي في إثبات التعاملات الإلكترونية.

وحتى يمكنا فهم منظومة التوقيع الإلكتروني فذلك يعتمد على فهم التوقيع التقليدي، الذي تتنوع وظائفه، حيث قد يكون التوقيع على الوثيقة بنية الالتزام بموضوع الوثيقة أو قد يكون نية التوقيع مجرد أن يكون الموقَع شاهداً على ما تتضمنه الوثيقة من بيانات، وحتى في حالة وجود توقيع فقد لا تتجه نية الموقَع إلى الالتزام بشيء، فقد يكون قد وقع نتيجة لإكراه أو كان من فاقدي الأهلية أو كان توقيعه غير مبرر أو غير واقعي.

وعليه فان التوقيع على المستندات الإلكترونية تكون بنفس الغرض والهدف للتوقيع على الوثيقة التقليدية، من حيث إقرار الموقَع على ما تحمله المستندات من بيانات وتصديقه على تلك البيانات وكذلك تحديد شخصية الموقَع، وبالتالي فان التوقيع على أي مستند إلكتروني مثل " البريد الإلكتروني " عن طريق كتابة اسم المرسل سيعتبر ذلك توقيعاً إلكترونياً، وهنا تكون قد تحددت شخصية مرسل البريد الإلكتروني بالإضافة إلى تصديقه بكتابة اسمه على محتوى البريد الإلكتروني.

وفى إحدى القضايا بمحكمة الاستئناف في كوينزلاند بأستراليا، والتي عرض فيها المدعى عليه عبر البريد الإلكتروني، تقديم ضمان شخصي لصالح المدعى فيما يتعلق بدفع مبلغ ٥٠٠٠ جنيه إسترليني، أن كتابة عنوان البريد الإلكتروني في العنوان يرقى إلى التوقيع الذى يعتمد على نية المرسل، سواء تم ذلك

التوقيع باستخدام اسمه كاملاً أو اسمه الأخير مسبوقاً بواسطه بعض أو كل الأحرف الأولى من اسمه أو باستخدام الأحرف الأولى من اسمه ، أو استخدام اسم مستعار أو مجموعة من الأحرف والأرقام، ويرى أغلب الفقهاء من أنه إذا قام أحد أطراف عملية إلكترونية بإنشاء وإرسال مستند تم إنشاؤه إلكترونياً، فسيتم معاملته على أنه وقع عليه بنفس القيمة التي سيعامل به القانون على أنه قد وقع على نسخة مطبوعة من نفس المستند الإلكتروني .

وفى مصر صدر القانون رقم ١٥ لسنه ٢٠٠٤ والذي ينظم التوقيع الإلكتروني، وذلك من أجل دعم الصناعة والتجارة الإلكترونية في مصر، وذلك من خلال حماية المعاملات الإلكترونية وتطبيقاتها للتأكيد على شرعية ممارسة الأنشطة المالية عبر الإنترنت، والتحول إلى النظام الرقمي في المعاملات التجارية والصناعية، من خلال استخدام التوقيع الإلكتروني ليتناسب مع المنظومة الرقمية الجديدة في المعاملات والتنافس مع النظم العالمية في ذلك المجال.

وتتولى " هيئة تنمية صناعة تكنولوجيا المعلومات " والتي أنشئت بموجب القانون رقم ١٥ لسنه ٢٠٠٤ من تنظيم التوقيع الإلكتروني، وقد قامت الهيئة في ١١ يوليو ٢٠٠٦ من إصدار أربع رخص لممارسة أنشطة وخدمات التوقيع الإلكتروني لأربع جهات وهي كالتالي:

-الشركة المصرية لخدمات الشبكات وتأمين المعلومات (sns).

-شركة مصر للمقاصة والإيداع الوقيد المركزي.

-الشركة المصرية لخدمات التوقيع الإلكتروني وتأمين المعلومات.

- وزارة المالية.

كما أنشئت بتلك الهيئة إدارة تسمى " إدارة التراخيص الخاصة بسلطة التصديق الإلكتروني " وهي التي تتولى مراجعة طلبات الشركات التي تتقدم للحصول على تراخيص توفير خدمة التوقيع الإلكتروني، حتى تقوم تلك الشركات بإصدار الشهادات الرقمية والتوقيعات الإلكترونية المطابقة لأصل توقيع المواطنين أو توقيع ممثلي شركات القطاع الخاص في التوقيع على المستندات وعملائهم، كما أنها تقدم الاستشارات الفنية وتقوم بالتوسط لحل المنازعات التي تنشأ بين الأطراف فيما يتعلق بالتوقيعات الإلكترونية.

وعليه فان هذه الإدارة تتولى عدة وظائف وهي، تقييم المعايير الفنية والموارد التقنية لتوفير خدمات التوقيع الإلكتروني، ونشر ثقافة تكنولوجيا التوقيع الإلكتروني محليا وإقليميا، تعظيم الاستفادة من تطبيقات الأعمال الإلكترونية، تلقي الشكاوى المتعلقة بأنشطة التوقيع الالكتروني والمعاملات الالكترونية وتكنولوجيا المعلومات، واتخاذ الإجراءات الضرورية بشأنها، و تقديم المشورة الفنية بشأن المنازعات التي تنشأ بين الأطراف فيما يتعلق بأنشطة التوقيع الالكتروني والمعاملات الالكترونية وتكنولوجيا المعلومات،وإقامه المعارض والمؤتمرات والندوات المتخصصة في مجال تكنولوجيا المعلومات والاتصالات داخليًا وخارجيًا .

تقوم هيئة تنمية صناعة تكنولوجيا المعلومات" إيتيدا "بتشغيل السلطة الجذرية للتصديق الإلكتروني باعتبارها واحدة من المهام الأساسية لها وفقا لأعلى معايير الأمن الالكتروني وتخدم عملاءها على مدار الساعة، وتعتبر السلطة الجذرية الوطنية هو الكيان موضع الثقة لجميع الأطراف المعولّة في هذا المجال .وعلاوة على ذلك، تُعد السلطة الجذرية الوطنية هي القاعدة القانونية والوطنية التي ستؤثر على جميع تطبيقات تكنولوجيا المعلومات والتجارة الإلكترونية ومُعاملات التجارة الإلكترونية .وكما توفر الاعتراف المتبادل في جميع أنحاء مصر والسلطات الجذرية الأخرى في الدول المختلفة.

السلطة الجذرية لديها حقوق وقف تشغيل أي سلطة إصدار الشهادات في حالة قصور الأمن، وكذلك النسخ الاحتياطي لبيانات التوقيع الالكتروني الخاصة بمزودي خدمات الشهادات للحفاظ على توافر هذه الخدمة في حالة فشل أو إفلاس واحد من مقدمي خدمات إصدار شهادات التوقيع

الالكتروني، ومسؤولة عن قابلية التشغيل البيني بين الدول الأخرى التي توفر نقطة تواصل بين مصر والدول الأخرى في فيما يتعلق بالتوقيع الالكتروني، ومراجعة كافة متطلبات مفتاح الشفرة المعلن الفنية الخاصة بمقدمي خدمات إصدار شهادات PKI التوقيع الالكتروني مقابل التعليمات التنفيذية المصرية وجميع المعايير الدولية المُحدثة، وتقدم الاستشارات الفنية للمجتمع ككل في مجال أمن المعلومات وخاصة في البنية التحتية الرئيسية العامة.

وتعتبر خدمات التوقيع الإلكتروني له أهمية كبيرة في حماية وحفظ سرية المعلومات الخاصة بالأفراد والمؤسسات والكيانات الاقتصادية وخاصة في مجال الاتصال وتكنولوجيا المعلومات سواء بالنسبة للقطاع الحكومي أو الخاص.

ولذلك يعتبر مركز تميز التوقيع الإلكتروني ESCC والذي يقدم خدمات إنشاء مراكز البنية التحتية للتوقيع الإلكتروني وخدماته وتطبيقاته على مختلف أنظمة التشغيل ويربط برمجيات وأجهزة العملاء ببنية شفرة المفتاح المعلن Public Key.

أهمية هذا البحث:

ترجع أهمية البحث إلى حاجة الناس إلى الثقة والأمان في المعاملات التي تتم عبر الانترنت، خاصة وأن المعاملات عبر الإنترنت مازالت حديثة خاصة في مجال العقود الإلكترونية، ولا شك أن الثقة في الأشخاص الذين تتعامل معهم عبر الإنترنت تكاد تكون منعدمة فأنت غير متأكد من شخصية ونوايا من يراسلك عبر البريد الإلكتروني حيث أنك في الغالب لا تكون بينك وبينهم معرفة شخصية قبل ذلك فما هو موقفك إذا كانت تلك المراسلات بشأن تعاملات مالية حول صفقة تجارية ...لا شك أن أزمة الثقة هذه هي ما تثير قلق الكثير من الناس.

من هنا ظهرت فكرة التوقيع الإلكتروني لزيادة مستوى الأمن والخصوصية عبر الشبكة ...ومن خلال تلك التكنولوجيا يتم الحفاظ على سرية المعلومات والرسائل المتبادلة بين الأشخاص عبر شبكة الإنترنت وذلك عن طريق التأكد من شخصية المرسل والمستلم إلكترونياً والتأكد من مصداقية هذه الشخصيات مما يسمح بكشف أي تلاعب أو تحايل يتم من قبل الغير، كما لا يمكن لأي شخص أخر تعديل أو تحريف تلك الرسائل.

أهداف البحث:

يهدف هذا البحث إلى ما يلي:

١-التعريف بفكرة التوقيع الإلكتروني.

٢-التطرق إلى وظيفة التوقيع الإلكتروني.

٣-معرفة أنواع التوقيع الإلكتروني.

٤-الوقوف على فوائد التوقيع الإلكتروني.

٥-مدى الاعتراف القانوني للتوقيع الإلكتروني.

٦-التعرف على التشريعات التي أقرت بالتوقيع الإلكتروني.

إشكالية البحث:

أصبح الاستثمار هو عصب كل القطاعات في الدولة، لأنه بتضاعف الاستثمارات يؤدى ذلك إلى زيادة الدخل القومي الذي يعتبر هو الممول الرئيسي لأغلب قطاعات الدولة، وعليه فيجب أن تتسم السياسة التشريعية الاستثمارية للدولة بالمرونة وبالتطور الذي يحض على جذب المزيد من الاستثمارات، الأمر الذي حذي بالدول إلى تطوير منظومة المعاملات التجارية والاستثمارية عبر الإنترنت، ومن ثم تنظيم التوقيع الإلكتروني لإضفاء الثقة والأمان على المعاملات التجارية الإلكترونية.

كما أن المشرع المصري كان على وعي بأهمية وجود تنظيم تشريعي للإمضاء الإلكتروني، الأمر الذي جعل المشرع المصري يهتم بتنظيم التوقيع الإلكتروني بالقانون رقم ١٥ لسنة ٢٠٠٤.

منهجية البحث:

تتمحور هذه الدراسة حول التعريف بالتوقيع الإلكتروني في ظل المعاملات الإلكترونية والتعريف بفوائدها وأنواعها، والأهمية التي أولتها التشريعات الدولية من أجل حث الدول على تطوير تشريعاتها من أجل أن تتضمن منظومة التوقيع الإلكتروني، من خلال وضع الأسس اللازمة لمساعدة الدول على أن تنظم في تشريعاتها التوقيع الإلكتروني، وإضفاء الثقة في التوقيع الإلكتروني خاصة في المعاملات التجارية الإلكترونية، والعقود الإلكترونية.

بالإضافة إلى أهمية تنظيم التشريع المصري للتوقيع الإلكتروني في ظل القانون رقم ١٥ لسنة ٢٠٠٤، من أجل أن يساير التطور الدولي في المعاملات التجارية الإلكترونية وخاصة الدولية منها من خلال الإنترنت وأدواتها.

ولقد اعتمدت في تلك الدراسة على استخدام المنهج الاستقرائي لمعرفة الجهود الدولية والفقهية القانونية في تأصيل التوقيع الإلكتروني، كما الاعتماد على المنهج التحليلي في تحليل النتائج المتولدة عن تلك الجهود السابقة.

خطة البحث:

نظراً لحداثة التجارة الإلكترونية وحداثة تنظيم التوقيع الإلكتروني خاصة في مصر، بالإضافة إلى أن المنظومة الإلكترونية في المعاملات التجارية وما يستتبع ذلك من تنظيم التوقيع الإلكتروني لم تصل بعد إلى مستوى المعاملات التجارية التقليدية، الأمر الذي جعلنا نظراً لأهمية التطبيق العملي للتوقيع الإلكتروني وخاصة في المعاملات التجارية الإلكترونية نحاول في بحثنا التعريف بالإمضاء الإلكتروني وفهم خواصه ووظائفه وأهميته من خلال تقسيم دراستنا إلى المباحث التالية:

المبحث الأول: التعريف بالتوقيع الإلكتروني ووظيفته.

المبحث الثاني: أنواع التوقيع الإلكتروني وفوائده.

المبحث الثالث: الأثر القانوني والمصادقة للتوقيع الإلكتروني.

