جامعه بنها
كلية الحقوق
قسم القانون المدني

خدمات التصديق الإلكتروني
(دراسة مقارنة)

بحث مقدم من الباحث
عماد الدين سعد قطب زعيتر

تحت إشراف
الأستاذ الدكتور
سمير حامد عبد العزيز الجمال
أستاذ القانون المدني
ووكيل كلية الحقوق جامعة دمياط

مقدمة

أهميةُ موضوعِ البحثِ:

إنَّ نظامَ عمل مقدم خدمات التصديق الإلكتروني في مصر وبعض الدول العربية يختلف عن نظام عمله في اللائحة الأوربية، حيث يقتصر تقديم خدمات التصديق الإلكتروني في مصر على الأشخاص الاعتبارية فقط ويشترط أيضًا في الحصول على ترخيصٍ من هيئة تنمية صناعة تكنولوجيا المعلومات قبل مباشرة عمله في تقديم هذه الخدمات، أما في اللائحة الأوربية التى تطبق على دول الاتحاد الأوربي بما فيها فرنسا، تقوم على مبدأ حرية تقديم خدمات التصديق الإلكتروني، حيث يمكن لأي شخصٍ سواء كان طبيعيًا أو اعتباريًا في تقديم خدمات الثقة الإلكترونية ولكنها فرقت بين مقدم خدمة ثقة مؤهل وغير مؤهلٍ، الأول يخضع لمعايير متطلبات اللائحة التى يجب الامتثالُ لها قبل مباشرة عمله لاكتساب صفة مقدم خدمة ثقة مؤهل واكتساب الخدمات التى يقدمها صفة المؤهلة، أما الثاني فلا يخضع قبل مباشرة عمله في تقديم هذه الخدمات لأي متطلباتٍ، سوى المتطلبات التى نصَّت عليها اللائحة الأوربية التى تسرى على جميع مقدمي خدمة الثقة سواء كان مؤهل أو غير مؤهلًا، وتسري أيضًا على الخدمات التى يقدموها سواءً كانت مؤهلةً أو غير مؤهلةٍ.

حيثُ تقعُ على جهات التصديق الإلكتروني التى تحصل على ترخيص من هيئة تنمية صناعة تكنولوجيا المعلومات بممارسة نشاطها، التزاماتٌ عند تقديم خدمات التصديق الإلكتروني، وأهمُّها وهو الالتزام بإصدار شهادة التصديق الإلكتروني بعد الالتزام بالمتطلبات التى ينص عليها قانون التوقيع الإلكتروني المصري واللائحة التنفيذية وما تضعه هيئة تنمية صناعة تكنولوجيا المعلومات من التزاماتٍ عند تقديم هذه الخدمات.

أما في اللائحة الأوربية [eIDAS][(١٣٤٤)] فهى لم تقتصر على تقديم خدمة إصدار شهادات التصديق الإلكتروني بل تضمنت خدمات أخرى يمكن تقديمها من مقدم خدمة الثقة المؤهل أو غير المؤهل،حيث لا تفرض اللائحة على مقدم خدمات الثقة تقديم جميع خدمات الثقة الواردة في اللائحة، فله حريةٌ في تقديم أي من خدمات الثقة وله أن يقدم خدمةً واحدةً من خدمات الثقة أو أكثر من خدمة، فإنَّ اللائحة تحدد فقط خدمات الثقة التى تقدم والنظام القانوني المطبق على هذه الخدمات عند تقديمها.

منهجُ الدراسةِ:

يقوم منهجُ الدراسةِ في البحث على المنهج المقارن، ونعرض من خلاله التشريعات التى تنظم خدمات التصديق الإلكتروني، في اللائحة الأوربية المؤرخة ٢٣ يوليو رقم ٢٠١٤/٩١٠ بشأن تحديد الهوية الإلكترونية وخدمات الثقة (eIDAS) وإلغاء التوجيه الأوربي ١٩٩٩/٩٣، و القانون الفرنسي، و القانون البلجيكي الصادر في ٢١ يوليو ٢٠١٦ الذي ينفذُ اللائحة الأوربيةَ و ينظمُ الأرشفةَ الإلكترونيةَ مع مقارنتها بالقانون المصري الذي ينظم خدمات التصديق الإلكتروني، و نحاول من خلال ذلك الاستفادة من بعض النصوص القانونية التى تعرضت للموضوع بالدراسة،

(١٣٤٤) Règlement n°910/2014 du 23 juillet 2014 sur l'identification électroniq ue et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n°1999/93/CE,Disponible sur http://www.europa.eu.

والوصول إلى بعض الحلول، لنضعها أمام المشرع المصري، لعله يهتدي بها إذا رأى التدخل لتعديل قانون التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤، ليتناسب مع زيادة حجم التجارة الإلكترونية، وأهمية دور مقدم خدمات التصديق الإلكتروني في بث الثقة في المعاملات الإلكترونية.

خطة البحث: **المبحث الأول: تقديم خدمة إصدار شهادات التصديق الإلكتروني.** المطلب الأول: ماهية شهادات التصديق الإلكتروني. الفرع الأول: التعريفات التشريعية لشهادة التصديق الإلكتروني. الفرع الثاني: التعريفات الفقهية لشهادة التصديق الإلكتروني. المطلب الثاني: شروط إصدار شهادة التصديق الإلكتروني. الفرع الأول: شروط إصدار شهادة التصديق الإلكتروني في القانون المصري. الفرع الثاني: متطلبات إصدار شهادات التصديق الإلكتروني المؤهلة في اللائحة الأوربية. المطلب الثالث: الأثار القانونية المترتبة على إصدار شهادة التصديق. الفرع الاول: مدى حجية شهادة التصديق الإلكتروني الوطنية. الفرع الثاني: مدى حجية شهادة التصديق الالكتروني الأجنبية.

المبحث الثاني: الخدمات الآخرى التي يقدمها مقدم خدمات التصديق. المطلب الأول : الخدمات الآخرى التى يقدمها مقدم خدمة الثقة في اللائحة الأوربية. الفرع الأول : خدمة التحقق المؤهلة من التوقيعات والأختام الإلكترونية. الفرع الثاني : خدمة البريد الإلكتروني المؤهل. الفرع الثالث : خدمة ختم الوقت الإلكتروني المؤهلة. الفرع الرابع : خدمة الحفظ المؤهلة للتوقيعات المؤهلة والأختام الإلكترونية. المطلب الثاني : الخدمات الآخرى التى تقدمها جهات التصديق الإلكتروني في القانون المصري. الفرع الأول : خدمة إصدار أدوات وتثبيت التوقيعات الإلكترونية. الفرع الثانى : خدمة حفظ مفاتيح الشفرة الخاصة المصدرة لمستخدم الخدمة. الفرع الثالث : خدمة الختم الإلكتروني والبصمة الزمنية.

المبحثُ الأولُ

خدمةُ إصدارِ شهاداتِ التصديقِ الإلكترونيةِ

تمهيدٌ وتقسيمٌ:

إنَّ الأهمية والدور الذي تلعبه شهادات التصديق في إثبات هوية من صدر منه التوقيع عن طريق ربطه بالمفتاح العام، مما يحقق عنصر الأمان في التعاملات الإلكترونية، ومما لا شكَّ فيه أنَّ عدم التأكد من شخصية المتعاقدين يجعل التوقيع الموضوع على الصفقة محل منازعة وشكَّ، ويلاحظ أنه في الوقت الحالي يوجد مقدمو خدمات المفاتيح ولكن يعيب هؤلاء أنهم لا يضمنون بشكل قاطع التحقق من هوية مرسل الرسالة ومعها المفتاح العام، أمام كل هذه المشكلات العملية أصبح وجود مقدم خدمات التصديق يضمن أمان الصفقة[١٣٤٥].

([١٣٤٥]) د. عبد الفتاح بيومي حجازي، النظام القانوني للتوقيع الإلكتروني، دار الكتب القانونية، القاهرة، ٢٠٠٧، ص ٩٣.

مما لاشكَّ فيه أنَّ جهة التصديق الالكتروني لها دور كبيرفى التعاملات الإلكترونية فهي تصدر شهادة التصديق الإلكتروني على التوقيع أو الختم الالكتروني و تصدر شهادة تفيد صحة التعاملات الإلكترونية ويترتب على أعمالها آثارًا قانونية في حق الموقع و الطرف الآخر في التعامل الإلكتروني، ولذلك تسأل جنائيًا في حالة ما إذ ساهمت في ارتكاب جريمة تتعلق بالتوقيع الإلكتروني وتُسأل مدنيًا كذلك في حالة حدوث أضرارٍ بحق أي طرفٍ من الأطرافِ(١٣٤٦).

ولذلك سوف نتناولُ هذا الالتزام من خلال ثلاثة مطالبَ: نخصصُ الأولَ لماهية شهادات التصديق الإلكتروني، ونبينُ في الثاني شروط إصدارِ شهادةِ التصديقِ الإلكترونيِ، ونكرسُ الثالثَ للآثارِ القانونيةِ المترتبةِ على تسجيلِ وإصدار شهادة التصديق الإلكتروني.

المطلبُ الأولُ

ماهية شهادةِ التصديقِ الإلكترونيِ

شهادةُ التصديقِ هي شهادةٌ إلكترونيةٌ تؤكد أنَّ الرقمَ السريَّ وهو أداة إنشاء التوقيع الإلكتروني للموقع، يعودُ للموقع المبيَّن اسمُه في الشهادة وهو يطابق الرقمَ العلنيَّ الذي يتم تسليمه للغير، وهكذا يتحقق الارتباط بين التوقيع الإلكتروني وبين شخصٍ معينٍ، فيقدمُ الغير على التعاقد معه وهو مطمئن إلى أنَّ التوقيع الإلكتروني يعود فعلًا إلى الشخص الذي يقوم باستعماله، و لذلك نقوم بتقسيم هذا المطلب إلى فرعين: نحصَّص الأول للتعريفات التشريعية لشهادة التصديق الإلكتروني، ونوضحُ في الثاني للتعريفات الفقهية لشهادة التصديق الإلكتروني.