المبحث الأول

التعريف بالتوقيع الإلكتروني ووظيفته

المطلب الأول

التعريف بالتوقيع الإلكتروني

الفرع الأول: مفهوم التوقيع الإلكتروني:

يمكن تعريف التوقيع الإلكتروني على أنه " وسيلة للتوثيق الإلكتروني لهوية شخص ما، مع اتجاه نية ذلك الشخص لتوضيح مواقفه من ودلالته على ذلك التوقيع "١ ، أو يقصد بها " البيانات في صورة إلكترونية والتي يمكن استخدامها لتحديد هوية الموقّع فيما يتعلق بتلك البيانات وللإشارة إلى موافقته على المعلومات الواردة في تلك البيانات.

إلا أن هذا الاصطلاح لم يجد له صدى عالمياً في التشريعات الدولية، ويمكن تعريف التوقيع الإلكتروني على انه " بيانات الكترونية، سواء كانت على شكل حروف أو أرقام أو رموز أخرى، مرتبطة ارتباطا منطقياً بمستند إلكتروني، تستخدم بغرض توثيق ذلك السجل أو الموافقة عليه".

[1] Evidence Act 1995 (Cth) s71 and Evidence Act 1995 (NSW) s71

وفى قانون المعاملات الإلكترونية الأسترالي لا يستخدمون اصطلاح " توقيع إلكتروني" ولكنهم يستخدمون بدلاً منها اصطلاح " اتصال إلكتروني"، على الرغم من أن عبارة " الاتصال الإلكتروني" أضيق نطاقاً من عبارة " التوقيع الإلكتروني"، وتم تعريف الاتصال الإلكتروني وفقاً للقانون الاسترالي بأنه:

(أ) إبلاغ المعلومات في شكل بيانات أو نص أو صور عن طريق الطاقة الكهرومغناطيسية الموجهة أو غير الموجهة أو كليهما.

(ب) نقل المعلومات في شكل صوت عن طريق الطاقة الكهرومغناطيسية الموجهة أو غير الموجهة، أو كليهما، حيث تتم معالجة الصوت عن طريق نظام التعرف الآلي على الصوت.

كما أن قانون المعاملات الإلكترونية النيوزيلاندي لعام ٢٠٠٢ قد نص في تعريفة لمفهوم التوقيع الإلكتروني على أنه " معلومات في شكل إلكتروني، تستخدم لتحديد هوية الشخص والإشارة إلى موافقته على تلك المعلومات " .

كما تضمن قانون سنغافورة للمعاملات الإلكترونية لعام ١٩٩٨ أحكاماً واسعة النطاق تتناول التوقيعات الإلكترونية والرقمية، حيث يعرّف قانون سنغافورة التوقيع الإلكتروني على أنه " أي أحرف أو أحرف أو أرقام أو رموز أخرى في شكل رقمي مرفق بسجل إلكتروني أو مرتبط به منطقياً، ويتم تنفيذه أو اعتماده بقصد توثيق السجل الإلكتروني أو الموافقة عليه " .

قد يكون التوقيع الإلكتروني بسيطًا مثل كتابة اسم في نهاية البريد الإلكتروني. قد يكون تحولًا رياضيًا معقدًا مصممًا لتوفير مستوى من الأمان لضمان أن الرسالة الإلكترونية من المرسل المزعوم وغير معدلة، ويحتوي كل من نموذجي التوقيعات على بيانات في شكل رقمي مرفقة أو مرتبطة منطقيًا بمستند إلكتروني، إن مستوى الأمان الذي سيتم استخدامه هو أمر يخص الأطراف، اعتمادًا على عوامل مثل المخاطر التجارية والقانونية المعنية ٢.

كما أنه في كثير من الأحيان قد يحتاج أطراف المعاملات الإلكترونية من خلال الإنترنت إلى التحقق من هوية المرسل والمصادقة على تلك الرسالة أو البيانات التي وقع عليها الشخص المرسل.

---

[2] د/ إبراهيم بن سطم بن خلف العنزي، التوقيع الإلكتروني وحمايته الجنائية، رسالة دكتوراه، جامعة نايف العربية للعلوم الأمنية، ٢٠١٠، ص٢٢.

وقد وضعت لجنة الأمم المتحدة للتجارة الإلكترونية (الأونسيترال) القواعد الموحدة بشأن التوقيع الإلكترونية وهي كالتالي:

١-عدم تحديد نوع الطريقة التي يتم بها استخدام التوقيع الإلكتروني، فاتحاً المجال لإيراد أية طريقة تراها الدول ملائمة من ترميز أو تكويد أو تشفير أو أية طريقة أخرى تكون مناسبة.

٢-التعريف ركز على أن أية طريقة للتوقيع يجب أن تحقق وظائف التوقيع من تحديد لهوية الشخص الموقع والتعبير عن إرادته بالموافقة على مضمون رسالة البيانات، ومن المؤكد أن كل توقيع أيا كانت الطريقة المستخدمة في إنشائه يجب أن يحقق تلك الوظائف.

ويعرف الاتحاد الأوروبي نوعين من التوقيع الإلكتروني :-

١-التوقيع الإلكتروني: " معلومات على شكل إلكتروني متعلقة بمعلومات إلكترونية أخرى ومرتبطة بها ارتباطاً وثيقاً ويستخدم أداة للتوثيق.

التوقيع الإلكتروني ٢-التوقيع الإلكتروني المعزز: هو توقيع إلكتروني يشترط فيه أن يكون:

- مرتبطا ارتباطا فريداً من نوعه مع صاحب التوقيع. -قادراً على تحقيق تحديد صاحب التوقيع والتعرف عليه باستخدامه.

- تم إيجاده باستخدام وسائل يضمن فيها صاحبه السرية التامة.

- مرتبطاً مع المعلومات المحتوى في الرسالة حيث أنه يكشف أي تغيير في المعلومات.

ويعرف القانون المصري رقم (١٥) لسنة ٢٠٠٤، ولائحته التنفيذية رقم ١٠٩ لسنة ٢٠٠٥ التوقيع الإلكتروني على أنه:

" ما يوضع على محرر إلكتروني ويأخذ شكل أحرف وأرقام ورموز وإشارات وما إلى ذلك، وله شخصية فريدة تسمح بتحديد هوية شخص الموقع وتمييزه عن الآخرين".

ونلاحظ في هذا التعريف أن المشرع المصري في تعريفه للتوقيع الإلكتروني قد أصابه القصور، حيث أنه حصر في تعريفه للتوقيع الإلكتروني على أنه لتحديد شخصية الموقع ودون اعتبار إلى أن التوقيع الإلكتروني يستخدم أيضاً للإشارة لموافقة الموقّع على البيانات التي قام من أجلها بالتوقيع الإلكتروني ٣.

حيث أن أغلب التشريعات الدولية وخاصة قانون الأونسيترال النموذجي للتوقيع الإلكتروني في عام ٢٠٠١ قد حاولت في وضعها للنموذج الاسترشادى لحض الدول على تشريع التوقيع الإلكتروني، وحتى تبث الطمأنينة في فاعلية التوقيع الإلكتروني من خلال التأكيد على تكافؤ التوقيع الإلكتروني مع التوقيع العادي من أن التوقيع في العموم سواء كان إلكترونياً أو عادياً فإن الهدف منه التعريف بشخص الموقّع والتأكيد على أن التوقيع يشير إلى موافقه الموقّع على البيانات التي بسببها وقع الشخص عليها. ٤

ومن هنا نجد أن من أهداف التوقيع في العموم هو التأكيد على موافقه الموقّع على البيانات التي وقع عليها في المستند وهذا مالم يبرزه تعريف المشرع المصري في تعريفه للتوقيع الإلكتروني.

٣) نسرين عبد الحميد نبيه ، الجانب الإلكتروني للقانون التجاري، نشر بمنشأة المعارف، الطبعة الأولى، الإسكندرية، ٢٠٠٨، ص٣٣٨ .

٤) عبد الحكيم زروق، تنظيم التبادل التجاري، تنظيم التبادل الإلكتروني للمعطيات القانونية عبر الإنترنت، منشورات دار الأورمان، الطبعة الأولى، الرباط، ٢٠١٦، ص٦٧

المطلب الثاني

وظيفة التوقيع الإلكتروني

إن وظيفة التوقيع في العوم تكون أكثر من مجرد توثيق لصحة الوثيقة الموقع عليها، فعلى سبيل المثال إذا ما ظهرت توقيعات على وثيقة ما كعقد بيع مثلاً، فتعتمد وظيفة تلك التوقيعات على نية الشخص الموقّع ما إذا كانت متجهة إلى أن يكون أحد أطراف التعاقد أو شاهد على العقد ٥.

وتشمل وظائف التوقيع ما يلي:

- تحديد شخصية الموقّع.

أن يدل التوقيع الموجود على المحرر أنه ينسب لشخص معين بالذات فيعل الورقة الموقعة منسوبة إليه وهذه الوظيفة يقوم بها التوقيع الكتابي في شكل علامة خطية وشخصية لصاحب التوقيع، وتعد الورقة التي تحمل التوقيع دليلاً كتابياً كاملاً يحتج بها على من وقعها. والتوقيع الالكتروني يقوم بنفس الدور، وذلك في شكل رموز أو أرقام أو حروف أو أية إشارات تدل على شخصية الموقع، وتميزه عن غيره.

وبذلك فإن التوقيع سواء كان كتابي أو الكتروني يؤدي هذه الوظيفة ولكن الاختلاف في كيفية وضع التوقيع على المحرر.

فالتوقيع الكتابي ينشأ على محررات ورقية ذات طبيعة مادية تحاكي الشكل الذي تم به التصرف القانوني، وذلك بالحضور المادي لأطراف التصرف ومقابلتهم وجهاً لوجه في مجلس واحد، لذا كان من الضروري أن يأتي التوقيع مادياً على ذات المحررات الورقية.

- **الموافقة على محتويات الوثيقة.**

[5]) See A McCullagh, P Little and W Caelli, 'Electronic signatures: Understand the past to develop the future, [1998] UNSWLJ 56 and A McCullagh, W Caelli and P Little, 'Signature stripping: A digital dilemma', [2001] JILT (1).

وتتعلق هذه الوظيفة بمسألة التأكد من رضاء صاحب التوقيع وقبوله الالتزام بمضمون التصرف القانوني وإقراره له، فالتوقيع الكتابي إذا ثبتت نسبة المستند إلى موقعه كان ذلك دليلاً على قبوله الالتزام بمضمون العمل القانوني المدون في المحرر، فتوقيع الشخص بخط يده أو بأية وسيلة يقرها القانون على ورقة يؤكد إقراره بما يدون فيها وقبوله الالتزام بما ورد فيها من تصرفات قانونية.

وبالنسبة للتوقيع الإلكتروني فتتضح موافقة الموقّع على المستند من مجرد وضع توقيعه الإلكتروني على المستند أياً ما كان شكل هذا التوقيع فإنها تدل موافقة الموقّع على تلك البيانات وأنه يرغب في الالتزام بها.

- توضيح وتحديد نوعية المشاركة الشخصية للموقّع في عملية التوقيع.

وذلك ما إذا كان طرف في هذه الوثيقة أو مجرد شاهد على بيانات والتزامات تلك الوثيقة.

- ربط شخص معين بمحتويات الوثيقة.

-الإشارة إلى تأليف الوثيقة من قبل الموقّع.

ويعتبر التوقيع ملزماً قانونياً على الشخص الموقّع وفق أغلب التشريعات في حالة عدم وجود عوامل فساد مثل الاحتيال أو التزوير أو عدم الأهلية فيما يتعلق بمحتويات الوثيقة حتى ولو لم يقرأ الشخص الموقّع للوثيقة ٦.

وتوجد متطلبات رئيسية في وظيفة التوقيع يمكن إجمالها فيما يلي:[7]

[6] ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، ٢٠٠٧، ص٤٧.

-إذا ما توجد أدلة على وجود حالة فساد بالوثيقة.

-تعمل كتحذير من أن هذه الوثيقة تحمل عواقب قانونية.

-تعمل كوسيلة للاعتماد، حيث قد يعتمد عليها الآخرون لاحقاً.

-توفير مستوى من التأمين، لضمان قدر من الثقة لمختلف العناصر المشاركة في عملية التبادل الالكتروني والحفظ والاختزان الطويل الأمد للبيانات الالكترونية. وبفضل هذا المناخ يمكن أن يصل معدل الثقة في التوقيع الالكتروني إلى مستوى متطابق من المعدل الذي يمكن تحقيقه من خلال المستندات الورقية. وحتى يتم منح صفة قانونية للتوقيع الالكتروني.

-إعطاء صفة أو صبغة قانونية قاطعة للتوقيع الالكتروني.

وهذا الأمر لا يتعلق فقط بضرورة ضمان خصوصية البيانات المرسلة من خلال التشفير والترميز ولكن أيضاً ضرورة ضمان باقي مستويات وخدمات التأمين والتي تتمثل في وحدة البيانات واستقامتها وعدم التنصل أو عدم القدرة على الإنكار والتحقق أو التوثيق أو التعرف على المستخدم، وبفضل الإطار التقني والقانوني الذي يمكن استخدامه يمكن للتوقيع الالكتروني تأدية كافة هذه الخدمات.