الفرعُ الأولُ

التعريفاتُ التشريعيةُ لشهادةِ التصديقِ الإلكترونيِ

أولًا: قانونُ التوقيعِ الإلكترونيَّ المصريَّ:

وقد عَّرفها قانون التوقيع الإلكتروني في المادة (١/و) بأنها: "الشهادةُ التى تصدر من الجهة المرخص لها بالتصديق، وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع".

حيث نجد المشرَّع المصريَّ قد عرَّف الشهادة من حيث الجهة التى تصدرها، وهي جهة التصديق والتى يجب أن تكون مرخص لها بالتصديق من الجهات المختصة بذلك، وقد عرَّف الشهادة من حيث الوظيفة التى تؤديها، وهو إثبات نسبة التوقيع إلى الموقع، بالتالى لا يستطيع الموقع بعد ذلك إنكار نسبة التوقيع إليه، حيث بصدور شهادة التصديق من الجهة المختصة بذلك، لا يستطيع الموقع إنكار ذلك التوقيع سوى الطعن عليه بالتزوير.

حيثُ يؤخذُ على المشرَّعِ المصريَّ في قانون التوقيع الإلكتروني أنه لم يعرف شهادات التصديق أكثر تفصيلًا، إنما عرفها من حيث الجهة التى تصدرها والوظيفة التى تؤديها، كما أن المشرع لم يذكر في تعريفه لهذه الشهادات البيانات التى يجب أن تتضمنها هذه الشهادات، التى تعد من الشروط الأساسية التى يجب توافرها فيها حتى تتمتع بالحجية القانونية في الإثبات، وحيث نجد أيضًا المشرع المصري اشترط أن يكون هناك ارتباطٌ بين صاحب الشهادة و المفتاح

(١٣٤٦) د. ممدوح محمد مبروك، مدى حجية التوقيع الإلكتروني في الاثبات، دار النهضة العربية، ٢٠٠٩، ص ١٤٨.

الخاص به، وهذا يؤخذ عليه أيضًا لأنه يجب أن يكون المفتاح الخاص سريًا للموقع لا يطلع عليه غيره، وذلك لمنع اختراقه وسرقته مما يضعف الثقة و الأمان في المعاملات الإلكترونية.

ثانيًا: التشريعات الأوربية:

نجد أن اللائحة الأوربية ٢٠١٤/٩١٠ لم تقتصر على تعريف شهادة التحقق من صحة التوقيع الإلكتروني بل تطرقت إلى تعريف شهادة الختم الإلكتروني وشهادة تصديق الموقع الإلكتروني في المادة الثالثة وذلك على النحو الآتي:"شهادة التوقيع الإلكتروني" بأنها تعني شهادةً إلكترونيةً تربط بياناتِ التحقق من صحة التوقيع الإلكتروني بشخصٍ طبيعيٍّ وتؤكد على الأقل اسمًا أو اسمًا مستعارًا لذلك الشخص، و "شهادة الختم الإلكتروني" تعني شهادة إلكترونية تربط بيانات التحقق من الختم الإلكتروني بشخص قانوني وتؤكد اسم ذلك الشخص و "شهادة مصادقة موقع الويب" تعني شهادةً تسمح بمصادقة موقع ويب وربط موقع الويب بالشخص الطبيعي أو الاعتباري الذي صدرت إليه الشهادة.

أما بخصوص المشرِّع الفرنسيَّ قد تناول شهادة التصديق الإلكتروني في المرسوم رقم ٢٧٢ لسنة ٢٠٠١ الخاص بالتوقيع الإلكتروني، في البند التاسع من المادة الأولى بأنها "وثيقةٌ في شكلٍ إلكتروني تقوم بربط الصلة بين بيانات التحقق من التوقيع وشخص الموقع ذاته"؛ وجديرٌ بالذكر تم إلغاء هذا المرسوم، بموجب المرسوم رقم ١٤١٦ لسنة ٢٠١٧ و الذى تم النص في المادة الثانية منه على استبقاء أحكامه على نحو لائحى مع استبدال كل إشارةٍ إلى المادة ١٣١٦-٤ الملغاة من القانون برقم هذا المرسوم.

حيثُ يتضح من تعريف المشرِّع الفرنسيَّ لشهادة التصديق، بأنه عرف شهادة التصديق بأنها مستندٌ إلكتروني لها حجيةٌ في الإثبات، وهو ما أكدته المادة ١٣٦٦ من القانون المدني رقم ١٣١لسنة ٢٠١٦، و التى ساوت بين المستندات الإلكترونية و التقليدية من حيث الإثبات، إلا أنه يعيب على المشرِّع الفرنسي، أنه لم يحدد الجهة التى تصدر عنها الشهادة، وكذلك لم يوضح التعريف الوظائف التى تؤديها هذه الشهادة، وكذلك اشترط أن يكون هناك ارتباط بين الموقع ومفتاحه العام والخاص(١٣٤٧).

الفرعُ الثاني

التعريفاتُ الفقهيةُ لشهادةِ التصديقِ الإلكترونِي

لقد حاول العديد من الفقهاء وضع تعريفٍ لشهادةِ التصديق الإلكتروني، وذلك لتوضيح مفهومها، وهدفها، وسنذكر بعض هذه التعريفات.

(١٣٤٧) Luc Grynbaum, La Preuve littérale et la signature à L'Heure de la communication électronique. J.C.P., nov. 1999, P. 13.

قد عَّرفها جانبٌ من الفقه [١٣٤٨] بأنها :" الشهادة التى يصدرها مقدمو خدمات التصديق، المرخَّص لهم من قبل الجهات المسئولة في الدولة، لتشهد بأن التوقيع الإلكتروني هو توقيعٌ صحيحٌ، و ينسب إلى من أصدره، و مستوفي الشروط والضوابط المطلوبة فيه باعتبارها دليلُ إثباتٍ يعول عليه".

كما عَّرفها جانبٌ من الفقه [١٣٤٩] بأنها:" الشهادةُ التى تصدر عن الجهة المرخص لها بالتصديق، لإثبات نسبة التوقيع الإلكتروني إلى شخصٍ معينٍ، استنادًا لإجراءات تصديقٍ معتمدةٍ بخصائصَ معينةٍ، تسمح بتميزه عن غيره، باعتباره دليل إثباتٍ يعول عليه".

كما عَّرفها جانبٌ من الفقه [١٣٥٠] بأنها:" هوية يصدرها شخص محايد، للتعريف بالشخص الذي يحملها وللمصادقة على توقيعه الإلكتروني، وعلى المعاملات التى يجريها عبر الإنترنت".

ويعرفها جانب من الفقه [١٣٥١] بأنها:" بطاقة إثبات الهوية الإلكترونية وهي الشهادة التى تصدر أثناء عملية التوقيع الإلكتروني من شأنها إثبات هوية الموقع".

ويعرفها جانبٌ من الفقه[١٣٥٢] بأنها:" صكٌ أمانٍ صادرٍ عن جهةٍ مختصةٍ، يفيد صحة وضمان المعاملة الإلكترونية، وذلك من حيث صحة البيانات، ومضمون المعاملة وأطرافها".

و يعرَّفها جانبٌ من الفقه [١٣٥٣] بأنها:" مستندٌ إلكتروني يؤكد به الشخص وقائعَ معينةً"، و حيث نلاحظ من هذا التعريف أنه غيرُ واضحٍ ولم يحدد لنا ما هي الجهة المختصة بإصدار الشهادة ولم يوضح الهدف من الشهادة بل اكتفي بالقول أن الهدف منها هو تأكيد وقائعَ معينةٍ.

وقد عرَّفها جانبٌ من الفقه[١٣٥٤] بأنها: "عبارةٌ عن سجَّل إلكتروني بيَّن مفتَّاحا عامًا إلى جانب اسم صاحب الشهادة، باعتباره موضوع الشهادة يؤكد أن الموقع المرتقب المحدد هويته في الشهادة، هو حائز المفتاح الخاص المناظر".

وقد عَّرفها الفقه في فرنسا[١٣٥٥] بأنها: "تنشيء علاقة بين الموقع والمعطيات والبيانات المستخدمة من أجل التحقق من سلامة هذا التوقيع".

[١٣٤٨] د. إبراهيم الدسوقي أبو الليل، توثيق المعاملات الإلكترونية ومسئولية جهة التوثيق تجاه الغير المضرور، مرجع سابق، ص ١٨٧٣.

[١٣٤٩] د. علاء حسين مطلق التميمي، الجهة المختصة بإصدار شهادة التصديق الإلكتروني، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١١، ص٢١.

[١٣٥٠] د. خالد ممدوح إبراهيم، التوقيع الإلكتروني، مرجع سابق، ص٢٢٦.

[١٣٥١] د. أيمن سعد سليم، التوقيع الإلكتروني، دار النهضة العربية، ٢٠١٣، ص ٣٣.

[١٣٥٢] د. محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، مرجع سابق، ص٣٤.

[١٣٥٣] د. أمير فرج يوسف، التوقيع الإلكتروني، دار المطبوعات الجامعية، الاسكندرية، ٢٠٠٨ ، ص٨١.

[١٣٥٤] د. تامر محمد سليمان الدمياطي، إثبات العقد الإلكتروني عبر الإنترنت، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٠٨، ص ٥٥١.

[١٣٥٥] Georges Didier , Cadre juridique pour les signatures électroniques Op.cit , p- 19.

حيث يتبين من خلال التعريفات التشريعية والفقهية السابقة لشهادات التصديق الإلكتروني، بأنها هى وثيقةٌ إلكترونيةٌ على شكل شهادةٍ رقميةٍ تثبت نسبة التوقيع للموقع، وتعتبر بمثابة بطاقةٍ شخصيةٍ للموقع والتى عن طريقها تبين ارتباط التوقيع الإلكتروني بالموقع دون غيره، إذ يمكن القول أن هذه الشهادة تهدف إلى القضاء على إمكانية انتحال الغير لشخصية المرسل، مما يجعل مقدم خدمات التصديق الإلكتروني الذي يصدر هذه الشهادات يشهد بصحة التوقيع الإلكتروني.