وعندما يتطلب القانون التوقيع الإلكتروني، فإنه وفقاً لأغلب التشريعات فإنه يعتبر الشرط قد تم الوفاء به إذا ما حدث " اتصال إلكتروني "، وعندما يكون التوقيع الإلكتروني معادلاً للتوقيع التقليدي، فيجب معاملته على قدم المساواة ٨ .

---

[7] Promoting Confidence in Electronic Commerce: legal issues on international use of electronic authentication and signature methods, United Nations Commission on International Trade Law (UNCITRAL), Vienna, United Nations, 2007 (released in 2009). Available at: http://www.uncitral.org/pdf/ English/texts/electron/08-55698_Ebook.pdf (last accessed 30 June 2013).

[8] See Electronic Commerce Expert Group, 'Electronic commerce: Building the legal framework, Report of the Electronic Commerce Expert Group to the Attorney-General', (1998), para 2.7.28

وإذا ما أخذنا قانون المعاملات الإلكترونية الأسترالي كمثال، نجد أنه يشترط في التوقيعات الإلكترونية شروط معينة، حيث ينص قانون التوقيع على ما إذا كان القانون يتطلب توقيع شخص معين، فإن هذا الشرط يتم الوفاء به فيما يتعلق برسالة إلكترونية إذا ما كان ما يأتي:

أ) استخدام طريقة لتحديد هوية الشخص وتوضيح موافقة الشخص على المعلومات المرسلة.

ب) إذا ما كان التوقيع الإلكتروني موثقة بقدر ما كانت مناسبة للأغراض التي تم من أجلها إرسال المعلومات.٩

المبحث الثاني

أنواع التوقيع الإلكتروني وفوائده

المطلب الأول

أنواع التوقيع الإلكتروني

يمكن أن تتخذ التوقيعات الإلكترونية العديد من الأشكال ويمكن إنشاؤها بواسطة العديد من التقنيات المختلفة. تشمل الأشكال الشائعة للتوقيعات الإلكترونية على سبيل المثال لا الحصر كلمة المرور أو رقم التعريف الشخصي (PIN) وتوقيعات البريد الإلكتروني والبطاقات الذكية والقياسات الحيوية والتوقيعات الممسوحة ضوئيًا والتوقيعات الرقمية. في الحياة اليومية، أكثر أشكال التوقيعات الإلكترونية شيوعًا والتوقيعات

٩) عبد الحكيم زروق، تنظيم التبادل التجاري، تنظيم التبادل الإلكتروني للمعطيات القانونية عبر الإنترنت، [9] منشورات دار الأورمان، الطبعة الأولى، الرباط، ٢٠١٦، ص١٩٦

الممسوحة ضوئياً وتوقيعات البريد الإلكتروني والتوقيعات الرقمية (PIN) الإلكترونية، وتعتبر التوقيعات الأكثر شيوعاً " كلمة موثقة أو التوقيعات الممسوحة ضوئياً " ١٠.

وتسمى كلمة المرور هذه أيضاً " برقم التعريف الشخصي "، والتوقيعات الممسوحة ضوئيًا للصور شائعة أيضًا. يسمح الماسح الضوئي الإلكتروني للمستخدمين بمسح قطعة من الورق بتوقيع مكتوب إلكترونية للتوقيع، ويمكن بعد ذلك إرفاق الصورة الرقمية بالوثيقة " JPEG " بخط اليد في الكمبيوتر لإنشاء صورة " صورة نقطية " أو كتوقيع إلكتروني، وهو أقل تكلفة من الطرق الأخرى، ومع ذلك فمن السهل تزويرها.

يمكن أن يتكون توقيع البريد الإلكتروني من نص أو صور أو كليهما. تحتوي معظم بوابات البريد الإلكتروني على أداة للمستخدمين لإنشاء توقيع واستخدامه. على سبيل المثال، يضيف Microsoft Outlook تلقائيًا النص أو الصور التي تم إنشاؤها كتوقيع على الرسائل، في السنوات الأخيرة، تم إطلاق المزيد والمزيد من برامج توقيع البريد الإلكتروني لمساعدة المستخدمين على تطوير توقيع بريد إلكتروني أكثر أمانًا؛ على سبيل المثال، قد تساعد بعض برامج إنشاء التوقيع في إنشاء علامات ورموز لإبراز الطابع الشخصي لتوقيع المستخدم في رسائل البريد الإلكتروني.

التأثير القانوني لتوقيع البريد الإلكتروني قابل للنقاش. يشير تقرير الأونسيترال حول تعزيز الثقة في التجارة الإلكترونية في عام ٢٠٠٧ إلى أنه "لا للأسماء المكتوبة على رسائل البريد الإلكتروني غير المشفرة ولا الإشارات الممسوحة ضوئيًا تقدم مستوى عاليًا من الأمان أو يمكنها تحديد هوية منشئ الاتصال الإلكتروني بدقة تظهر. ومع ذلك، تختار الكيانات التجارية بحرية استخدام هذه الأشكال من "المصادقة" من أجل سهولة الاتصالات ومناسبتها وفعاليتها من حيث التكلفة ١١.

---

١٠) نسرين عبد الحميد نبيه، الجانب الإلكتروني للقانون التجاري، نشر بمنشأة المعارف، الطبعة الأولى، الإسكندرية، ٢٠٠٨، ص٣٨٨.[10]

[11] SM Integrated Transware Pte Ltd v. Schenker Singapore (Pte) Ltd [2005] SGHC 58

يعد التوقيع الرقمي أحد أهم أشكال التوقيعات الإلكترونية وأكثرها موثوقية. من منظور تقني، يتم تعريفه على أنه "عملية مفتاح غير متماثل حيث يتم استخدام المفتاح الخاص لتوقيع البيانات رقميًا ويتم استخدام المفتاح العام للتحقق من التوقيع". التوقيعات الرقمية "توفر حماية التقنيات التشفير التي تلعب دورًا رئيسيًا في ضمان مستوى التجارة الإلكترونية وأمن نظام المعلومات، على الرغم من أن تنفيذ هذه التقنيات يتطلب إجراءات مناسبة وكافية.١٢

يمكن تعريف التشفير كعمل كتابي سري يتكون من سلسلة من الشفرات والرموز المستخدمة لإخفاء محتوى الرسالة. هناك نوعان من التشفير. يُعد الأول، المعروف باسم تشفير المفتاح المتماثل أو السري، طريقة تشفير ومصادقة بيانات يتشارك فيها المرسل والمستقبل نفس المفتاح. يسمى الثاني تشفير المفتاح غير المتماثل أو العام ويستخدم مفتاحين مختلفين لعملية التشفير وفك التشفير، والمعروفين باسم المفتاح الخاص والمفتاح العام. يتم استخدام مفتاح خاص (محتفظ به فقط من قبل مرسل البيانات المرسلة) بالتزامن مع خوارزمية التوقيع لتوقيع البيانات، ويستخدم مفتاح عام (غالبًا ما يكون عامًا في دليل على الإنترنت) من قبل مستلم البيانات مع الخوارزمية للتحقق من التوقيع المستلم. أي أن هذه المفاتيح هي رموز رياضية مختلفة عن بعضها البعض، ولكنها مرتبطة بشكل لا ينفصم. المفتاح الخاص يبقى مع الشخص الذي يملك التوقيع الإلكتروني ويتم الاحتفاظ به سرا، بينما يتم توزيع المفتاح العام بحرية.

[12] ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، ٢٠٠٧، ص٨١

المطلب الثاني

فوائد التوقيع الإلكتروني

هناك نوعان من الفوائد الرئيسية التي يمكن تحديدها باستخدام التوقيعات الإلكترونية، الأول هو إمكانية التحقق من موثوقية التوقيع الرقمي من قبل مقدمي الخدمة المعنيين. عند استخدام توقيع إلكتروني وإتمام عملية المصادقة، يجب أن يتمكن مقدمو الخدمة من السماح لمستلم البريد الإلكتروني بمعرفة ما إذا كان قد تم العبث بالبريد الإلكتروني أثناء العملية من كمبيوتر المرسل إلى كمبيوتر المستلم عند الطلب. بما أن الوثيقة موقعة رقمياً، سيقوم المفتاح الخاص بإجراء حساب رياضي لمحتويات المستند بالكامل. سيؤدي هذا إلى إنتاج ملخص، يتم تشفيره أيضًا وإرساله مع المستند. عندما يصل المستند إلى كمبيوتر المستلم والمفتاح العام يقوم بمصادقة التوقيع، سيقوم المفتاح العام بحساب مماثل لمحتويات المستند كما سيقدم ملخصًا. يعني الارتباط الرياضي بين المفتاحين أن الملخصات ستكون متطابقة إذا كانت الوثيقة المستلمة هي نفسها تمامًا مثل المستند الذي تم إرساله. الملخص الأول (الذي تم إنشاؤه بواسطة المفتاح الخاص) غير مشفر ثم مقارنته بالملخص الجديد (الذي تم إنشاؤه بواسطة المفتاح العام) وإذا كان أحدهما مختلفًا عن الآخر، فلن يلاحظ المستلم أن المستند قد تم اعتراضه وتغييره في الطريق.

الفائدة الثانية من التوقيعات الإلكترونية هي أنها تسمح بنقل واستلام رسائل البريد الإلكتروني الآمنة. هذه ملكية مرغوبة للغاية، خاصة بالنسبة للمحامين، الذين سيتعين عليهم في كثير من الأحيان التعامل مع المعلومات الحساسة للغاية والموثوقة. تصبح رسائل البريد الإلكتروني الآمنة ممكنة بمجرد حصول شخص ما على مفتاح عام لشخص آخر. يمكن إرسال المفتاح العام بالبريد الإلكتروني بشكل منفصل إلى فرد أو نسخه إلى قرص وإرساله عبر المنشور أو حتى تنزيله من موقع ويب مخصص ١٣. مثال على عملية التوقيع الرقمي على النحو التالي. إذا رغب "أ" في إرسال بريد إلكتروني آمن إلىB ، فسيستخدم A المفتاح العام لـ B لتشفير البريد الإلكتروني وأي مستندات مرفقة. بمجرد تشفيرها، فإن الطريقة الوحيدة التي يمكن من خلالها

[13] K. Bharvada (2002) 'Electronic signatures, biometrics and PKI in the UK', International Review of Law Computers and Technology, 16 (3): 265–75, at p. 268.

إلغاء تشفير البريد الإلكتروني هي استخدام المفتاح الخاص لمفتاح عام. لذلك، إذا قام المفتاح العام لـ A بتشفير البريد الإلكتروني، فلا يمكن فك تشفيره إلا بواسطة المفتاح الخاص لـ .A إذا اعترض أي شخص البريد الإلكتروني أثناء نقله، فلن يتمكن من عرض محتوياته إلا إذا كان لديه نسخة من مفتاح A الخاص.

فيما يتعلق بالوظائف، يمكن اعتبار التوقيعات الرقمية بمثابة عملية إنشاء واستخدام والتحقق من التوقيع الذي يمكن أن يحدد الموقع، ويصادق على المحتوى ويعمل كدليل للإجراءات القانونية١٤.

أولاً: يضمن التشفير غير المتماثل مستوى عالٍ من الأمان في الاتصالات الإلكترونية وتوافق سياق الرسالة المرسلة عبر شبكة مفتوحة مثلt لأصالة وحماية السلامة وعدم التنصل". من الجدير بالذكر أن التوقيعات الرقمية والبنى التحتية للمفتاح العام تعتبر أمثلة مهمة لإنترنت.

ثانيًا: توفر التوقيعات الرقمية توثيقًا لهوية الموقِّع من خلال إسناد الرسالة إلى الموقِّع، بحيث يُعرف من شارك في المعاملة. يستند الأساس المنطقي لهذه الوظيفة إلى حقيقة أنه لا يمكن تزوير التوقيعات الرقمية بسهولة، ما لم يفقد الموقّع التحكم في المفتاح الخاص إما عن طريق الخطأ أو عن قصد.

ثالثًا :يحمي التوقيع الرقمي سلامة البيانات المرسلة حتى يتمكن المستلم من التأكد من أن مقارنة هجمي الرسالة لن يغير الرسالة.

من الجدير بالذكر أن التوقيعات الإلكترونية عالية الجودة (التوقيعات الرقمية) مصحوبة بشهادة إلكترونية يمكن أن توفر ثلاث وظائف مهمة١٥:

١- للمصادقة على هوية الشخص الذي وقع على البيانات حتى يعرف من شارك في المعاملة، فبما أن التوقيع الإلكتروني محفوظ على بطاقة ذكية لا يغادرها أبداً ومحمية بكود سرى بالإضافة إلى تشفير البيانات أثناء إرسالها وهي موقعة إلكترونياً، بما لا يسمح لأي شخص لا يمتلك الصلاحيات بالتلاعب بها أو تغييرها.

---

[14] D. Capps (2002) 'Conveyancing in the 21st century: an outline of electronic conveyancing and electronic signatures', Conveyancer and Property Lawyer, September/October, pp. 443–55.

[15] ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، ٢٠٠٧، ص٩٠

٢- لحماية سلامة البيانات بحيث يمكن معرفة أن قراءة الرسالة لم يتم تغييرها، سواء عن طريق الخطأ أو التعمد.