بالتالي لا يجوز لمقدم خدمات التصديق الإلكتروني إصدار شهادة التصديق الإلكتروني على أي توقيعٍ إلكترونيٍّ إلا لمن يقدم لها المفتاح العام لهذا التوقيع، وذلك لأن عدم معرفة طالب شهادة التصديق بالمفتاح العام لصاحب التوقيع الإلكتروني إنما يعد قرينةً قويةً على عدم وجود ثمَّةَ معاملةٌ إلكترونيةٌ بينهما، و بناءً عليه تتميز شهادة التصديق على التوقيع الإلكتروني بمجموعةٍ من الخصائص، وهى أنها تربط بين المفتاح العام و الموقع[١٣٥٦]،

و تؤكد على صحة التوقيع الإلكتروني الذي تم تصديقه من قبل جهة التصديق، و أنها تصدر عن جهةِ تصديقٍ معتمدةٍ و مرخصٍ لها وصدورها عن هذه الجهة يمنحها الثقة والأمان.

المطلبُ الثالثُ

شروطُ إصدارِ شهادةِ التصديقِ الإلكترونيَّ

حيث يقتصر قانون التوقيع الإلكتروني المصري وبعض التشريعات العربية، على الشروط الواجب توافرها عند إصدار شهادة التصديق على التوقيع الإلكتروني، حيث نظمت هذه القوانين الشروط الواجب توافرها عند إصدار هذه الشهادة فقط، أما الوضع القانوني في اللائحة فلم يقتصر على شهادة التصديق على التوقيع الإلكتروني، فنظم شهادة الختم الإلكتروني وشهادة مصادقة الموقع، و لذلك سوف نقوم بتقسيم هذا المطلب إلى فرعين: نخصَّصُ الأولَ لشروطِ إصدارِ شهادةِ التصديق الإلكتروني في القانون المصري، ونكرس الثاني لمتطلبات إصدار شهادات التصديق الإلكتروني المؤهلة في اللائحة الأوربية.

يجب أن تتوافر في الجهة التي تقوم بإصدار شهادة التصديق على التوقيع الإلكتروني أن تكون صادرًا لها ترخيص من الجهة المختصة في القانون، ويجب أيضا أن تتضمن شهادة التصديق الإلكتروني مجموعة من البيانات التى يجب أن تتضمنها وذلك على النحو التالى:

الشرطُ الأولُ– صدورُ الشهادةِ من جهةِ تصديقِ إلكترونيٍّ مرخصٍ لها بذلك:

يجب أن تكون هذه الجهة مرخصًا لها بمزاولة نشاط إصدار شهادات التصديق؛ إذ أنه يشترط حصول جهات التصديق على الترخيص من هيئة تنمية صناعة تكنولوجيا المعلومات قبل مزاولة نشاطها، و وهذا ما أكدت عليه المادة (١٩) من قانون التوقيع الإلكتروني.

[١٣٥٦] د. أمير فرج يوسف، التوقيع الإلكتروني والحجية القانونية للتوقيع الإلكتروني في كافة المعاملات الإلكترونية، مكتبة الوفاء القانونية، الأسكندرية، ٢٠١١، ص٣٧.

وهذا يدل على أن المشرَّع المصريَّ في قانون التوقيع الإلكتروني، قد تشدد في اشتراط أن تحصل هذه الجهات على الترخيص، بالتالي لا يجوز لها أن تمارس نشاطها بإصدار شهادات التصديق دون حصولها المسبق على الترخيص و اعتمادها من الهيئة؛ والأكثر من ذلك نجد المشرَّعَ المصريَّ في قانون التوقيع الإلكتروني قد فرض عقوبةً جنائيةً على الجهات التى تصدر شهاداتِ تصديقٍ دون الحصول المسبق من الهيئة.

الشرط الثاني– يجب أن تتضمن شهادات التصديق بياناتٍ معينةً:

حتى يمكن الاعتداد بشهادة التصديق الإلكتروني وتكون لها القيمة القانونية التى تكتسبها الحجية الكاملة في الإثبات، لابُدَّ أن تتضمن البيانات التى نص عليها القانون، نظرًا لأهميتها وجوهريتها، حيث اشترط التشريع المصري على أن تتضمن شهادات التصديق الإلكتروني مجموعةً من البيانات وهي على النحو الآتي:

١– بيانات تتعلق بشهادة التصديق: هناك مجموعة من البيانات المتعلقة بهذه الشهادة وهي:

أ– صلاحية هذه الشهادة للاستخدام، حيث أن شهادة التصديق تستخدم للتأكد من هوية الموقع، و التأكد من صحة البيانات الواردة فيها، و يعدُّ هذا المجالُ الذي من الممكن أن تستعمل فيها الشهادة، فإذا استعملت بغير ما ذكر ونشأ من ذلك ضررٌ فلا يكون مقدم الخدمة مسئولًا عن ذلك الضرر.

ب– مدة صلاحية الشهادة، حيث أن جهاتِ التصديق الإلكتروني لا تكون مسئولةً عن الشهادات منتهية الصلاحية، إذ يذكر في الشهادة تأريخ بدء صلاحيتها وتأريخ انتهائها ليتسنى للمتعامل بناءً على شهادة التصديق معرفة مدة صلاحيتها وإنَّ التوقيع الإلكتروني قد تم إنشاؤه خلال الفترة المحددة في الشهادة وكذلك لتجنب أي تعديلٍ غيرِ مصرحٍ به من صاحب التوقيع خلال مدة الصلاحية[١٣٥٧].

ج– رقم مسلسل للشهادة، فكلُّ شهادةٍ تصدر عن جهة التصديق لابدَّ أن يكون لها رقمٌ مسلسلٌ، و الغرض من ذلك هو إدراج الشهادة وفق قاعدة بيانات يتم تحديثها بصورةٍ مستمرةٍ من أجل تحديد وبيان التغييرات التي تطرأ على الشهادات.

د– عنوان الموقع الإلكتروني المخصص لقائمة الشهادات الموقوفة أو الملغاة، فعند قيام جهة التصديق بإيقاف أية شهادة أو إلغائها، فإنه يلتزم بإنشاء موقع إلكتروني يتضمن سجلًا الكترونيًا متاحًا للمتعاملين يوضح فيه قائمةً بالشهادات الموقوفة والملغاة، فيجب عليها نشرها هذه الشهادات على موقعها الإلكتروني، حتى لا يتم الاعتماد على هذه الشهادات في التعامل، فيعد مقدم خدمات التصديق مخلًا بالتزامه و يتحمل ما ينشأ من ضررٍ نتيجة هذا الإخلال في حالة إذ يعتمد البعض في تعاملهم على شهاداتٍ موقوفةٍ أو ملغاةٍ لم يتم نشرها على الموقع الإلكتروني. هـ– الرقم السري للشهادة الإلكترونية.

٢– بياناتٌ تتعلق بصاحب التوقيع:

يجب أن تتضمن شهادة التصديق مجموعة من البيانات التى تخصُّ صاحبَ التوقيع وهي:

[١٣٥٧] د.عباس العبودي، تحديات الاثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ٢٠١٠، ص٢٢١.

أ- اسم صاحب التوقيع، سواء كان أسمُه الأصلي أو المستعار أو الشهرة في حالة الاستخدام لأحدهما، مع ملاحظة ما نصت عليه المادة (٤٦) من الترخيص رقم ١٠٣ لسنة ٢٠٠٦ الصادر من هيئة صناعة تكنولوجيا المعلومات في مصر والذي يتعلق بخدمة التسجيل وإصدار الشهادات أجاز للموقع أن يطلب خطِّيًا من جهة التصديق حجب البيانات المتعلقة به عن التداول كالاسم و العنوان وأي معلومات شخصية أخرى و التى تدرجها جهة التوثيق في الشهادة التى تصدرها. ب- صفة الموقع[١٣٥٨].

ج- بيانات التحقق من التوقيع (المفتاح العام)، حيث أنَّ الهدف من ذكر هذا المفتاح[١٣٥٩] هو لكي يقوم الطرف الأخر المتعامل مع الموقع بمطابقة المفتاح الخاص المرسل إليه مع المفتاح العام المثبت في الشهادة و بالتالي التأكد من هوية الموقع.

٣- بياناتٌ تتعلق بجهة التصديق:

يجب أن تتضمن شهادة التصديق مجموعةً من البيانات التى تخصُّ جهة التصديق وهي على النحو التالى:

أ- موضوع الترخيص الصادر لها موضحا فيه نطاقه، ورقمه، وتاريخ إصداره، وفترة سريانه، و ذلك بهدف منح المتعاملين المزيد من الثقة والطمأنينة بصلاحيته وأهلية مقدم خدمات التصديق وبالشهادة التى أصدرها.

ب- اسم، وعنوان الجهة المصدرة للشهادة، ومقرها الرئيسي، وكيانها القانوني، والدولة التابع لها، إذ يجب ذكر اسم وعنوان مقدم خدمات التوثيق وكذلك مقر عمله الرئيسي والدولة التابع لها إذا كان مقدم الخدمة أجنبيًا وكذلك عنوان الفرع إذا كان هنالك أكثر من فرع تابع لنفس المقدم، وذكر كيانه القانوني[١٣٦٠].

ج- هوية مقدم خدمات التصديق الإلكتروني التي أصدرها، وإمضاؤه الإلكتروني [١٣٦١]، حيث أنَّ الهدف من ذلك تحديدُ المسئولية القانونية لمصدر الشهادة، حتى يمكن معرفة عما إذ كان مرخصًا له أم لا، وكذلك فقد يسأل قانونا في حال تسريب منظومة فك الشفرة الخاصة ببيانات الشهادة، ولهذا لا بدَّ أن يكون اسمه معلومًا حتى يمكن تحديد مسئوليته القانونية إذا اقتضى الأمر ذلك؛ ويمكن اعتبار هذا التوقيع بمثابة تأكيد إضافي لصحة التوقيع الإلكتروني الموجود على السند الإلكتروني.

هذه البيانات الإلزامية التى نصت عليها اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري التى تم تعديلها بموجب القرار ٣٦١لسنة ٢٠٢٠وبعض قوانين الدول العربية، التى تلتزم بها جهات التصديق بإدراجها في شهادة التصديق الإلكتروني، بالإضافة إلى ذلك نصَّت اللائحةُ التنفيذية لقانون التوقيع الإلكتروني المصري، على البيانات الاختيارية

[١٣٥٨] حيث ذكرت اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري التى تم تعديلها بموجب القرار ٣٦١لسنة ٢٠٢٠صفة الموقع من ضمن البيانات في الشهادة إلا إنها لم توضح مدلولات هذا البيان فقد جاء مختصراً بدون أي إيضاح او تفاصيل يمكن الاستدلال بها على قصد المشرع،حيث نرى تقوم جهة التصديق بالتحقق من صفة الموقع وإدراجها في الشهادة سواء كانت شخصية أو وظيفية.

[١٣٥٩] د. سامح عبد الواحد التهامي،التعاقد عبر الإترنت، دار الكتب القانونية ،القاهرة، ٢٠٠٨، ص ٤٧٨ .

[١٣٦٠] د. حسن محمد بودي، التعاقد عبر الانترنت، دار الكتب القانونية ، مصر، ٢٠٠٩ ص٨٠.

[١٣٦١] د. عبد الفتاح بيومي حجازي، إثبات المعاملات الإلكترونية عبر الإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٩، ص١٧٠.

التى يمكن إدراجها في الشهادة مثل: ما يفيد اختصاص الموقع وصفته والغرض الذى تستخدم فيه الشهادة،حد قيمة التعاملات المسموح بها في الشهادة، مجالات استخدام الشهادة، و جديرٌ بالذكر أنَّ هذه البياناتِ التى تتضمنها الشهادة ينبغي أن تكون صحيحة، حيث لا يتحقق الغرض الذي أعدت الشهادة من أجله ولا تعزز الثقة بالتوقيع الإلكتروني مالم تكن الشهادة دقيقة فيما تحمله من بياناتٍ، لذا لا يعدُّ مقدم خدمات التصديق موفيًا بالتزامه إذا لم تكن الشهادة دقيقةً وصحيحةً في بياناتها.

وكذلك تعد هذه البيانات من الشروط الأساسية التى نصَّ عليها القانون المصري وقوانين بعض الدول العربية[١٣٦٢]، التى يجب توافرها من أجل اعتماد شهادة التصديق في التعاملات الإلكترونية، وحيث أنَّ بياناتِ شهادة المصادقة الإلكترونية هي مسئولية مزود خدمات المصادقة الإلكترونية وذلك في حالة عدم تدوين هذه البيانات ويسأل مقدم الخدمة عن تعويض الضرر الذي يلحق بالطرف المضرور من جراء هذا الخطأ[١٣٦٣].

حيث يذهب رأىٌ في الفقه إلى ضرورة اشتمال شهادة التصديق على بيانٍ يوضح الوضع المالي للموقع وفيما إذا كان هنالك أحكامٌ قضائيةٌ ضدهَّ من عدمه، وذكر رقم البطاقة الضريبية[١٣٦٤].

إلا أنَّ الراىَ محلُّ نقدٍ لأنه من غير المنطقي إطلاقًا ذكرَ هذا البيانِ في الشهادة، حيث لا نجد غالبًا مثل هذا البيان فيما يتعلق بالتعاملات التقليدية التى يجريها الموقع، فكيف نتصور وجوده في التعاملات الإلكترونية[١٣٦٥].

بالإضافة إلى ما تقدَّم فمن الضروري تعديلُ وتحديث هذه البياناتِ كلَّما دعت الحاجةُ إلى ذلك[١٣٦٦]، وهذا بالنسبة للبيانات الواردة في شهادة التصديق الإلكتروني والتى يتعلق بمقدم خدمات التصديق الإلكتروني من حيث هويته وبيان مسئوليته وحدودها، وما يتعلق بصاحب الشهادة والموقع، وما يتعلق بالشهادة ذاتها إذ تنص هذه البيانات تارةً على موضوع الترخيص وصلاحية الشهادة كتاريخ النفاذ والانتهاء، وتارةً أخرى تنص على نطاق الشهادة والمجالات التى من الممكن أن تستخدم فيها وكذلك بيانات المفتاح العام والرقم التسلسلي للشهادة.

الشرطُ الثالثُ – يجب في شهادة التصديق الإلكتروني أن تستجيب لمقتضيات السلامة والوثوق بها:

يجب أن تؤكد الشهادة أنَّ البيانات الموقَّعَ عليها بياناتٌ صحيحةٌ صادرةٌ عن الموقع، ولم يتم التلاعبُ فيها، ولم يطرأ عليها أي تعديلٍ سواءً بالحذف أو الإضافة أو التغير، ويتم ذلك باستخدام أنظمة معلوماتية متطورة تحقق الأمن وتخلق

[١٣٦٢] انظر: المادة (٢٢) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري رقم ١٥لسنة ٢٠٠٤، التى تم تعديلها بموجب القرار رقم ٣٦١لسنة ٢٠٢٠.

[١٣٦٣] انظر: الفصل ٢٢ من القانون المتعلق بالمبادلات و التجارة الإلكترونية التونسي رقم ٨٣ لسنة ٢٠٠٠.

[١٣٦٤] د.عباس العبودي، تحديات الاثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، مرجع سابق، ص٢١٩.

[١٣٦٥] د.غنى ريسان جادر الساعدى، د.أكرم تحسين محمد حسن، النظام القانوني لشهادة التوثيق الإلكتروني، دراسة مقارنة، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الثاني، ٢٠١٧، ص٥٩٠.

[١٣٦٦] د.سهى يحيى الصباحين، التوقيع الالكتروني وحجيته في الاثبات، رسالة دكتوراه، جامعة عمان العربية للدراسات العليا، الاردن، ٢٠٠٥ ، ص١٧٥.

الثقة لدى من يتعامل معولًا على هذه الشهادة[١٣٦٧]، ولذا يجب على جهة التصديق أن تستخدم بإصدارها للشهادة أنظمة تقنيات معلوماتية على مستوى عالٍ و موثوقٍ بها، بأن يكون بمنأى عن أي استعمالٍ غيرِ المشروع قانونًا، وتقدم مستوى معقولًا من الصحة والأمان، وأن تستخدم أنظمة أمن مقبولة وفق معطيات التقدم التقني و التكنولوجي، بالإضافة إلى أنَّ ممارسة نشاط إصدار شهادات التصديق الإلكترونية، يتطلب خبرةً معلوماتيةً في هذا المجال، ولالتزامها بالشروط والضوابط التقنية والفنية[١٣٦٨].

وتظهر أهمية المحافظة على شهادات التصديق الإلكتروني من الاستعمال غير المشروع، استنادًا إلى الدور الذي تؤديه هذه الشهادة،إذ تبعث في التوقيع الإلكتروني الموثوقية والاطمئنان لدى المتعاملين مع الموقع في التعاملات الإلكترونية، لدى تعويلهم على هذه الشهادة، حيث أنَّ تلك المحافظة تمنح التوقيع الإلكتروني الحجية القانونية في الإثبات، ولذلك يلزم من تلك الجهات أن تتخذ الاحتياطات اللازمة لحماية هذه الشهادات من الاختراق والعبث ببياناتها[١٣٦٩].

الفرعُ الثاني
متطلباتُ إصدارِ شهاداتِ التصديقِ الإلكترونيِ المؤهلةِ
في اللائحة الأوربية

لم تقتصر اللائحة الأوربية ٩١٠لسنة ٢٠١٤على تقديم خدمات التصديق الإلكتروني في إصدار شهادة التصديق على التوقيع الإلكتروني فقط كما هو منصوصٌ عليه في قانون التوقيع الإلكتروني المصري، بل تضمنت اللائحةُ الأوربيةُ شهاداتٍ أخرى لم تكن منصوصًا عليها في التوجيه الأوربي رقم ٩٣لسنة ١٩٩٩ الذي تم إلغاؤه، وهي شهادة الختم الإلكتروني، وشهادة مصادقة الموقع الإلكتروني، حيث فرقت اللائحة بين الشهادات المؤهلة للتوقيع الإلكتروني، والختم الإلكتروني، ومصادقة الموقع الإلكتروني الصادرة من مقدم خدمة ثقة مؤهل الذي يستوفى المتطلبات الواردة في الملحق الأول والثالث والرابع من اللائحة، وبين مقدم خدمة ثقة غير مؤهلٍ يصدر شهاداتٍ غيرَ مؤهلةٍ. حيث عرَّفت المادة الثالثة من اللائحة الشهادات المؤهلة، للتوقيع الإلكتروني، بأنها التى تصدر عن مزود خدمة ثقةٍ مؤهلٍ وتفي بالمتطلبات المنصوص عليها في الملحق الأول، و للختم الإلكتروني، بأنها التى يصدرها مزود خدمة ثقةٍ مؤهلٍ وتفي بالمتطلبات المنصوص عليها في الملحق الثالث، و مصادقة موقع الويب بأنها، التى تصدر عن مزود خدمة ثقة مؤهلٍ وتفي بالمتطلبات المنصوص عليها في الملحق الرابع، و طبقًا لهذه التعريفات يجب أن تفي هذه الشهادات المتطلبات المنصوص عليها في اللائحة وذلك على النحو الآتي:

أولًا– أن تصدر شهادات التصديق الإلكتروني المؤهلة من مقدم خدمةِ ثقةٍ مؤهلٍ:

[١٣٦٧] د. إبراهيم الدسوقي أبو الليل، توثيق التعاملات الإلكترونية و مسئولية جهة التوثيق تجاة الغيرالمضرور، مرجع سابق، ص ١٨٧٤.

[١٣٦٨] د. تامر محمد سليمان الدمياطي، إثبات التعاقد الإلكتروني عبر الإنترنت، مرجع سابق، ص ٥٦٥.

[١٣٦٩] د. عبد الفتاح بيومي حجازي، مقدمة في التجارة الإلكترونية، مرجع سابق، ص١٥١.