٣- عدم الإنكار للسماح بإثبات لاحقة على من شارك في المعاملة، وبالتالي منع أي شخص من إنكار أنه / أنها أرسلت أو تلقي البيانات، وخاصة في ظل وجود طرف ثالث كهيئة تصديق على التوقيع الإلكتروني.

لذلك، يحق للوثائق التي تم توثيقها بتوقيع إلكتروني آمن، افتراض النزاهة، وأن التوقيع هو توقيع الشخص المرتبط به، وأن المستخدم قد أبرم التوقيع بقصد التوقيع أو الموافقة على الوثيقة.

عندما تنطوي المعاملات على عدة مراحل في أوقات مختلفة، من الصعب إثبات اتساق الهوية،

فعلى سبيل المثال، كيف يمكن إثبات من شارك في صفقة معينة؟ ما الذي يجعل هوية المرسل والمستلم للبيانات لا يمكن إنكاره؟ كيف يمكن للمرء أن يحدد من قد يكون قرأ هذه الرسالة؟ هل المرسل لديه السلطة للقيام بهذه الصفقة؟ ماذا يحدث إذا فقد مفتاح فك التشفير؟ من المسؤول إذا تم اختراق مفتاح فك التشفير؟

في ظل هذه الظروف، يلعب التحقق دورًا مركزيًا في عملية تحديد الهوية داخل البنية التحتية للمفتاح العام، للتحقق من التوقيع الرقمي، يجب أن يكون لدى المحقق حق الوصول إلى المفتاح العام للمُوقّع وأن يتأكد من تطابقه مع المفتاح الخاص للمُوقِّع. نظرًا لكونه مجرد زوج من الأرقام.

وسيحتاج الأشخاص الذين لم يتعرفوا من قبل ولكنهم يرغبون في التعامل مع بعضهم البعض عبر شبكات الكمبيوتر مثل الإنترنت إلى وسيلة للتعرف على بعضهم البعض أو مصادقتهم. من الضروري استخدام طرف ثالث موثوق به أو أكثر لربط موقّع محدد بمفتاح عام محدد لبناء علاقة ثنائية.

ويمكن لهذا الطرف الثالث، وهي هيئة تصديق أن تشهد على طرف من خلال إصدار شهادة تثبت هويته / هويتها، أو أن يشهد على امتلاكه لمؤهلات أو سمات ضرورية، وبالتالي فإنه يثبت الثقة في المعاملات الإلكترونية١٦.

١٦) نسرين عبد الحميد نبيه ، الجانب الإلكتروني للقانون التجاري، نشر بمنشأة المعارف، الطبعة الأولى، [16] الإسكندرية، ٢٠٠٨، ص٤٠٧

المبحث الثالث

الأثر القانوني والمصادقة للتوقيع الإلكتروني

المطلب الأول

الأثر القانوني للتوقيع الإلكتروني

حتى يمكن الاعتراف بالتوقيع قانوناً وبانة فعال لابد من تلبية بعض المتطلبات وهي كالتالي:

١- نية التوقيع.

٢- تحديد هوية الشخص الموقّع.

٣- سلامة وأصلية التوقيع.

وفقاً للعديد من التشريعات فانه ثبت الاعتراف القانوني للتوقيع القانوني، وكذلك تم الاعتراف بالأثر القانوني للتوقيع القانوني من قبل الأمم المتحدة من خلال قانون الأونسيترال النموذجي بشأن التوقيع الإلكتروني في ٢٠٠١، كما تم الاعتراف بذلك الأثر وفقاً للقانون المصري رقم ١٥ لسنة ٢٠٠٤.

من المتفق عليه بشكل عام أنه يجب اعتبار التوقيعات الإلكترونية معادلة من الناحية الوظيفية للتوقيعات الأصلية والنسخ الأصلية، على الرغم من أنه يجب استيفاء شروط معينة لإنشاء توقيع إلكتروني موثوق. من الملاحظ أن الشرط الأول هو أن الطريقة المستخدمة يجب أن تكون قادرة على إثبات هوية الطرف وإشارة إلى نية الطرف، وفيما يتعلق بالشكل الصحيح للتوقيع ففي قانون الأونسيترال النموذجي بشأن

التجارة الإلكترونية، واتفاقية الأمم المتحدة للاتصال الإلكتروني في التعاقدات الدولية ١٧ ، فهما يشيران إلى عبارة "موافقة الطرف على المعلومات الواردة" ، وهو تحسن ملحوظ في أنه يؤكد هوية الطرف ونية الطرف للحصول على المعلومات، بينما يتطلب قانون الأونسيترال النموذجي للتوقيعات الإلكترونية "سلامة المعلومات التي تتعلق بها"١٨ .

قد توفر التشريعات الوطنية والإقليمية المزيد من القواعد المحددة لتحديد أن التوقيع الإلكتروني "موثوق به حسب الاقتضاء" على مختلف المستويات. على سبيل المثال، فإن توجيهات المفوضية الأوروبية بشأن التوقيعات الإلكترونية التي تخضع للمراجعة من قبل اللائحة المقترحة بشأن التعريف الإلكتروني وخدمة الثقة للمعاملات الإلكترونية تحتوي على أحكام ذات صلة بشأن إنشاء التوقيعات الإلكترونية المؤهلة التي يتم التحقق من صحة التوقيعات الإلكترونية المتقدمة من قبل الشهادات ذات الجودة المؤهلة ومقدمو خدمات التصديق المعتمدون وأجهزة إنشاء التوقيع الآمنة ١٩.

وفى قضايا محكمة العدل للاتحاد الأوربية، تم الاعتراف ضمنياً بالأثر القانوني للتعاقد عبر الإنترنت عبر موقع ويب تفاعلي، كما أن هناك قضايا قضائية وطنية تعترف بالآثار القانونية للتعاقد عبر الانترنت في الصين والولايات المتحدة.[٢٠]

[17] UN Convention on the Use of Electronic Communications on International Contracts 2005 (hereafter 'The UN Convention'), Article 9; see also Report of the Working Group on Electronic Commerce on the work of its 42nd session (Vienna, 17–21 November 2003) (A/CN.9/546), at pp. 54–7.

[18] See *UNCITRAL Guide to the Model Law of Electronic Commerce*, paras 52–61, in particular para 58; www.uncitral.org.

[19] EC Directive on Electronic Signatures 1999, Articles 2 and 5; see also COM (2012)238 final,
Articles 20 to 27.

[20] عادل رمضان الأبيوكى، التوقيع الإلكتروني في التشريعات الخليجية، دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، ٢٠٠٩،ص١

ففي الولايات المتحدة الأمريكية في القضية الرائدة لشركة Cloud Corporation ضد .Hasbro Inc.، كان هناك العديد من عمليات تبادل البريد الإلكتروني بين الأطراف التي تركز على تواريخ التسليم والكميات التي يتم وصفها بأنها "أكثر أو أقل اعتمادًا على الصيغة" ليتم تسليمها في تلك التواريخ. تم التأكيد على أن اسم المرسل الموجود في رسالة بريد إلكتروني يفي بمتطلبات التوقيع في قانون الاحتيال دون الحاجة إلى الاعتماد على القانون الفيدرالي (التوقيعات الإلكترونية في قانون التجارة الوطنية والعالمية٢١) .

في المقابل، في قضية ميهتا ضد JPF الإنجليزية الرائدة، توصلت المحكمة إلى استنتاج مختلف بشأن ما إذا كان البريد الإلكتروني يحمل التوقيع وفقًا لقانون الاحتيالات. والحقيقة هي أن السيد ميهتا كان مديرًا لشركة بيدكير (المملكة المتحدة) المحدودة. فشلت بيدكير في الدفع للمورد، جي بيريرا فيرناندير (JPF)، وانتهى الأمر في النهاية بناءً على عريضة مقدمة من .JPF كانت القضية تتعلق بالمدعى عليه السيد ميهتا الذي طلب من أحد موظفيه إرسال بريد إلكتروني إلى محامي JPF للحصول على ضمان شخصي. لم يتم توقيع البريد الإلكتروني من قبل السيد ميثا ولكن تم وصفه في العنوان بأنه وارد من .Nelmehta@aol.comالمسألتان الرئيسيتان في جلسة الاستئناف هما:

١- ما إذا كان البريد الإلكتروني يشكل ملاحظة أو مذكرة كافية للاتفاق المزعوم لأغراض القسم ٤ من قانون الاحتيال.

٢- بافتراض أن البريد الإلكتروني كان مذكرة، سواء كانت موقعة بشكل كاف من قبل أو نيابة عن السيد ميهتا، فقد تم الدفع نيابة عن JPF بأن وجود عنوان البريد الإلكتروني على نسخة البريد الإلكتروني الذي استلمه محامو JPF كان توقيعًا مناسبًا لهذه الأغراض .

٣- من الواضح أن النقاط المحورية هنا هي ما إذا كان البريد الإلكتروني عبارة عن مذكرة أو ملاحظة كافية، وما إذا كان عنوان البريد الإلكتروني الذي تم إدخاله تلقائيًا للمرسل يمكن أن يشكل توقيعًا. اعتبر القاضي "بيلينج كيو سي" أن البريد الإلكتروني كان بالفعل ملاحظة أو مذكرة، لأن البريد الإلكتروني كان مكتوبًا ولم يعترض السيد ميهتا على قبول العرض شفهيًا من قبل JPF. 65 نظرًا لأن اسم المدعى عليه أو الأحرف الأولى منه لم تكن كذلك تظهر في نهاية البريد الإلكتروني أو

[21] Cloud Corporation v. Hasbro. Inc., No. 02-1486, 314 F.3d 289 (the United States Court of Appeals for the Seventh Circuit, Dec. 26, 2002); see also Shattuck v. Klotzbach, No. 011109A, 2001 WL 1839720 (Mass. Super. Dec.11, 2001).

في نص البريد الإلكتروني ، اعتبر القاضي أن المسألة هنا تتعلق بما إذا كان قد تم توقيع مذكرة ، وليس بأي نية أو بأي صفة السيد "ميهتا" أو وقع أحد موظفيه على الوثيقة ذات الصلة.

٤- وهكذا خلص القاضي إلى أن وجود عنوان البريد الإلكتروني في أعلى البريد الإلكتروني لا يشكل توقيعًا، بعد حكم إيفانز ضد هور، الذي ينص على ما يلي: "ما إذا كان الاسم موجودًا في متن المذكرة، أو في البداية، أو في النهاية، إذا كانت النية للتوقيع، فهناك مذكرة اتفاق بالمعنى المقصود في النظام الأساسي. اعتبر القاضي إدراج عنوان بريد إلكتروني في مثل هذه الظروف كمثال واضح على الإدراج العرضي لاسم في حالة عدم وجود نية مخالفة. ومع ذلك، إذا قام طرف أو وكيل طرف بإرسال بريد إلكتروني بكتابة اسمه / اسمها أو اسم مديرها إلى الحد المطلوب أو المسموح به بموجب السوابق القضائية الموجودة في نص البريد الإلكتروني، فسيكون ذلك توقيعًا مناسبًا لأغراض القسم ٤ من قانون الاحتيال ٢٢.

٥- مع تقدم المجرمين (المهاجمين) باستخدام تقنيات المعلومات، ليس من السهل مراقبة وكشف رسائل البريد الإلكتروني الاحتيالية في نظام البريد الإلكتروني العادي. من الشائع أنه في حين قد يبدو البريد الإلكتروني شرعيًا، فيمكن تغيير وتبديل أي معلومات بهذا الميل، فلا يمكن لمستلمي البريد الإلكتروني الاعتماد فقط على عنوان البريد الإلكتروني الخاص بالمرسل للتحقق من المصدر الحقيقي للبريد الإلكتروني. وبالتالي فإن النقطة التي تمت مناقشتها حول ما إذا كان رأس البريد الإلكتروني يمكن أن يخول التوقيع يجب أن تركز على ما إذا كان نظام البريد الإلكتروني في مستوى ضمان أمان مناسب لضمان أن المرسل هو الذي أرسل البريد الإلكتروني، بدلاً من ذلك مما إذا كان عنوان البريد الإلكتروني نفسه يشكل توقيعًا. وبالتالي، فإن القلق بشأن التأثير القانوني للأسماء المكتوبة في رسائل البريد الإلكتروني يجب أن يركز أيضًا على أمان نظام البريد الإلكتروني، أي ما إذا كان نظام البريد الإلكتروني يستخدم بوابات أو طبقات آمنة مثل للتحقق من هوية البريد الإلكتروني البريد الإلكتروني للمستخدمين، بدلاً من الشكل المكتوب للأسماء المضمنة في البريد الإلكتروني.٢٣

[22] Mehta v. JPF [2006] EWHC 813 (Ch); [2006] 1 WLR 1543; [2006] 2 ALL ER 891, 7 April 2006

[23] ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، ٢٠٠٧، ص١٠٢

٦- إذا كانت أنظمة البريد الإلكتروني المستخدمة على مستوى أعلى من ضمان الأمان ولم يتم اختراقها، فلا شيء يمكن أن يقف في طريق الأسماء المكتوبة الواردة في مراسلات البريد الإلكتروني التي تشكل توقيعات صحيحة حيث توجد أدلة كافية على أن البريد الإلكتروني ينشأ من أصحاب الحساب أو المستخدمين المصرح لهم. ونتيجة لذلك، ليس من المناسب تحديد الفعالية بناءً على ما إذا كان الاسم المكتوب في الجزء السفلي من البريد الإلكتروني كتوقيع أو حتى توقيع آلي يقوم المستخدم بإنشائه في مربع ثابت باستخدام زر التوقيع في البريد الإلكتروني نظام البريد، وبالتالي، فإن مستوى الأمان الذي توفره الطريقة المستخدمة يعد حيويًا لتحديد الأثر القانوني لشكل توقيع صالح في رسائل البريد الإلكتروني. هناك مسألة أخرى تتعلق بالأمان تحتاج إلى توضيحها وهي التفاعلات بين المشاركين عندما يكون هناك عامل مشترك.