تقومُ اللائحةُ الأوربيةُ على مبدأ حرية تقديم خدمات الثقة، فيجوز لأي شخصٍ سواء كان طبيعيًا أو اعتباريًا في تقديم خدمة أو أكثر من خدمات الثقة المحددة في اللائحة، وعلى حرية مقدم خدمة الثقة في الحصول على صفه مؤهل والخدمات التي يقدمها صفة المؤهلة، ولكن إذا كان إخطار مقدم خدمة الثقة مؤهلًا و تكون الخدمات التى يقدمها مؤهله، فإن اللائحة تفرض عليه عند الحصول على صفة مؤهل، ويقوم بإصدار شهادات المؤهلة، للتوقيع الإلكتروني والختم الإلكتروني مصادقة موقع الويب، يجب أن يمتثل لمتطلبات لائحة الخدمات المؤهلة التى حصلت على الموافقة من الهيئة الإشرافية والتسجيل في القائمة الموثوق بها، ومع ذلك لن يمنع شىء نفس المقدم من تقديم خدماتٍ غيرِ مؤهلةٍ والتى لن تخضع بعد ذلك لمتطلبات اللائحة.

ثانيًا– إنشاء ملف لتسجيل طلبات الحصول على الشهادات المؤهلة وحفظه:

للحصول على شهادة مؤهلة للتوقيع الإلكتروني، تحت مسئولية الشخص الطبيعي، يجب أن يتضمن ملف التسجيل، طلبًا للحصول على شهادةٍ إلكترونيةٍ مؤرخةٍ أقل من ثلاثة أشهر وموقعةٍ من قبل مقدم الطلب، تشتمل على جميع العناصر اللازمة لإصدار الشهادة، و يجب أن يكون طلب الشهادة والشروط العامة للاستخدام موقعةً بإحدى الطريقتين:الأولي موقعةٌ بتوقيعٍ بخط اليد، والثانيةِ توقيعٌ إلكترونيٌّ باستخدام توقيع متقدم، وأن تكون شهادة التوقيع الإلكتروني شهادةً مؤهلةً.

للحصول على شهادةٍ مؤهلةٍ للختم الإلكتروني ومصادقة موقع الويب، تحت مسئولية الشخص الاعتباري، يجب أن يتضمن ملف التسجيل، طلبًا للحصول على شهادةٍ إلكترونيةٍ مؤرخةٍ أقل من ثلاثة أشهرٍ وموقعةٍ من ممثلٍ مفوضٍ للشخص الاعتباري، ويشمل على جميع العناصر اللازمة لإصدار الشهادة، وأن تكون طلب الشهادة الشروط العامة للاستخدام مؤرخةً وموقعةً بإحدى الطرقِ الآتية: الأولى موقعةٌ بتوقيعٍ بخط اليد، والثانيةِ التوقيعُ عليه إلكترونيًا باستخدام توقيع متقدم، والثالثةِ ختمٌ إلكترونيٌّ باستخدام ختم متقدم، فى الحالتين الأخيرتين يجب وأن تكون شهادة التوقيع الإلكتروني أو الختم الإلكتروني شهادةً مؤهلةً؛ ويجب الاحتفاظ بملفات التسجيل لمدة سبعة سنوات بعد انتهاء الشهادة موضوع الطلب(١٣٧٠).

ثالثًا– يجب أن تتضمنَ شهاداتُ التصديق الإلكترونية المؤهلة البيانات الأتية وذلك علي النحو الآتي:

١– بيانات الشهادات المؤهلة للتوقيعات الإلكترونية:

الإشارة على الأقل في شكلٍ مناسبٍ للمعالجة الآلية، إلى أنَّ الشهادة قد صدرت كشهادةٍ مؤهلةٍ للتوقيع الإلكتروني، و البيانات التى تمثل بشكل لا لبس فيه مقدم الخدمة الثقة المؤهل الذي يصدر الشهاداتِ المؤهلةَ، إذا كان شخصًا اعتباريًا أن يذكر الاسم ورقم التسجيل، كما هو مذكورٌ في السجلات الرسمية، وإذا كان شخصًا طبيعيًا يذكر اسم الشخص، و إذا تم استخدام اسمًا مستعارًا فيجب الإشارةُ إليه بوضوحٍ على الأقل اسمُ الموقع أو اسمٌ مستعارٌ، و بيانات

(١٣٧٠) Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet - Modalités de qualification selon le règlement eIDAS .des services qualifiés selon le RGS, version en vigueur.
Disponible sur http://www.ssi.gouv.fr

التحقق من صحة التوقيع الإلكتروني التى تتوافق مع بيانات إنشاء التوقيع الإلكتروني، و تفاصيل بداية ونهاية و فترة صلاحية الشهادة، و رمز هوية الشهادة، الذي يجب أن يكون فريدًا لمقدم خدمة الثقة المؤهل، و التوقيع الإلكتروني المتقدم أو الختم الإلكتروني المتقدم لمقدم خدمة الثقة المؤهل، الموقع الذي تتوفر فيه الشهادة التى تدعم التوقيع الإلكتروني المتقدم أو الختم الإلكتروني المتقدم على أن يكون مجانًا، و موقع الخدمات التى يمكن استخدامه للاستعلام عن حالة صلاحية الشهادة المؤهلة، و بيانات إنشاء التوقيع الإلكتروني المتعلقة ببيانات التحقق من صحة التوقيع الإلكتروني في جهاز إنشاء توقيع إلكتروني مؤهل، أن تكون على الأقل في شكلٍ مناسبٍ للمعالجة الآلية[١٣٧١].

٢- بياناتُ الشهاداتِ المؤهلةِ للأختامِ الإلكترونيةِ.

الإشارة على الأقل في شكلٍ مناسبٍ للمعالجة الآلية، إلى أنَّ الشهادةَ قد صدرت كشهادةٍ مؤهلةٍ للختم الإلكتروني، و البيانات التى تمثل بشكلٍ لا لبس فيه مقدم الخدمة الثقة المؤهل الذي يصدر الشهادات المؤهلة، إذا كان شخصًا اعتباريًا أن يذكر الاسم ورقم التسجيل، كما هو مذكورٌ في السجلات الرسمية، وإذا كان شخصًا طبيعيًا يذكر اسم الشخص، و اسم منشيء الختم ورقم التسجيل، كما هو مذكورٌ في السجلات الرسمية، و بيانات التحقق من الختم الإلكتروني، والتى تتوافق مع بيانات إنشاء الختم الإلكتروني، و تفاصيل بداية ونهاية و فترة صلاحية الشهادة، و رمز هوية الشهادة الذي يجب أن يكون فريدًا لمقدم خدمة الثقة المؤهل، و التوقيع الإلكتروني المتقدم أو الختم الإلكتروني المتقدم لمقدم خدمة الثقة المؤهل، والموقع الذي تتوفر فيه الشهادة التى تدعم التوقيع الإلكتروني المتقدم أو الختم الإلكتروني المتقدم على أن يكون مجانًا، و موقع الخدمات التى يمكن استخدامها للاستفسار عن حالة صلاحية الشهادة المؤهلة، و بيانات إنشاء الختم الإلكتروني المتعلقة ببيانات التحقق من الختم الإلكتروني في جهاز إنشاء ختم إلكتروني مؤهل، أن تكون على الأقل في شكلٍ مناسبٍ للمعالجة الآلية[١٣٧٢].

٣- بياناتُ الشهاداتِ المؤهلةِ لمصادقةِ موقعِ الويبِ.

الإشارة على الأقل في نموذجٍ مناسبٍ للمعالجة الآلية، إلى أنَّ الشهادة قد صدرت كشهادةٍ مؤهلةٍ لمصادقة موقع الويب، و البيانات التى تمثل بشكلٍ لا لبس فيه مقدم الخدمة الثقة المؤهل الذي يصدرُ الشهاداتِ المؤهلةَ، بالنسبة للشخص الاعتباري يذكر الاسم ورقم التسجيل، كما هو مذكورٌ في السجلات الرسمية، وبالنسبة للشخص الطبيعي يذكر اسم الشخص، و إذا كانت الشهادة للشخص الطبيعي أن يذكر اسم الشخص الذي صدرت له الشهادة، أو اسمه المستعار، إذا تم استخدام اسم مستعار فيجب الإشارة إليه بوضوح، و أما إذا كانت الشهادة للشخص الاعتباري أن يذكر اسم الشخص الاعتباري الذي صدرت له الشهادة ورقم التسجيل، كما هو مذكورٌ في السجلات الرسمية، و محل الإقامة للشخص الطبيعي أو الاعتباري الذي صدرت له الشهادة، كما هو موضحٌ في السجلات الرسمية، و النشاط الذي يديره الشخص الطبيعي أو الاعتباري الذي صدرت له الشهادة، و تفاصيل بداية ونهاية فترة صلاحية الشهادة، و رمز هوية الشهادة الذي يجب أن يكون فريدًا لمقدم خدمة الثقة المؤهل، و التوقيع الإلكتروني المتقدم أو الختم

([١٣٧١]) انظر: الملحق الأول من اللائحة الأوربية رقم ٩١٠لسنة ٢٠١٤.

[١٣٧٢] انظر: الملحق الثالث من اللائحة الأوربية ٩١٠لسنة ٢٠١٤.

الإلكتروني المتقدم لمقدم خدمة الثقة المؤهل، الموقع الذي تتوفر فيه الشهادة التى تدعم التوقيع الإلكتروني المتقدم أو الختم الإلكتروني المتقدم على أن يكون مجانًا، و موقع الخدمات التى يمكن استخدامها للاستفسار عن حالة صلاحية الشهادة المؤهلة[١٣٧٣].

يتضح مما سبق أن شهادة التصديق على التوقيع الإلكتروني تختلف عن شهادة التصديق على الختم الإلكتروني، وتكمن أوجه الاختلاف في الآتي:

الاختلافُ الأول: يكمن في أنَّ شهادةَ التوقيع الإلكتروني بأنها "شهادةٌ إلكترونيةٌ ترتبط بها بيانات التحقق من التوقيع الإلكتروني لشخصٍ طبيعيٍّ ويؤكد على الأقل الاسم أو اسمًا مستعارًا لهذا الشخص" كما تستخدم المواد المتعلقة بالتوقيع الإلكتروني مصطلح "موقّع" المعرّف في المادة الثالثة البند التاسع بأنه" يعني الشخص الطبيعي الذي ينشئ توقيعًا إلكترونيًا".

وتسمح اللائحة الأوربية باستخدام الأسماء المستعارة في المعاملات الإلكترونية[١٣٧٤]، وبشكلٍ خاصٍّ في شهادات التوقيع الإلكتروني[١٣٧٥]، و يجب أن يذكر بوضوح أن هذا اسم مستعار؛ ومع ذلك لا تنصُّ اللائحة على أي التزامٍ على مقدم خدمة الثقة فى الحفاظ على هوية الأشخاص الذين يختبئون وراء اسمٍ مستعارٍ، و قد يكون ضروريًا في سياق الإجراءات القانونية تحديد الهوية الأشخاص عملاً بالقانون الوطني.

وجديرٌ بالذكر أن المشرَّع البلجيكيَّ نصَّ على أنه عندما يستخدم حائز شهادة التوقيع الإلكتروني اسمًا مستعارًا، يتعين على مقدم الخدمة الثقة الذي أصدر الشهادة إبلاغ السلطات الإدارية أو القضائية المختصة، بناءً على طلبها بالمعلومات المتعلقة بهوية صاحبها التى تحت تصرفها اللازمة للتحقيق والكشف عن الانتهاكات، ينفذ حامل شهادة الختم الإلكتروني المؤهلة التى تم إنشاؤها في بلجيكا، التدابير اللازمة حتى يتمكن من تحديد اسم وسلطات الشخص الطبيعي الذي يمثل الشخص الاعتباري والذي يستخدم عمليًا ختمًا إلكترونيًا مؤهلًا، للسلطات الإدارية أو القضائية المختصة التى تعمل في سياق التحقيق والكشف عن الانتهاكات، وتحديد هوية وسلطات الممثل القانوني للشخص الإعتباري [١٣٧٦].

أما بخصوص شهادات الأختام الإلكترونية، فهذه الخدمة الموثوقة الجديدة التى أنشأتها اللائحة الأوربية تسمح بالتصديق على العلاقة بين البيانات الإلكترونية المختومة والشخص المعنوي، أي إنه ختم إلكتروني آمن مخصص للأشخاص الاعتباريين، و من الناحية العملية التكنولوجيا وأدوات الأجهزة والبرمجيات المستخدمة لإنشاء الختم الإلكتروني هي نفسها المستخدمة لإنشاء التوقيع الإلكتروني، الا أن الختم الإلكتروني يختلف عن التوقيع الإلكتروني

[١٣٧٣] انظر: الملحق الرابع من اللائحة الأوربية ٩١٠لسنة ٢٠١٤ .

[١٣٧٤] انظر: المادة الخامسة في البند الثاني من اللائحة الاوربية.

[١٣٧٥] وجديرٌ بالذكر إنه غير مسموح باستخدام أسماء مستعارة في الشهادات المؤهلة للأختام الإلكترونية.

[١٣٧٦] انظر: المادة الثانية عشر من القانون البليجكي الذي ينفذ اللائحة الأوربية وينظم الأرشفة الإلكترونية رقم ٢١لسنة ٢٠١٦.

في أن الأول مخصص للشخص الطبيعي أما الثاني مخصص للأشخاص الاعتباريين، وأن مستخدم التوقيع هو صانع التوقيع الإلكتروني هو الذي تم تحديده في شهادة التصديق هو شخصٌ طبيعيٌّ، أما مستخدم الختم هو صانع الختم.

أما تعريف شهادة الختم الإلكتروني فهى شهادةٌ إلكترونيةٌ تربط بين بيانات التحقق من ختم إلكتروني لشخصٍ قانونيٍّ وتأكيد اسم هذا الشخص؛ وبالتالي لا تحدد شهادة الختم الإلكتروني أي شخصٍ طبيعيٍّ، و يجب على مقدم خدمة الثقة الذي يصدر هذه الشهادة تنفيذ التدابير اللازمة لتكون قادرة على تحديد هوية الشخص الطبيعي الذي يمثل الشخص الاعتباري الذي تُمنح له الشهادة المؤهلة للختم الإلكتروني.

ويكمن الاختلاف الأساسي الثاني في التأثيرات المرتبطة بالتوقيع والختم الإلكتروني، في الواقع أن المادة (٣/١٠) تحدد بوضوح التوقيع الإلكتروني على أنه "بياناتٌ في النموذج الإلكتروني يستخدمه الموقع للتوقيع"، يعني التوقيع المكتوب بخط اليد ليس فقط في تعريف نفسه كمؤلف المستند ولكن أيضًا موافقة صريحة على محتوى هذا الأخير، باستخدام توقيعه بخط اليد وبالتالي يكون لديه قوة جذابة للشخص الطبيعي الذي يستخدمه، على النقيض من ذلك تعرف المادة (٣/٢٥) الختم الإلكتروني بأنه "البيانات في شكل إلكتروني، التي يتم ربطها أو ربطها منطقيًا ببياناتٍ أخرى في شكلٍ إلكترونيٍّ لضمان أصل وسلامة هذا الأخير "؛ يتضح من نص هذه المادة أنها حريصة على عدم استخدام الفعل "علامة" لختم إلكتروني، وبالتالي لا تنص اللائحة على أن الختم الإلكتروني وحده يمكنه ذلك الربط القانوني للشخص الاعتباري[١٣٧٧]، من الواضح أن اللائحة الأوربية لم ترغب في لمس القواعد الوطنية لتمثيل الأشخاص الاعتباريين[١٣٧٨].

على عكس بلجيكا أو إسبانيا الذين يعرفون توقيع الأشخاص الاعتباريين، لذلك تأذن بإمكانية استخدام شهادة توقيع تحدد هوية الشخص الاعتباري من الناحية القانونية، فإن الدول الأخرى لم تظهر مثل هذا الانفتاح لتجنب خطر الارتباك وأيضًا احترام تنوع النظم القانونية ولذلك اختارت اللائحة إنشاء خدمتين موثوقتين منفصلتين وفقًا لفئة المستخدم (الشخص الطبيعي أو الاعتباري) وقصر الغرض من الختم الإلكتروني على ضمان أصل وتكامل البيانات التى يغطيها هذا الختم، يمكن أن يؤدي استخدام الختم الإلكتروني إلى إلزام الشخص الاعتباري بشكلٍ مباشرٍ من الناحية القانونية استخدام الختم الإلكتروني، بالنسبة للبلدان التي تعرف بالفعل التوقيع الإلكتروني للأشخاص الاعتباريين، لم يعد من الممكن إصدار شهادة توقيع إلكترونية باسم شخص اعتباري، لذلك سيتعين على هذه البلدان استخدام شهادات الختم الإلكترونية[١٣٧٩].

[١٣٧٧] في هذا الصدد تنص الفقرة ٥٨من مقدمة اللائحة الأوربية على إنه: عندما تتطلب معاملة ما ختمًا إلكترونيًا مؤهلًا من شخص قانوني، يجب أن يكون التوقيع الإلكتروني المؤهل من الممثل المفوض للشخص القانوني مقبولًا على قدم المساواه.

[١٣٧٨] انظر: Sur la question de la signature des personnes morales en droit belge, voy. B. VANBRABANT, , « La signature électronique des personnes morales », in La preuve, Liège, Formation permanente CUP, 2002, vol. 54, pp. 173 à228 ;D. MOUGENOT, La preuve, tiré à part du Répertoire Notarial, 4ème édition, Larcier, Juin 2012, pp. 216-217. En droit français, voy. E. Caprioli, Signature électronique et dématérialisation, LexisNexis, 2014, pp.166 à 168.

[١٣٧٩] انظر:

أما بخصوص تقديم شهادة مصادقة الموقع حيث أن الهدف منها هو ضمان صحة الرابط بين موقع الويب ومديره؛ في الواقع، لم نعد نعول حتى يومنا هذا عدد الشركات التى تقع ضحية النصب الاحتيالي، أي المحتالين الذين ينشئون مواقع زائفة عبر الإنترنت، من أجل انتحال هوية شركة شخص طبيعي وبالتالي استخراج مبالغ مالية من مستخدمي الإنترنت الذين هم ساذجون قليلًا، فهى تهدف بشكل أساسى إلى الضمان لمستخدمى الإنترنت، وتعزيز مناخ الثقة في المعاملات التجارية عبر الإنترنت، من خلال شهادة مؤهلة مصادقة الموقع وصحة وشرعية الموقع وحقيقة أن الشخص الجسدي المشار إليه هو المسئول عن الموقع.

وجديرٌ بالذكر إن المادة (٤٥) من اللائحة الأوربية الوحيدة المخصصة لهذه الخدمة لا تذكر الآثار القانونية المرتبطة بهذه الخدمة؛ وعليه يعود للقاضي تبعًا لظروف القضية، تحديد الآثار القانونية التي يمكن أن يستند إليها، خاصة فيما يتعلق بالضمانات المقدمة من الشهادة المؤهلة المرتبطة بتلك الخدمة، ولكنها تشترط في الشهادات المؤهلة لمصادقة موقع الويب أن تستوفى الشروط المنصوص عليها في الملحق الرابع من اللائحة الأوربية، و أن تحتوي هذه الشهادة بشكلٍ خاصٍّ على تفاصيل الاتصال بمزود الخدمة الذي أصدر الشهادة، وتفاصيل الاتصال بالشخص الطبيعي أو الاعتباري الذي يشغل الموقع وكذلك اسم النطاق الذي يديره هذا الشخص من أجل القيام به، ويمكن الوصول إليها على موقعها على الإنترنت؛ و يجب عليه أن لا يصدر الشهادة المؤهله دون التحقق من المعلومات الموضحة في الشهادة المذكورة [١٣٨٠].

المطلبُ الثالثُ

الآثارُ القانونيةُ المترتبةُ علي إصدارِ شهادةِ التصديقِ الإلكترونيَّ

تمهيدٌ وتقسيمٌ:

نظرًا لخطورة وأهمية الدور الذى تقوم به شهادة التصديق الإلكتروني، في تأكيد صحة وسلامة المحرر الإلكتروني، وإلزام موقع المحرر بمضمونه، ولذلك يثيرُ التساؤلُ، حول القيمة القانونية لشهادة التصديق الإلكتروني، الصادرة عن مقدم خدمات التصديق الإلكتروني الوطني أو الأجنبي، وما هي الشروط الواجب توافرها بشهادة التصديق الإلكتروني، حتي تتمتع بالحجية في الإثبات، ولذلك سوف نتناول ذلك من خلال فرعين: نخصَّصُ الأول مدى حجية شهادة التصديق الإلكتروني الوطنية، ونبيِّنُ في الثاني مدى حجية شهادة التصديق الإلكتروني الأجنبية.