٧- على سبيل المثال، تخيل سيناريو يتضمن مستخدمًا (بصفته مديرًا) ووكيلًا إلكترونيًا (بصفته وكيلًا) ومستخدمًا آخر (كطرف ثالث): يستخدم المستخدم الوكيل الإلكتروني كوكيله الخاص للتعاقد، ويدخل الطرف الثالث في تفاعل يهدف إلى العقد مع الوكيل، دون معرفة من (ماذا) يقف وراء هذا الأخير. لا أحد من المستخدمين يعرف مع من يتفاعل وكيله. الرابط الوحيد بينهما هو الوكيل. وبالتالي، إذا حدث خطأ ما، فلن يتمكن الطرف الثالث من مخاطبة المستخدم مباشرة، لأن الوكيل الإلكتروني لم يقدم تعريفًا للمستخدم. يمكن حل هذه المشكلة إذا قدر المستخدم أفعال الوكيل، وبهذه الطريقة قدم تعريفه للطرف الثالث. حل آخر، من أجل زيادة الثقة في استخدام الذكاء الاصطناعي، يمكن أن يكون اعتماد وكالة: إذا كان لدى الطرف الثالث سبب معقول للاعتقاد بأن الوكيل تصرف نيابة عن المدير، فإن المدير سيكون هو المسئول وسوف يكون هناك حاجة متزايدة ٢٤، لتوضيح هذه القضايا في المراجعات التشريعية والتفسيرات القضائية.

المطلب الثاني

مصادقة التوقيع الإلكتروني

[24] EU Commission Legal-IST Project, 'Report on Legal Issues of Software Agents', p. 64

أولاً–تعريف المصادقة:

في البيئة التقليدية، ليس للمصادقة والتوقيع نفس المعنى في النظم القانونية المختلفة وبشكل عام، تُعرف المصادقة بمستند أو دليل يربط بشخص أو مكان أو شيء، في حين يعتبر التوقيع "أي اسم أو رمز يستخدمه الطرف بنية تشكيله كتوقيع له". في معظم الولايات القضائية للقانون المدني، تُفهم المصادقة في نطاق ضيق وبطريقة صارمة على أنها أصالة مستند تم التحقق منه والمصادقة عليه من قبل سلطة عامة مختصة أو كاتب عدل.٢٥

تم اقتراح تعريف رسمي لـ "المصادقة" في اقتراح المفوضية الأوروبية بشأن لائحة التعريف الإلكتروني وخدمات الثقة للمعاملات الإلكترونية في السوق الداخلية في عام ٢٠١٢ على النحو التالي:

عملية إلكترونية تتيح التحقق من الهوية الإلكترونية لشخص طبيعي أو اعتباري؛ أو من أصل وسلامة البيانات الإلكترونية.٢٦

في عام ٢٠١٣، يعرّف الدليل الإلكتروني للمصادقة الإلكترونية الذي اقترحته وزارة التجارة الأمريكية "المصادقة" بأنه "عملية إثبات الثقة في هوية المستخدمين أو نظم المعلومات"، و "المصادقة الإلكترونية" على أنها "عملية إنشاء الثقة في هوية المستخدم تقدم إلكترونيا لنظام المعلومات.

[25] United Nations Commission on International Trade Law (UNCITRAL), Fortieth Session, Possible future work on electronic commerce, Comprehensive reference document on elements required to establish a favorable legal framework for electronic commerce: sample chapter on international use of electronic authentication and signature methods, Vienna, 25 June – 12 July 2007, A/CN.9/630, p. 4.

[26] عبد الحكيم زروق، تنظيم التبادل التجاري، تنظيم التبادل الإلكتروني للمعطيات القانونية عبر الإنترنت، منشورات دار الأورمان، الطبعة الأولى، الرباط، ٢٠١٦، ص٢٣٤

يشار إلى أن مفهوم "المصادقة الإلكترونية" يختلف عن "التعريف الإلكتروني". يشير مصطلح "التعريف الإلكتروني" إلى "عملية استخدام بيانات تعريف الشخص في شكل إلكتروني تمثل بشكل لا لبس فيه شخص طبيعي أو اعتباري". من وجهة النظر التكنولوجية، يمكن وصف المصادقة الإلكترونية بأنها العملية التي يتم من خلالها التحقق من هوية الكمبيوتر أو مستخدم الشبكة. من وجهة نظر وظيفية، تضمن المصادقة أن الفرد، في الواقع، هو من يدعي أنه. بشكل عام، لا ينبغي اعتبار المصادقة الإلكترونية مجرد "عملية إلكترونية" ولكن أيضًا "وسيلة" لتوفير التجارة الإلكترونية الجديرة بالثقة أو خدمة التسليم الإلكتروني، والتي تستخدم لحماية مستند إلكتروني من التعديلات غير المكتشفة، لتوفير معلومات محدودة، ولكن موثوقة، حول شخص ما، ولتوقيع توقيع في بيئة إلكترونية، لا سيما الموقع الذي يشير إلى الموافقة على الوثائق الموقعة. على عكس المصادقة الإلكترونية، تركز التوقيعات الإلكترونية بشكل خاص على التحقق من هوية المالكين والتعامل مع مشكلة إسناد المستندات، بينما تتعامل المصادقة الإلكترونية مع مشكلة موثوقية تشفير المفتاح (أي المفتاح العام والمفتاح الخاص).٢٧

تُعرف "الشهادة" بأنها "شهادة إلكترونية تربط بين التوقيع الإلكتروني أو بيانات التحقق من صحة ختم الشخص الطبيعي أو الاعتباري على التوالي بالشهادة وتؤكد تلك البيانات الخاصة بهذا الشخص". يمكن لشهادات التوقيع الإلكتروني أن تجمع بين وظائف التوقيع والمصادقة، لأن هذا النوع من التصديق يتطلب أن "الشخص الذي تم التوقيع عليه قد أدلى ببيان يثبت أن التوقيع أو وسيلة لإنتاج التوقيع أو التواصل أو التحقق منه، أو إجراء المطبق على التوقيع هو وسيلة صالحة لإثبات صحة أو سلامة الاتصال أو البيانات أو كليهما.٢٨

[27] Promoting Confidence in Electronic Commerce: legal issues on international use of electronic authentication and signature methods, the United Nations Commission on International Trade Law (UNCITRAL), Vienna, United Nations, 2007 (released in 2009). Available at: http://www. uncitral.org/pdf/English/texts/electcom/08-55698_Ebook.pdf (last accessed 30 June 2013).

[28] نسرين عبد الحميد نبيه، الجانب الإلكتروني للقانون التجاري، نشر بمنشأة المعارف، الطبعة الأولى، الإسكندرية، ٢٠٠٨، ص٤٢٤

في لائحة اقتراح المفوضية الأوروبية بشأن التعريف الإلكتروني وخدمات الثقة للمعاملات الإلكترونية في السوق الداخلية، تم تقديم مفهوم جديد لـ "الختم الإلكتروني" ، وهو ما يعني " البيانات في شكل إلكتروني مرتبطة أو مرتبطة منطقيًا ببيانات إلكترونية أخرى إلى ضمان أصل وسلامة البيانات المرتبطة. تم التأكيد على أن وظائف الأختام الإلكترونية هي "كدليل على أن المستند الإلكتروني صادر عن شخص اعتباري، مما يضمن اليقين من أصل الوثيقة وسلامتها و" المصادقة على أي أصل رقمي للشخص الاعتباري ". هذا التعريف غير واضح من حيث العلاقة بين الأختام الإلكترونية والمصادقة الإلكتروني، كما يبدو أنه من المنطقي أن نفهم أن الختم الإلكتروني هو منتج (مثل ختم) ناتج عن فعل المصادقة الإلكترونية لتوقيع أو لسجل إلكتروني.

ثانياً–سلطات التصديق (الطرف الثالث):

هي جهة خارجية أو كيان موثوق به يتحقق من هوية شخص، يسمى مشتركًا، ويشهد بأن المفتاح العام أو زوج من المفاتيح العامة والخاصة يستخدم لإنشاء توقيعات رقمية ينتمي إلى ذلك الشخص. يُعرف "المرجع المصدق" أيضًا باسم "مقدم خدمة التصديق" و "مزود خدمة الثقة" في الاتحاد الأوروبي و "مزود خدمة التحقق الإلكتروني" في الصين.

يوفر طريقة للتأكد من أن المفتاح العام ينتمي إلى المالك المطالب به بطريقة مستقلة. في الولايات المتحدة، تحدد إرشادات المصادقة الإلكترونية التي اقترحتها وزارة التجارة الأمريكية في عام ٢٠١٣ المرجع المصدق على أنها "كيان موثوق به يصدر شهادات المفتاح العام ويلغيها" من منظور تقني، أي أن المرجع المصدق يقوم بذلك عن طريق إصدار أو إلغاء شهادة رقمية، والتي تربط الفرد بمفتاح تشفير عام معين. تحتوي الشهادة على المفتاح العام واسم الموقِّع، الموقعين رقميًا من قبل المرجع المصدق. أي، لربط زوج مفتاح مع مُوقِّع محتمل، يصدر المرجع المصدق شهادة رقمية، وهي عبارة عن سجل إلكتروني يضمن أن المُوقِّع المُحدد المُعرَّف في الشهادة يحمل المفتاح الخاص المقابل.٢٩

٢٩) التوقيع الإلكتروني في التشريعات الخليجية، دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، ٢٠٠٩، ص٨٦. عادل رمضان الأبيوكى،

والوظيفة الرئيسية للشهادة هي ربط زوج مفتاح بمشترك معين، ويمكن لـ "مستلم" الشهادة استخدام المفتاح العمومي المدرج في الشهادة للتحقق مما إذا كان التوقيع الرقمي قد تم إنشاؤه من قبل الموقّع المحتمل الذي يحمل المفتاح الخاص المقابل.٣٠

من الجدير بالملاحظة أن طرفًا ثالثًا موثوقًا به مثل CA يمكنه لعب دور كوكي، فعلى سبيل المثال، يمكّن PayPal ٣١أي فرد أو شركة لديها عنوان بريد إلكتروني من إرسال المدفوعات واستلامها عبر الإنترنت بشكل آمن وسهل وسريع. يحتاج العملاء الذين يسجلون في PayPal فقط إلى تقديم معلومات حسابهم مرة واحدة. ثم يتم تخزينه على خادم آمن ومشفّر للغاية. عند شراء شيء ما باستخدامPayPal ، يقوم المستخدمون ببساطة بإجراء التحويل من خلال حساباتهم على PayPal بدلاً من بطاقة الائتمان. تعتبر هذه الطريقة أكثر أمناً وأماناً وملاءمة من توفير المعلومات المالية لمواقع متعددة للبائعين الأفراد.

يتم إنشاء المرجع المصدق بواسطة كيان عام أو شخص اعتباري أو طبيعي. يعترف كل من الاتحاد الأوروبي والولايات المتحدة والصين بهذا الشكل من التأسيس في تشريعاتها ذات الصلة. على سبيل المثال، ينص توجيه المفوضية الأوروبية بشأن التوقيعات الإلكترونية صراحةً على ما يلي٣٢:

١- يمكن تقديم خدمات التصديق إما من قبل كيان عام أو شخص اعتباري أو طبيعي، عندما يتم تأسيسها وفقًا للقانون الوطني؛ في حين لا ينبغي للدول الأعضاء أن تمنع مقدمي خدمات التصديق من العمل خارج خطط الاعتماد الطوعية؛ يجب التأكد من أن خطط الاعتماد هذه لا تقلل من التنافس على خدمات التصديق.

٢- المرجع المصدق مسؤول عن عملية التصديق التي قد تتفاعل مع مزود خدمة الاعتماد في عملية المصادقة. تبدأ عملية المصادقة بإثبات المدّعي امتلاك والتحكم في رمز مميز مرتبط بالهوية المزعومة إلى المحقق من خلال بروتوكول المصادقة. بمجرد إثبات الحيازة والتحكم، يتحقق التحقق

[30] D. I. Bainbridge (2008) Introduction to Information Technology Law, 6th edn (Harlow: Pearson Longman), pp. 360–1.

[31] See PayPal at: https://www.paypal.com/uk/webapps/mpp/home (last accessed 30 June 2013).

[32] Selected Bibliography on Description of Digital Signatures, Appendix 6 on 'The Role of Certification Authorities in Consumer Transactions' prepared by the Internet Law and Policy Forum. Available at: http://www.ilpf.org/groups/ca/app6.htm (last accessed 30 June 2013).

من صحة بيانات الاعتماد، عادة من خلال التفاعل مع وبمجرد تأكيد دقة الشهادة، يمكن نشر الشهادة لإتاحتها لأطراف ثالثة ترغب في الاتصال بالمدّعي.

هناك العديد من أشكال المرجع المصدق المتاحة في السوق الإلكترونية.) تسمى "سلطات التصديق المعترف بها "، والمعروفة باسم "مقدمي الخدمات الموثوقة " أو "مقدمي خدمات التصديق المعتمدين" في الاتحاد الأوروبي وبعض كيانات التصديق الأخرى ، تعمل بموجب شكل من الترخيص أو الاعتماد الطوعي تسمى "نظام الاعتراف الطوعي لسلطات التصديق". ولكن لا يوجد توحيد موحد فيما يتعلق بهذه الأشكال من تلك المراجع في أوائل العقد الأول من القرن الحادي والعشرين.

وقد فرضت بعض البلدان نظام تسجيل إلزامي على جميع المراجع المصدقة، ولكن في السنوات الأخيرة اعتمدت معظم البلدان مثل الاتحاد الأوروبي والولايات المتحدة والصين نظامًا للاعتراف الطوعي، وهو أن للمراجع حق التقدم بطلب للحصول على الاعتراف على أساس طوعي ولكن فقط تلك المراجع التي حققت معايير موضوعية معينة سيتم "الاعتراف بها" أو "مؤهلة". وقد حثت اللائحة المقترحة من قبل المفوضية الأوروبية بشأن التعريف الإلكتروني وخدمات الثقة للمعاملات الإلكترونية في السوق الداخلية كل دولة عضو على إنشاء قوائم موثوقة مع المعلومات والحفاظ عليها ونشرها فيما يتعلق بمزودي الخدمات الموثوقة المؤهلين. وفي الولايات المتحدة، يمكن أن تشمل المراجع المصدقة كيانات حكومية اتحادية وحكومية، أو أشخاصًا أو كيانات خاصة مرخص لها بالعمل كسلطات مصدق عليها من قبل الدولة، وأشخاص أو كيانات خاصة تعمل كسلطات مصادقة لأغراض تجارية.

على سبيل المثال، تقدم الشركات الخاصة مثل GlobalSign وVeriSign، Inc. الشهادات والخدمات الرقمية ذات الصلة إلى الأشخاص الطبيعيين والاعتباريين. في فبراير ٢٠١٣، تم أيضًا إنشاء مجلس أمن سلطة التصديق، وهو مجموعة مناصرة، في الولايات المتحدة لاستكشاف وتعزيز أفضل الممارسات التي تعزز أمن مواقع الويب والمعاملات عبر الإنترنت.٣٣

[33] Electronic Authentication Guideline, February 2013, NIST, US Department of Commerce (800-63-2), p. 8. A Credential Service Provider (CSP) is 'a trusted entity that issues or registers Subscriber tokens and issues electronic credentials to Subscribers. The CSP may encompass Registration Authorities (RAs) and Verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use

بشكل عام، يحتاج المرجع المصدق إلى الامتثال لمجموعة من المتطلبات ليتم منحه ترخيصًا أو معتمدًا أو مؤهلا تشمل الشروط الشائعة المعايير المالية والفنية (مثل المؤهلات، وإدارة الأجهزة، وظروف البرمجيات)، والموظفين الأكفاء ذوي الخبرة، وإجراءات الإدارة المناسبة والقدرة على إدارة المخاطر والتعويض. كان قانون "توقيع يوتا " الرقمي أول تشريع يضع شروطًا لإنشاء مراجع التصديق في عام ١٩٩٥، وقد اعتمدت الأونسيترال والاتحاد الأوروبي والصين أيضًا أحكامًا ذات صلة بشأن متطلبات إنشاء مقدمي خدمات موثوقين أو مؤهلين للثقة. وهي المادة ١٠ من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام ٢٠٠١، والملحق الثاني من توجيهات المفوضية الأوروبية بشأن التوقيعات الإلكترونية والمادة ١٧ من قانون التوقيعات الإلكترونية في الصين. كما قامت الصين بإصدار إجراءات وإشعارات محلية إلى تحقيق أفضل ممارسات المصادقة الإلكترونية للمعاملات الإلكترونية في مختلف القطاعات بما في ذلك قطاع الصحة وصناعة المعلومات. على سبيل المثال، أصدرت وزارة الصناعة وتكنولوجيا المعلومات في جمهورية الصين الشعبية تدابير لإدارة الشهادات الإلكترونية لعام ٢٠٠٩ وفقًا لقانون التوقيعات الإلكتروني الصيني والقوانين الأخرى ذات الصلة لتنظيم خدمات التصديق الإلكتروني والإشراف على التصديق الإلكتروني مقدمي الخدمة. ٣٤

وتقترح المادة ١٩ من اللائحة المقترحة من المفوضية الأوروبية بشأن التعريف الإلكتروني وخدمات الثقة للمعاملات الإلكترونية في السوق الداخلية متطلبات تفصيلية لمقدمي خدمات الثقة الموثوقين بما في ذلك الوسائل المناسبة للتحقق والموظفين الأكفاء والموارد المالية الكافية لتحمل المسؤولية عن المخاطر والشروط والأحكام الدقيقة الخدمة والأنظمة والمنتجات الموثوقة للأمان وتخزين البيانات، وإجراءات التزوير وسرقة البيانات.

بالإضافة إلى ذلك، من الشائع أيضًا أن القوانين الوطنية والإقليمية قد تفرض واجب الإخطار على مقدمي الخدمات الموثوقة عن أي خرق للأمن وفقدان تكامل البيانات. أي أنه يجب على مقدمي الخدمات

---

[34] Certificate Authority Security Council. Available at: https://casecurity.org/ (last accessed 30 June 2013).

الاستئمانية إبلاغ الهيئة الإشرافية المختصة عن أي خرق دون تأخير لا مبرر له، علاوة على ذلك، غالبًا ما يكون على مقدمي الخدمات واجب التصرف في ظروف معينة بهدف منع أو وقف الأنشطة غير القانونية.٣٥

ثالثاً–المسؤولية:

إن المبادئ المتعلقة بمسؤولية مقدمي الخدمات الموثوقة محددة في المادة ٦ من توجيه المفوضية الأوروبية بشأن التوقيعات الإلكترونية، يضع نظامين مختلفين للمسئولية، والذي سيتم تطبيقه اعتمادًا على نوع الشهادة. بالنسبة للشهادات المؤهلة، تم تنسيق مسؤولية سلطة إصدار الشهادات تجاه الأطراف الثالثة من خلال فرض معايير دنيا، وستخضع جميع الشهادات، التي تشمل الشهادات غير المؤهلة، لقواعد وطنية تتعلق بالمسؤولية كما هي الآن.[٣٦]

في عام ٢٠١٢، اقترحت المادة ٩ من اللائحة المقترحة من المفوضية الأوروبية بشأن التعريف الإلكتروني والخدمات الاستئمانية للمعاملات الإلكترونية في السوق الداخلية توفير المسؤولية لمزود الخدمة الاستئمانية على النحو التالي:

١- يكون مقدم الخدمة الاستئمانية مسؤولاً عن أي ضرر مباشر يحدث لأي شخص طبيعي أو اعتباري بسبب عدم الامتثال للالتزامات المنصوص عليها في المادة ١٥ (١)، ما لم يثبت مقدم الخدمة الاستئمانية أنه لم يتصرف بإهمال.

٢- يتحمل مقدم خدمة الثقة المؤهلة المسؤولية عن أي ضرر مباشر يحدث لأي شخص طبيعي أو اعتباري بسبب عدم استيفاء الشروط المنصوص عليها في هذه اللائحة، ولا سيما في المادة ١٩، ما لم يتمكن مقدم خدمة الثقة الموثوقة من إثبات أنه لم يتصرف بإهمال.

التوقيع الإلكتروني في التشريعات الخليجية، دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، [35] عادل رمضان الأبيوكى، ٢٠٠٩،ص١١٥.

[36] Measures for the Administration of Electronic Certification Services 2009, Article 1. 109 COM (2012) 238, final, Brussels 4 June 2012, Article 19(1) (2).

هذا الحكم المقترح بشأن مسؤولية مقدمي خدمات الثقة مطابق للمادة ٦ من توجيه المفوضية الأوروبية بشأن التوقيعات الإلكترونية من حيث تحديد الحد الأدنى للمعيار. توضح صياغة هذا الحكم المقترح أن من الواضح أن هذه المسؤولية تنطبق على كل من مقدمي الخدمات الموثوقة "غير المؤهلين" و "المؤهلين" للضرر "المباشر" فقط ما لم يتمكن مقدمو الخدمات الموثوقون من إثبات أنهم لم يتصرفوا بإهمال. وتتناول ثلاث قضايا:

– يجب أن يخضع مقدمو الخدمات الاستئمانية غير المؤهلين والغير مؤهلين لمعايير المسؤولية.

– يجب أن يكون مقدمو الخدمات الموثوق بهم مسؤولين فقط عن الضرر "المباشر" الذي يحدث.

– يجب أن يتحمل مقدمو خدمات الثقة عبء الإثبات.

يبدو أن القاعدة الجديدة المقترحة من المفوضية الأوروبية بشأن الضرر "المباشر" هي تحقيق توازن بين المصالح والحقوق بين الأطراف المختلفة.

في الصين، يوفر قانون التوقيعات الإلكترونية في الصين أيضًا الأحكام ذات الصلة (المواد ٢٧–٣٣)[٣٧] بشأن مسؤولية مقدم الخدمة عن الضرر الذي يلحق بأي شخص طبيعي أو اعتباري يعتمد على التوقيع الإلكتروني الصادر ما لم يتمكن مقدم الخدمة من إثبات ذلك ليس لديه خطأ.

هناك شيء مشترك في تشريعات الاتحاد الأوروبي والصين فيما يتعلق بمسؤولية مقدم خدمة الثقة وهو أن مقدم خدمة الثقة يجب أن يكون مسؤولاً عن الأفعال المهملة. عادة ما تكون الأفعال الإهمال التالية بمثابة مسؤولية مقدم خدمة الثقة:[٣٨]

١–عدم أخذ الأدلة المناسبة لهوية صاحب التسجيل.

٢–عدم الاحتفاظ بالسجلات المناسبة، ومنع إصدار الشهادات المزورة وإلغاء الشهادات.

[37] China Electronic Signatures Law 2004, Articles 27–33.

[38] د/محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، الإسكندرية، ٢٠١٠، ص٢٧٧.

٣- عدم قيام الموظفين بتضمين سجلات موثوق بها في الشهادات.

٤- عدم سحب الشهادة بعد علمها بالخطأ.

والسؤال الذي يثور هو كيف يمكن إعفاء مقدم خدمة الثقة من المسؤولية تجاه طرف ثالث. يمكن انتهاك عقد الخدمة الذي يقدمه موفر خدمة الثقة بفعل إهمال من موفر خدمة الثقة الذي يؤثر على طرف ثالث يعتمد على شهادة غير صحيحة، فمن المسلم به عمومًا أنه إذا تكبد أي طرف ثالث أي خسارة بعد الدخول في علاقة تجارية مع طرف بناءً على اعتماد شهادة غير صحيحة صادرة عن مرجع مصدق، فقد يتم إهمال المرجع المصدق بسبب أنه فشل في التحقيق بدقة قبل إصدار الشهادة، ومسؤولة تجاه الطرف الذي يعتمد على هذه الشهادة بموجب قانون الالتزامات، أي أنه يمكن للطرفين رفع دعوى قضائية إما لخرق العقد أو الإهمال في الضرر. في مثل هذه الحالات، ستكون هناك مسؤولية متزامنة في العقد وفي الضرر الناتج عن خرق إهمال للعقد.

عندما يتداخل واجب الرعاية التعاقدي مع واجب رعاية مماثل جوهريًا يفرضه الإهمال، يمكن للمدّعي أن يختار أيًا كان سبب الدعوى الذي يفضّله، أو يترافع كليهما.

وهذا يعني أن الضرر وإخلال العقد خطأ مدني في العقد، يتم إنشاء الالتزامات وتحديدها بشكل عام من قبل الأطراف (وليس المحاكم)، أي أن الأطراف لديها خيار فيما يتعلق بالتزاماتها القانونية بموجب هذا العقد. في المقابل، يُرتكب الضرر عندما يفشل الفرد في تنفيذ أفعاله وفقًا للمعيار الذي ينص عليه القانون، وفي الضرر تفرض المحاكم واجب التصرف "بشكل معقول" وستعوض المحاكم الطرف المتضرر عن الخسارة التي تكبدها بسبب عدم تصرف الطرف الآخر وفقًا لهذا المعيار.