الفرعُ الأولُ

مدى حجيَّةِ شهادة التصديق الإلكتروني الوطنية

D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et lesservices de confiance (eIDAS) : analyse approfondie », février 2015, dossier publié sur le site,p.26. www.droit-technologie.org

[١٣٨٠] وجديرٌ بالذكر ان التكنولوجيا المستخدمة لمصادقة الموقع، هي نفس التكنولوجيا المستخدمة للتوقيع الإلكتروني أو الختم الإلكتروني.

و سوف نقوم بالتعرف على القيمة القانونية لشهادة التصديق الإلكتروني الصادرة من مقدم خدمات التصديق الإلكتروني الذي يخضع للقانون الوطني سواء في قانون التوقيع الإلكتروني المصري وفي اللائحة الأوربية وذلك على النحو الآتي:

أولًا– موقفُ المشرِّع المصريَّ من حجيَّةِ شهادة التصديق الإلكتروني الوطنية:

حيث اشترط المشرِّعُ المصريُّ لمنح التوقيع الإلكتروني وكذلك شهادة التصديق الصادرة بشأنه الحجية القانونية في الإثبات، توافر الشروط المنصوص عليها في المادة (١٨) من هذا القانون و هي: الاول ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره، و الثانى سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني، و الثالث إمكانية كشف أي تعديلٍ أو تبديلٍ في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني، وتحدد اللائحة التنفيذية لهذا القانون الضوابط الفنية والتقنية اللازمة لذلك.

وبالرجوع إلي اللائحة التنفيذية لقانون تنظيم التوقيع الإلكتروني، الصادرة بموجب القرار الوزاري رقم ١٠٩ لسنة ٢٠٠٥ التى تم تعديلها بموجب القرار رقم ٣٦١لسنة ٢٠٢٠، نجد أنها وضحت كيفية إعمال هذه الشروط وذلك على النحو التالى:

فيما يتعلق بالشرط الأول: من حيث ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره، فإن ذلك يتحقق إذا كان التوقيع مستندًا إلى منظومة تكوين بيانات إنشاء توقيع إلكتروني مؤمنةٍ، وأن يكون التوقيع مرتبطًا بشهادة تصديق إلكتروني معتمدةً ونافذة المفعول صادرةً من جهة تصديقٍ إلكترونيٍّ مرخصٍ لها أو معتمدةٍ[١٣٨١]، و هذا الشرط يعني أن يدل التوقيع الموجود على المحرر بأنه ينسب إلى شخصٍ معينٍ، حتى يقوم التوقيع الإلكتروني بوظيفته بالإثبات يلزم أن يكون التوقيع دالًا على شخصية صاحبه و مميزًا عن غيره من الأشخاص، فطريقة التوقيع تحدد شخصية الموقع، ويكون ذلك باتخاذ التوقيع الإلكتروني شكل أرقام أو حروف مميزة لشخصية الموقع وتميزه عن غيره[١٣٨٢].

فيما يتعلق بالشرط الثاني: المتعلق بسيطرة الموقع وحده على الوسيط الإلكتروني حيث عرف قانون التوقيع الإلكتروني، الوسيط الإلكتروني في المادة (١/د) بأنه" أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني"، فقد حددت المادة الحادية عشر من اللائحة التنفيذية لقانون التوقيع الإلكتروني التى تم تعديلها بموجب القرار ٣٦١لسنة ٢٠٢٠، كيفية سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني المستخدم فى عملية تثبيت التوقيع الإلكتروني، عن طريق حيازة الموقع لأداة حفظ المفتاح الشفري الخاص المتضمنة البطاقة الذكية المؤمنة و الكود السري المقترن بها، و وهذا

[١٣٨١] انظر : المادة (٩) من الائحة التنفيذية لقانون التوقيع الإلكتروني ١٥ لسنة ٢٠٠٤.

[١٣٨٢] ألاء أحمد محمد الحاج علي، التنظيم القانوني لجهات التصديق التوقيع الإلكتروني، رسالة ماجستير، جامعة النجاح الوطنية، فلسطين،٢٠١٣،ص ٧٥ .

يعني أن تكون الوسيلة المستخدمة لإنشاء التوقيع خاضعةً لسيطرة الموقع دون غيره، وبهذا يضمن عدم تحكم أي شخصٍ آخرَ سوى الموقع بالمفتاح الخاص، مما يضمن تعيين هوية الموقع بدقة[١٣٨٣].

فيما يتعلق بالشرط الثالث: الخاص بإمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني الموقع إلكترونيًا، فإن هذا الأمر يتحقق باستخدام تقنية شفرة المفتاحين العام والخاص، وبمضاهاة شهادة التصديق الإلكتروني وبيانات إنشاء التوقيع الإلكتروني بأصل هذه الشهادة وتلك البيانات[١٣٨٤].

بالرجوع إلي المادة التاسعة من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري التى تم تعديلها بموجب القرار ٣٦١لسنة ٢٠٢٠، أنها منحت حجية الإثبات المقررة للكتابة الإلكترونية الرسمية أو العرفية لمنشئها، ولكنها وضعت الشروط والضوابط لهذه الحجية في الإثبات وهى، أن تكون الكتابة الإلكترونية محددًا مصدر، و وقت وتاريخ إنشائها، و أن تخضع لنظام حفظ إلكتروني، و غير خاضعه لمنشئ الكتابة الإلكترونية لعدم العبث بهذه الكتابة، و أن تكون مرتبطة بشهادة تصديق إلكتروني وصادرة من جهةٍ مرخصٍ لها بذلك حتى تتمتع الكتابة الإلكترونية أو المحررات الإلكترونية بالحجية القانونية في الإثبات.

وحيث اعترفت محكمة النقض المصرية بحجَّية الكتابة الإلكترونية في الإثبات، إنه لا يجوز جحدها وطلب تقديم أصولها، إنما يجوز فقط المبادرة إلى الادَّعاءِ بتزويرها[١٣٨٥]. بالتالي نجد المشرَّعَ و القضاء المصري ساوى بين المستندات الإلكترونية والمستندات الخطَّية ومنحها الحجية التي تتمتع بها المستندات الورقية في الإثبات.

ثانيًا : موقف اللائحة الأوربية من حجية شهادة التصديق الإلكتروني الصادرة من مقدم خدمة الثقة في دول الاتحاد الأوربي.

حيثُ تستفيدُ جميع خدمات الثقة المؤهلة من تخفيف عبء الإثبات على المستخدم في حالة النزاع، و بند الافتراضات المنصوص عليه في اللائحة الأوربية، لذا تشير المادة (٢/٢٥) إلى أنَّ الأثرَ القانوني للتوقيع الإلكتروني المؤهل يعادل ذلك توقيعًا مكتوبًا بخط اليد، ويستفيد أيضًا من افتراض سلامة البيانات ودقة أصل البيانات التي ترتبط بالتوقيع الإلكتروني، و المادة (٢/٣٥) على أن الختم إلكتروني المؤهل يستفيد من افتراض سلامة البيانات ودقة أصل البيانات التى ترتبط بالختم الإلكتروني المؤهل[١٣٨٦].

[١٣٨٣] عبير ميخائيل الصفدي، النظام القانوني لجهات التوثيق الإلكتروني، رسالة ماجستير،جامعة الشرق الأوسط للدراسات العليا، فلسطين،٢٠٠٩، ص١٠٥وما بعدها.

[١٣٨٤] انظر: المادة (١٢) من اللائحة التنفيذية لقانون التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤.

[١٣٨٥] الطعن رقم ١٧٦٨٩ لسنة ٨٩ قضائية، الدائرة التجارية جلسة ٢٠٢٠/٣/١٠.

[١٣٨٦] انظر:

Pour un commentaire relatif à la clause d'assimilation dans le cadre de la signature électronique, voy. E.MONTERO, « Définition et effets juridiques de la signature électronique en droit belge : appréciation critique », in La Preuve, Formation permanente CUP, Liège, Volume 54, mars 2002, p. 75-81 ; B. DE GROOTE, « Het bewijs in de elektronische handel – Enkele bedenkingen », A.J.T., 2001, pp. 881-901 ; P. LECOCQ et B. VANBRABANT, « La preuve du contrat conclu par voie électronique » in Le commerce électronique : un nouveau mode de contracter ?Editions du jeune barreau de Liège, 2001, pp.

على العكس من ذلك، تستفيد خدمات الثقة غير المؤهلة ببساطةٍ من شرط عدم التمييز والذي يتمثل في اعتبار أنَّ الأثرَ القانونيَّ لخدمة الثقة غيرِ المؤهلةِ مقبولٌ كدليلٍ أمام المحكمة لا يمكن رفضه لمجرد أن هذه الخدمة نموذج إلكتروني أو أنه لا يفي بمتطلبات نفس خدمة الثقة المؤهلة في حالة وجود نزاع، فإن الأمر متروك لمستخدم هذه الخدمات لتقديم دليل على ذلك موثوق فيه يكفي لمحاولة إقناع القاضي بأنهم يقدمون الضمانات المتوقعة من هذه الخدمات بشكل طبيعي [١٣٨٧]. و بناءً على ما سبق سوف نقوم بتوضيح مدى حجية شهادات التصديق الإلكتروني الصادرة من مقدم خدمة الثقة في اللائحة الأوربية وذلك على النحو الآتي:

أولًا: مدى حجِّية شهادة التصديق على التوقيع الإلكتروني: حيث اشترطت اللائحة الأوربية للاعتراف بالقيمة القانونية لشهادة التصديق على التوقيع الإلكتروني الصادرة من مقدم خدمة ثقة وطني، أن تكون التوقيعاتُ الإلكترونيةُ متقدمةً، بناءً على شهادةٍ مؤهلةٍ، والتى يتم إنشاؤها باستخدام جهازٍ مؤهلٍ لإنشاء توقيع إلكتروني، وذلك حتى تستفيد من الآثار القانونية المنصوص عليها في المادة ٢٥ من لائحة [eIDAS].