في قانون العقود، فإن الطرف الذي يعتمد على شهادة غير صحيحة، المعروفة باسم "طرف ثالث" أو "الطرف المعوّل"، ويكون ضحية خسارة مالية لن يكون قادراً إلا على رفع دعوى قضائية ضد خرق العقد إذا كان ينص عقد خدمة التصديق بين المرجع المصدق والطرف صراحة على أنه يجوز للطرف الثالث تطبيقه عندما تهدف فترة ما إلى منحه فائدة. إذا لم يكن الأمر كذلك، فلن تكون هناك علاقة تعاقدية بين المرجع المصدق والطرف المعول (طرف ثالث). كونه خارج المجال التعاقدي، سيتعين على الطرف الرد أن يثبت مسؤولية

المرجع المصدق على أساس ملتوي، وفي كثير من الأحيان، قد يُعتبر المرجع المصدق مسؤولًا بشكل جسيم إذا كان عليه واجب العناية بتقديم بيانات دقيقة.[٣٩]

من ناحية أخرى، يجب على الطرف المعوّل أيضًا اتخاذ خطوات معقولة للتحقق من موثوقية التوقيع الإلكتروني، فعلى سبيل المثال، تنص المادة ١١ من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية على أن "يتحمل الطرف المعول النتائج القانونية المترتبة على إخفاقه" في اتخاذ خطوات معقولة للتحقق من موثوقية التوقيع الإلكتروني وصحة أو تعليق أو إبطال الشهادة، ومراعاة أي قيد فيما يتعلق بالشهادة. مع مراعاة الصعوبة التي يوجهها طرف ثالث لإثبات إهمال مقدمي خدمة التوثيق بسبب تعقيدات العملية التقنية المعنية، يجب أن تكون المسؤولية الصارمة قابلة للتطبيق على مقدمي الخدمة ويجب أن يتحمل مقدمو الخدمة عبء الإثبات في المسؤولية التعاقدية أو المتوترة. يجب الاعتراف بأن المرجع المصدق يجب أن يكون مسؤولًا تمامًا تجاه أي طرف ثالث عن الفشل في الكشف عن أخطاء الطرف وله واجبات لإثبات انتهاك العقد أو الإهمال في الإجراءات.[٤٠]

وبالتالي من الواضح أنه من مصلحة مقدمي خدمة التوثيق أن تحدد أو تستثني مسؤوليتها، لكيلا تعرض للخطر جدوى صناعة تقديم خدمة التوثيق، ومن الأهمية بمكان أن مقدم الخدمة لا ينبغي أن تكون مسؤولة إذا تصرفت بشكل معقول. لن يكون المرجع المصدق "مسؤولاً عن الضرر الناتج عن تجاوز هذا الحد الأقصى"، إذا كان المشترك قد تكبد خسارة مالية بسبب محتال، فسيميل إلى محاولة مقاضاة المرجع المصدق إذا لم يكن من الممكن تحديد مكان المحتال أو كان معسرًا.

ومن غير المألوف أن العديد من مقدمو الخدمة قد حاولوا تحديد نطاق مسؤوليتهم وتحديدها عند إصدار الشهادات في وثائقهم الخاصة. ففي الولايات المتحدة، فإن المستندات التي تحدد معايير ممارساتها الجيدة ومسؤولياتها هي بيان "ممارسة الشهادة "، وهو عبارة عن "بيان بالممارسات التي يستخدمها مقدمو خدمة

[39] أ/ عبد الملك العياضى، آثار التوقيع الإلكتروني، جامعة الملك سعود، ٢٠١٢، ص١٢٧.

[40] s. Hindelang (2002) 'No remedy for disappointed trust – the liability regime for certification authorities towards third parties

التوثيق في إصدار الشهادات"، واتفاقية الطرف المعتمد، وهو ما "يخطر الطرف المعتمد بالضمانات وبإخلاء المسؤولية وتحديد فئات الشهادات وحدود المسؤولية وحدود الأضرار السارية على الشهادة الصادرة".[٤١]

وفي عام ١٩٩٧، اقترح أن حلاً آخر، لم يتم استكشافه بعد، لتجنب المسؤولية الجسيمة سيكون في سوق التأمين لنشر المخاطر والتكاليف في جميع الجهات ذات الصلة في الصناعة بأكملها. ففي السنوات الأخيرة، أصبح التأمين السيبراني أكثر شيوعًا للأفراد والشركات لتقليل مخاطر سرقة البيانات وفقدانها وتظهر منتجات التأمين السيبراني بشكل متزايد أي Cybersecurity بواسطة شركة (ChubbSM)ويتم تقديمها للمستهلكين والشركات التي تعتمد بشكل كبير على البيانات في أنظمة التجارة الإلكترونية في السوق.

من الجدير بالذكر أن هناك مناهج مختلفة في تشريعات الاتحاد الأوروبي والولايات المتحدة والصين، حيث تتمتع صناعة المعلومات في إطار مجلس الدولة على أساس الاتفاقات ذات الصلة أو مبدأ المعاملة بالمثل، وشهادات التوقيعات الإلكترونية الصادرة عن خدمات التحقق الإلكترونية الخارجية خارج أراضي جمهورية الصين الشعبية لها قوة قانونية متساوية مع تلك الصادرة عن خدمات التحقق الإلكترونية المنشأة بموجب هذا القانون[٤٢].

في الولايات المتحدة، صمت قانون التوقيع الإلكتروني القسم ٣٠١ (أ) (١) بشأن الاعتراف بالشهادات الأجنبية ولكنه يشجع بشكل عام على الاعتراف الدولي بالتوقيعات الإلكترونية:

يشجع وزير التجارة على قبول واستخدام التوقيعات الإلكترونية، على أساس دولي، وفقًا للمبادئ المحددة في الفقرة (٢) وبطريقة تتفق مع القسم من هذا القانون، يتخذ وزير التجارة جميع الإجراءات اللازمة بطريقة تتسق

[41] M. J. Ostey and M. Pulcanio (1999) 'The liability of certification authorities to relying third parties', John Marshall Journal of Computer and Information Law, 17 (3): 961.

٤٢) ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، ٢٠٠٧،

[42] ص١٤٥

مع هذه المبادئ لإزالة أو الحد من معوقات التجارة في التوقيعات الإلكترونية، إلى أقصى حد ممكن، بغرض تسهيل تنمية التجارة بين الولايات والتجارة الخارجية.

في منظمة دولية مثل الأونسيترال، المادة ١٢ من القانون النموذجي بشأن التوقيعات الإلكترونية تعزز أيضًا الاعتراف الدولي بالشهادات والمواصفات الأجنبية التي:

١-عند تحديد ما إذا كانت شهادة أو توقيع إلكتروني فعالاً من الناحية القانونية، أو إلى أي مدى، لا يُراعى ما يلي:

(أ) إلى الموقع الجغرافي الذي صدرت فيه الشهادة أو تم فيه إنشاء التوقيع الإلكتروني أو استخدامه.

(ب) الموقع الجغرافي لمقر عمل المصدر أو المُوقِّع.

٢-يكون للشهادة الصادرة خارج [الدولة المشترعة] الأثر القانوني نفسه في [الدولة المشترعة] للشهادة الصادرة في [الدولة المشترعة] إذا قدّمت مستوى موثوقا من المعادلة إلى حد كبير.

٣-يكون للتوقيع الإلكتروني الذي يتم إنشاؤه أو استخدامه خارج [الدولة المشترعة] الأثر القانوني نفسه في [الدولة المشترعة] للتوقيع الإلكتروني الذي يتم إنشاؤه أو استخدامه في [الدولة المشترعة] إذا كان يوفر مستوى موثوقا من المعادلة إلى حد كبير.

وتجدر الإشارة إلى أن المادة ١٢ من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية تعترف صراحة بالشهادات والتوقيعات الأجنبية دون تمييز جغرافي، وتنص على "مستوى معادل إلى حد كبير من الموثوقية" باعتباره الاختبار الرئيسي للاعتراف بالشهادات الأجنبية والتوقيعات الإلكترونية. كما أنه يوفر قابلية المعيار من خلال إدخال مبدأ حرية الأطراف في المادة ١٢ (٥). ويعبر عن أنه في حالة موافقة الأطراف على استخدام أنواع معينة من التوقيع الإلكتروني أو الشروط، يجب الاعتراف بهذا الاتفاق على أنه

مناسب لأغراض الاعتراف عبر الحدود، ما لم يكن هذا الاتفاق غير صالح أو فعال بموجب القانون المعمول به[٤٣].

إن قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، في جوهره، ليس مصمماً لإيجاد قواعد موحدة ملزمة على قدم المساواة في جميع أنحاء العالم ولكنه يساعد على مواءمة المعايير القانونية مع المفاهيم المنطقية فوق الوطنية. وفي الوقت نفسه، تترك مساحة كافية للدول لإضافة قواعد خاصة أو مرغوبة لنظامها القانوني. بالإضافة إلى ذلك، فإنه يسهل المزيد من الإصلاح القانوني على المستوى العالمي. طريقة وضع القانون هذه، من القوانين النموذجية الدولية إلى التشريعات الوطنية، "قد تمهد الطريق أيضًا للطرق فوق الوطنية لتطبيق هذه القواعد القانونية الجديدة للتجارة الإلكترونية بطريقة موحدة أو منسقة على الرغم من التقاليد القانونية المختلفة.

تؤكد المذكرة التفسيرية لاتفاقية الأمم المتحدة بشأن استخدام الاتصالات الإلكترونية في العقد الدولي لعام ٢٠٠٧ مبدأ "التكافؤ الوظيفي" الذي لا ينبغي أن يكون مكان منشأ التوقيع الإلكتروني، في حد ذاته، عاملاً يحدد بأي شكل من الأشكال ما إذا كان يجب الاعتراف بالشهادات الأجنبية أو التوقيعات الإلكترونية وإلى أي مدى يمكن أن تكون فعالة من الناحية القانونية في الدولة المتعاقدة[٤٤].

لا شك في أن الصكوك الدولية مثل قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية واتفاقية الأمم المتحدة بشأن استخدام الاتصالات الإلكترونية في العقود الدولية مهمة لتشجيع المعاملات التجارية

[43] Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market, COM (2008) 798 final of 28.11.2008; Digital Agenda for Europe, COM (2010) 245 of 19.05.2010; and the Proposal for a Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, COM (2012) 238 final of 04.06.2012.

[44] W. J. Craig, Hague Conference on E-Commerce Law, Introductory and Background Issues, Hague E-Commerce Conference, 26–27 October 2004. Available at: http://hcch. e-vision.nl/upload/wop/e-comm_craig.pdf (last accessed 30 June 2013).

الإلكترونية عبر الوطنية وبناء الثقة من خلال اليقين القانوني. يجب أن تأخذ الصكوك التشريعية الدولية في الاعتبار عدم وجود معايير تقنية دولية مشتركة، والوجود المستمر لتهديدات الأمن والاحتيال وكذلك عدم وجود قاعدة قانونية مشتركة فيما يتعلق بالمعاملات العابرة للحدود. المعاملات عبر الحدود، يصبح التنسيق الدولي للتشريعات أكثر أهمية. [٤٥]

ولتيسير التنسيق الدولي، ولا سيما الاعتراف القانوني بالشهادات الأجنبية والتوقيعات الإلكترونية، طالبت اتفاقية الأونسيترال مواصلة النظر في هذه القضايا. وقد صدر تقرير الأونسيترال في فبراير لعام ٢٠٠٧ بشأن تعزيز الثقة في التجارة الإلكترونية، بتمتع صناعة المعلومات في إطار مجلس الدولة على أساس الاتفاقات ذات الصلة أو مبدأ المعاملة بالمثل، وشهادات التوقيعات الإلكترونية الصادرة عن خدمات التحقق الإلكترونية الخارجية خارج أراضي جمهورية الصين الشعبية لها قوة قانونية متساوية مع تلك الصادرة عن خدمات التحقق الإلكترونية المنشأة بموجب هذا القانون.

تنشأ العوائق الدولية التي تعوق تعزيز استخدام التوقيعات الإلكترونية في التجارة الدولية من خلال تحديد مناهج وطنية خاصة بالتكنولوجيا ويلاحظ أن إحدى العقبات الرئيسية التي تحول دون استخدام التوقيعات والمصادقة الإلكترونية عبر الحدود هي الافتقار إلى قابلية التشغيل البيني ، بسبب المعايير المتعارضة أو المتباينة أو تنفيذها غير المتسق ويمكن نشر التوافق التجاري والقانوني وإمكانية التشغيل البيني التقني لخطط المصادقة على المستويين الوطني والدولي ، لتسهيل التفاعلات والمعاملات عبر الإنترنت في القطاعين الخاص والعام.

وتوصي قوانين الأونسيترال ببناء آليات الاعتراف بخدمات المصادقة الأجنبية والعمل على القواعد الوطنية المتعلقة بمسؤولية مقدمي الخدمات المعتمدين الذين يمتثلون لمعيار دولي موحد. في تقرير الأونسيترال لعام ٢٠٠٧ بشأن تعزيز الثقة في التجارة الإلكترونية، من المؤكد أن المبدأين –" مكان المنشأ، والمعاملة بالمثل والتحقق المحلي" و "التكافؤ الموضوعي" المنبثق عن القانون النموذجي للتوقيعات الإلكترونية (المادة ١٢) بواسطة القوانين الوطنية لتعزيز المعيار الدولي للأمن وإزالة العقبات التي تحول دون الاعتراف بالشهادات الأجنبية والتوقيعات الإلكترونية كما يشير إلى أن الاعتراف المتبادل يمكن أن يحدث عادة على مستوى البنية التحتية للمفاتيح العمومية وليس على مستوى مقدم خدمة التصديق الفردي. إن تطبيق قابلية التشغيل البيني

٤٥) د إبراهيم بن سطم بن خلف العنزي، التوقيع الإلكتروني وحمايته الجنائية، جامعة نايف العربية للعلوم الأمنية، ٢٠١٠.[45]

التقني وكذلك تنسيق سياسات الشهادات وبيانات الممارسة سيسهم في تعزيز التصديق والاعتراف عبر الحدود.[٤٦]

وبناء الثقة في التجارة الإلكترونية له أهمية كبيرة لتطوره حيث قد تكون هناك حاجة إلى قواعد خاصة للاعتراف بالشهادات الأجنبية والتوقيعات الإلكترونية. ينبغي تحديث الصكوك القانونية الدولية، أو القوانين النموذجية عبر الوطنية، أو التشريعات الوطنية، أو أدوات التنظيم الذاتي، أو الاتفاقيات التعاقدية، ومواصلة تطويرها لزيادة اليقين والأمن في استخدامها مع قواعد خاصة.

الخاتمة: –

تطور الحياة وخاصةً الحياة التكنولوجية، كان له تأثير على الحياة الاقتصادية وطرق ممارسة العمل التجاري، الأمر الذي أدى إلى ضرورة تطوير التشريعات، بما يتوافق مع تطور الحياة،

[46] OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication (Paris, June 2007). Available at: http://www.oecd.org/dataoecd/32/45/38921342.pdf (last accessed 30 June 2013).

ومن هنا نرى مدى أهمية التوقيع الإلكتروني، ليتوافق مع هذا التطور بالتوازي مع درجات الفاعلية والأمان التي يجب أن تتوفر به، فإن مشكلة الأمن والخصوصية على شبكة الإنترنت تشغل حيزا كبيرا من اهتمام المسؤولين، كما تثير قلق الكثير من الناس مما يسبب نوع من انعدام الثقة بشبكة الإنترنت، ولذلك تم اللجوء الى تكنولوجيا التوقيع الإلكتروني.

وحتى يتم الرفع من مستوى الأمن والخصوصية للمتعاملين مع الشبكة ويتم ذلك بقدرة هذه التكنولوجيا على الحفاظ على سرية المعلومات أو الرسالة المرسلة وعدم قدرة أي شخص آخر، على الاطلاع أو تعديل أو تحريف الرسالة، كما يمكنها أن تحدد شخصية وهوية المرسل إلكترونياً، والتأكد من مصداقية هذه الشخصيات مما يسمح لها بكشف أي متحايل أو متلاعب.

وخلت التوقيعات الإلكترونية عالم الإنترنت بحيث تشمل اتفاقات مبرمه عبر البريد الإلكتروني وادخل رقم التعريف في ماكينة الصراف الآلي وتوقيع قسيمة الأتمان باستخدام جهاز لوحة القلم الرقمي وتوقيع المستندات الإلكترونية عبر الأنترنت.

وكان أول اتفاق تم التوقيع علية الكترونياً من قبل الولايات المتحدة وايرلندا عام ١٩٨٨ لتعزيز التجارة الإلكترونية.

ونشرت الأمم المتحدة في عام ١٩٩٦ قانون الأونسيترال الذي يخص التجارة الإلكترونية وكان له أثر كبير في تطوير قوانين التوقيع الإلكتروني حول العالم، ثم نشرت قانون الأونسيترال النموذجي للتوقيعات الإلكترونية في ٢٠٠١ والتي اعترفت فيه بالأثر القانوني للتوقيعات الإلكترونية.

الأمر الذي حذي بالمشرع المصري إلى تنظيم التوقيع الإلكتروني إلى تنظيم التوقيع الإلكتروني بالقانون رقم ١٥ لسنة ٢٠٠٤، ويقع القانون في ثلاثين مادة ويهدف إلى توفير البيئة التشريعية اللازمة لدعم التعاملات بالمستندات الموقعة الكترونيا. وجدير بالذكر أن نطاق ال قانون يشمل المعاملات المدنية والتجارية والإدارية التي يمكن إتمامها إلكترونياً، مما يساعد على رفع كفاءة العمل الإداري وتفعيل التجارة الالكترونية والارتقاء بمستوى أداء الخدمات الحكومية بما يتفق مع إيقاع العصر.

وقد أقر القانون إنشاء هيئه عامة ذات شخصية اعتبارية وتتبع وزير الاتصالات والمعلومات، وتسمى "هيئه تنمية صناعه تكنولوجيا المعلومات "، تعمل هذه الهيئة على إدارة وتنظيم وتحديد معايير التوقيع الالكتروني وإصدار وتجديد التراخيص لمزاولة الأنشطة في مجال المعاملات الالكترونية، كما تعمل علي تنمية صناعه تكنولوجيا المعلومات والاتصالات إلى جانب ذلك علي حماية حقوق الملكية الفكرية وتقييم الجهات العاملة في مجال تكنولوجيا المعلومات وتقديم المشورة الفنية لمثل هذه الجهات، وخاصة بشان المنازعات التي قد تنشا بين الاطراف المعنية بأنشطة التوقيع الالكتروني والمعاملات الالكترونية. وقد اشتملت باقي مواد القانون على أسس إثبات صحة وحجية التوقيع الالكتروني وشهادات التصديق الالكتروني، إلى جانب ما يجب أن تحدده اللائحة التنفيذية لهذا القانون من معايير فنية وتقنية وتنظيمية.

إلا أننا نرى أن مشكلة قانون التوقيع الإلكتروني المصري أنه قانون أُنشئ دون أن يوضع في البيئة الخاصة به، حيث أنه لا يوجد قانون ينظم التجارة الإلكترونية في الأساس، والذي يعتبر التوقيع الإلكتروني إحدى أدواته، فكان من الأحرى بالمشرع المصري أن ينظم التجارة الإلكترونية بادئ ذي بدء قبل تنظيم التوقيع الإلكتروني أو أن ينظم التوقيع الإلكتروني داخل قانون للتجارة الإلكترونية.

وإن كان المشرع المصري بصدد القيام بتشريع ينظم التجارة الإلكترونية إلا أنه حتى الأن لم يصدر هذا التشريع، على الرغم من دول عديدة سبقتنا في ذلك وخاصة الدول العربية مثل الأردن والسعودية ودولة الإمارات العربية، حيث تعتبر التجارة الإلكترونية واحدة من التعابير الحديثة والتي أخذت بالدخول إلى حياتنا اليومية حتى أنها أصبحت تستخدم في العديد من الأنشطة الحياتية والتي هي ذات ارتباط بثورة تكنولوجيا المعلومات والاتصالات. التجارة الإلكترونية تعبير يمكن أن نقسمه إلى مقطعين، حيث أن الأول، وهو "التجارة"، والتي تشير إلى نشاط اقتصادي يتم من خلال تداول السلع والخدمات بين الحكومات والمؤسسات والأفراد وتحكمه عدة قواعد وأنظمة يمكن القول بأنه معترف بها دولياً، أما المقطع الثاني "الإلكترونية" فهو يشير إلى وصف لمجال أداء التجارة، ويقصد به أداء النشاط التجاري باستخدام الوسائط والأساليب الإلكترونية مثل الإنترنت.

إلا أنه في النهاية فان التوقيع الإلكتروني يعتبر هو أداة العصر لإتمام العمليات التجارية المستقبلية على مستوى العالم، وعلى المشرع المصري تطوير التشريعات التجارية وأن يسرع في تنظيم التجارة الإلكترونية في مصر بالتوازي مع قانون التوقيع الإلكتروني المصري.

أهم النتائج:

إن دراسة التوقيع الإلكتروني أعطانا كثير من النتائج يمكن إجمالها فيما يلي:

١- تطور المعاملات التجارية عبر الحدود وخاصة بالنسبة للمنتجات غير الملموسة.
٢- أهمية تعزيز الاستفادة من تكنولوجيا المعلومات في تطوير التجارة العالمية.
٣- محاولة إيجاد حلول سريعة لمعوقات التجارة العالمية.
٤- الدور الفعال للتوقيع الإلكتروني لتطوير العقود الإلكترونية.
٥- الاهتمام بحماية البيانات والأمن الإلكتروني.
٦- دور التشريعات الدولية في المساهمة في تطوير التشريعات الوطنية فيما يختص بالتوقيع الإلكتروني.
٧- أن للتوقيع الإلكتروني نفس الأثر القانوني للتوقيع العادي في التشريعات الدولية والمحلية.

أهم التوصيات:

وفى رأيي فإن التوقيع الإلكتروني يجب أن يتم تنظيمه من خلال عدة أوجه يمكن إجمالها فيما يلي:

١- تطوير البنية التحتية التكنولوجية للدولة نظراً لدخول عصر التجارة الإلكترونية عالمياً.
٢- إيجاد تشريع لقانون متكامل للتجارة الإلكترونية يندمج فيه قانون التوقيع الإلكتروني.
٣- تطوير قانون التوقيع الإلكتروني الحالي وبما يتماشى مع تطور التجارة العالمية.
٤- تطوير العقود التجارية بما يتماشى مع التطور في التوقيع الإلكتروني حتى لا يكون هناك تفاوت بينهم.
٥- توحيد التشريعات الإلكترونية فيما يختص بالقوانين التجارية والعقود والتوقيع الإلكتروني لتسهيل العمليات التجارية المستقبلية.

Abstract

مع دخول عصر المعاملات الإلكترونية، وخاصة التجارية منها أصبح الاعتراف بالتوقيع الإلكتروني قانوناً وتطبيقه عملياً أمراً في غاية الأهمية، لأنه أصبح أداة التعاملات المستقبلية في التعاملات الإلكترونية بين الناس والهيئات الاقتصادية، حيث سهلت لهم تبادل المعلومات مع ضمان توثيقها مما أضفى ضمانة شرعية على تبادل المستندات والمعاملات التجارية، خصوصاً في ظل صدور التشريعات الوطنية والدولية التي اهتمت بوضع تشريعات تنظم منظومة التوقيع الإلكتروني.

With the entry of the era of electronic transactions, especially commercial ones, the recognition of electronic signature in law and its practical application has become very important, because it has become a tool for future transactions in electronic transactions between people and economic bodies, as it facilitated the exchange of information while ensuring its documentation, which gave a legal guarantee on the exchange of documents and transactions.

Commercial, especially in light of the issuance of national and international legislation that focused on developing legislation that regulates the electronic signature system.

المراجع

١-مراجع عربية:

أ) د إبراهيم بن سطم بن خلف العنزي، التوقيع الإلكتروني وحمايته الجنائية، جامعة نايف العربية للعلوم الأمنية، ٢٠١٠

ب) أ/ عبد الملك العياضى، آثار التوقيع الإلكتروني، جامعة الملك سعود، ٢٠١٢، ص١٢٧

ج) د/محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، الإسكندرية، ٢٠١٤

د) عادل رمضان الأبيوكى، التوقيع الإلكتروني في التشريعات الخليجية، دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، ٢٠٠٩.

هـ) ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، الطبعة الأولى، ٢٠٠٧.

و) نسرين عبد الحميد نبيه، الجانب الإلكتروني للقانون التجاري، نشر بمنشأة المعارف، الطبعة الأولى، الإسكندرية، ٢٠٠٨،

ل) عبد الحكيم زروق، تنظيم التبادل التجاري، تنظيم التبادل الإلكتروني للمعطيات القانونية عبر الإنترنت، منشورات دار الأورمان، الطبعة الأولى، الرباط، ٢٠١٦

٢-مراجع أجنبية:

1- OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication (Paris, June 2007). Available at: http://www.oecd.org/dataoecd/32/45/38921342.pdf (last accessed 30 June 2013).

2- W. J. Craig, Hague Conference on E-Commerce Law, Introductory and Background Issues, Hague E-Commerce Conference, 26–27 October 2004. Available at: http://hcch. e-vision.nl/upload/wop/e-comm_craig.pdf (last accessed 30 June 2013).

3- Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market, COM (2008) 798 final of 28.11.2008; Digital Agenda for Europe, COM (2010) 245 of 19.05.2010; and the Proposal for a Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, COM (2012) 238 final of 04.06.2012.

4- M. J. Ostey and M. Pulcanio (1999) 'The liability of certification authorities to relying third parties', John Marshall Journal of Computer and Information Law, 17 (3): 961.

5- Measures for the Administration of Electronic Certification Services 2009, Article 1. 109 COM (2012) 238, final, Brussels 4 June 2012, Article 19(1) (2).

6- Selected Bibliography on Description of Digital Signatures, Appendix 6 on 'The Role of Certification Authorities in Consumer Transactions' prepared by the Internet Law and Policy Forum. Available at: http://www.ilpf.org/groups/ca/app6.htm (last accessed 30 June 2013).

7- S. Baker and M. Yeo (1999) Survey of International Electronic and Digital Signature Initiatives, from the Internet Law & Policy Forum Working Group 1999. Available at: http://www.ilpf. org/groups/survey.htm (last accessed 30 June 2013).

8- Promoting Confidence in Electronic Commerce: legal issues on international use of electronic authentication and signature methods, United Nations Commission on International Trade Law (UNCITRAL), Vienna, United Nations, 2007 (released in 2009). Available at: http://www.uncitral.org/pdf/ english/texts/electcom/08-55698_Ebook.pdf (last accessed 30 June 2013).

الفهرس