ثانيًا: مدى حجية شهادة التصديق على الأختام الإلكترونية: حيث اشترطت اللائحة الأوربية للاعتراف بالقيمة القانونية لشهادة التصديق على الأختام الإلكترونية الصادرة من مقدم خدمة ثقة وطني، أن تكون الأختامُ الإلكترونيةُ متقدمةً، بناءً على شهادةٍ مؤهلةٍ، والتى تم إنشاؤها باستخدام جهازٍ مؤهلٍ لإنشاء ختمٍ إلكترونيٍّ مؤهلٍ، وذلك حتى تستفيد من الآثار القانونية المنصوص عليها في المادة ٣٥ من لائحة [eIDAS].

وبناءً على توافر هذه الشروط تستفيد شهادة التصديق على التوقع الإلكتروني المؤهل من الآثار القانونية المنصوص عليها في المادة ٢٥، و تستفيد شهادة التصديق على الأختام الإلكترونية المؤهلة من الآثار القانونية المنصوص عليها في المادة ٣٥ من لائحة [eIDAS]، و هي لا يجوز حرمان أي توقيعٍ أو ختمٍ إلكترونيٍّ من الآثار القانونية والمقبولية كدليلٍ في الإجراءات القانونية فقط على أساس أنها في شكل إلكتروني أو أنها لا تفي بمتطلبات التوقيعات الإلكترونية المؤهلة أو الأختام الإلكترونية المؤهلة، وحيث يتمتع بافتراض سلامة البيانات وصحة أصل تلك البيانات التى يرتبط بها التوقيع الإلكتروني المؤهل أو الختم الإلكتروني المؤهل، و لكن هذه الحجية مفترضة قابلة لإثبات عكسها، ويقع على من يدَّعي خلاف ذلك عبء الإثبات.

الفرعُ الثاني

مدى حجَّية شهادةِ التصديقِ الالكترونيَّ الأجنبيةِ

شهادة التصديق الإلكتروني الأجنبية هي شهادةٌ مؤمنةٌ بواسطة التوقيع الإلكتروني والصادرة من جهات تصديقٍ أجنبيةٍ ومعترفٌ بها وتشهد بصحة البيانات التى تتضمنها و تماثل نظيرتها من الشهادات الصادرة داخل إقليم

(١٣٨٧) D. GOBERT, « Le règlement européen du 23 juillet 2014 surl'identification électronique et lesservices de confiance (eIDAS) : analyse approfondie" op.cit.p.28.

112 et s. ; M. E. STORME, « De invoering van de elektronische handtekening in ons bewijsrecht – Een inkadering van en commentaar bij de nieuwe wetsbepalingen », R.W., 9 juin 2001, n° 41, pp. 1505-1525.

الدولة[١٣٨٨]، و حيثُ يثير التساؤل عن مدى حجية شهادة التصديق الالكترونية الأجنبية في الإثبات فهل تعاملت التشريعات في الدول، مع شهادة التصديق الاجنبية، كأنها شهادةُ تصديقٍ إلكترونيةٍ صادرةٍ من مقدم خدمة تصديق وطنية، واعترفت بها دون شرطٍ أو قيدٍ، أم أنَّ هذه التشريعاتِ اشترطت شروطًا معينةً، للاعتراف بحجَّية شهادة التصديق الاجنبية؟ والإجابة على هذا التساؤل سوف نتناول موقف المشرِّعِ المصريَّ، واللائحة الأوربية.

أولًا: موقفُ المشرِّع المصريَّ من حجَّية شهادة التصديق الإلكتروني الأجنبية.

قد اشترط قانون التوقيع الإلكتروني في المادة (٢٢) للاعتراف بحجَّية شهادة التصديق الأجنبية، أن يتمَّ الاعترافُ أولًا بمقدم خدمات التصديق الأجنبي، وهذا أمرٌ يقع على عاتق هيئة تنمية صناعة تكنولوجيا المعلومات لتنظيمه، ولاشكَّ في سلامة قصر هذا الاختصاص على الهيئة المذكورة لأنها تمثل الحكومة المصرية؛ وأن يكون هذا الاعتماد نظير مقابل يحدده مجلس إدارة الهيئة، يتعين على رئيس مجلس إدارة الهيئة أن يصدر قرارًا تنظيميا يتضمن قواعد عامة تحدد قيمة هذا المقابل والقواعد المتعلقة بسداده.

ويرى بعض الفقه[١٣٨٩]" أنه يجوز أن يكون هذا الاعتماد مجانًا، وذلك تأسيسًا على أنَّ نصَّ المادة (٢٢) من قانون التوقيع الإلكتروني لا تتعلق بالنظام العام ولم يرد فيه ما يفيد أنه نص أمر، ومن ثم فأنه تعد من القواعد القانونية المكملة التى تجوز للأفراد الاتفاق على استبعاد حكمها".

حيثُ أنه باعتماد الجهة المختصة بإصدار شهادات التصديق الإلكتروني الاجنبية تتمتع الشهادات التى تصدرها بذات الحجية في الإثبات المقررة لشهادات التصديق الالكتروني الكائنة في مصر؛ كما نجد أن دور هيئة تنمية صناعة تكنولوجيا المعلومات ينحصر في اعتماد شهادات التصديق الإلكتروني الصادرة من الجهة الأجنبية، وليس إصدار تراخيص لهذه الجهات، حيثُ أنَّ الترخيصَ لها بإصدار شهادات التصديق الإلكتروني قد صدر لها من جهة الترخيص في بلدها.

تعقيبٌ علي موقف القانون المصري من حجية شهادة التصديق الأجنبية:

أولًا: ينعقد الاختصاص في القانون المصري باعتماد الأجنبية المختصة بإصدار شهادات التصديق الإلكتروني إلى هيئة تنمية صناعة تكنولوجيا المعلومات وحدها، مما لا شكَّ في سلامة قصر هذا الاختصاص على الهيئة لأنها تمثل الحكومة المصرية.

ثانيًا: لا تعتمد هيئة تنمية صناعة تكنولوجيا المعلومات شهادات التصديق الإلكتروني الأجنبية ذاتها، إنما تعتمد الجهات المختصة المصدرة لهذه الشهادات، حيث يعتبر مسلك المشرِّع المصريَّ في ذلك محمودًا، لأن اعتماد شهادات

[١٣٨٨] د. خالد مصطفي فهمي، إبرام العقد الإلكتروني في ضوء التشريعات العربية والمنظمات الدولية، دار الجامعة الجديدة، الاسكندرية،٢٠٠٧، ص١٦٥.

[١٣٨٩] د. أيمن سعد سليم، التوقيع الالكتروني، دراسة مقارنة، مرجع سابق، ص٤٤.

التصديق الإلكترونية الأجنبية ذاتها، يعني ضرورة تقديم كلَّ شهادةٍ على حداها للهيئة لاعتمادها، مما يؤدي ذلك إلى تعقيد وبيروقراطية في الإجراءات.

ثالثًا: لم ينص المشرِّع المصريَّ على مبدأ المعاملة بالمثل، بحيث لا يعتد في مصر بشهادات التصديق الإلكتروني الأجنبية إلا إذا كانت دول إصدار هذه الشهادات تعتد بشهادات التصديق الإلكتروني الصادرة في مصر، و حيث نرى كان يجب على المشرِّعِ المصريَّ النصُّ على مبدأ المعاملة بالمثل، لأنَّ هذا المبدأ من المعايير الدولية التى تحكم علاقات الدول ببعضها البعض، حيث لا يمكن لمشرِّعٍ وطنيٍّ يعترف بالوثائق الأجنبية، لإنتاج آثارٍ قانونيةٍ على أراضيها مالم تكن تشريعات تلك الدول تعترف بذات الوثائق الوطنية على أراضيها هي الأخرى.

ثانيًا: موقف اللائحة الأوربية من حجية شهادة التصديق الأجنبية.

في اقتصاد عالم بيئة الإنترنت لا تعرف حدودًا لم تستطع اللائحة الأوربية الاستغناء عن حكم لتمديد أثار تقديم خدمات الثقة المفيدة إلى خارج الاتحاد الأوربي، بالرجوع إلى المادة الرابعة عشر نجد إن اللائحة الأوربية اعترفت بحجية شهادة التصديق الأجنبية الصادرة من مقدم خدمة ثقة أجنبي، ولكن في حالتين وذلك على النحو الآتي:

الحالة الأولى– أن تكون الخدمات الموثوقة التى يقدمها مقدم الخدمة الثقة مساوية من الناحية القانونية لخدمات الثقة المؤهلة التى يقدمها مقدمو خدمات الثقة المؤهلون في الاتحاد الأوربي.

الحالة الثانية– أن يكون هناك اتفاق مبرم بين الاتحاد الأوربي والبلد الأجنبي أو منظمة دولية بشأن الاعتراف بمقدم خدمات الثقة والخدمات التى يقدمها.

مما لا شكَّ فيه إن الاتفاقات الدولية فقط تضمن الآن الاعتراف بخدمات الثقة المؤهلة ولكن بشرط أن تضمن الاتفاقية خضوع مقدمى الخدمات المقيمين في بلد ثالث لنفس المتطلبات المطبقة على مقدمى الخدمات الثقة في الاتحاد الأوربي، أي جميع المتطلبات الواردة في اللائحة الأوربية، بما في ذلك تلك المتعلقة بالرقابة، وإجراءات الترخيص المسبق و التسجيل في القائمة الموثوقة؛ وكذلك فإنَّ الاتفاقاتِ الدوليةَ تؤدي إلى الاعتراف بخدمات الثقة المؤهلة التى يقدمها مقدمو خدمات الثقة المؤهلون في الاتحاد الأوربي من قبل الدولة الأخرى أو منظمة دولية التى أبرمت الاتفاق وذلك تطبيقًا لمبدأ المعاملة بالمثل.

المبحثُ الثاني

الخدماتُ الأخرى التي يقدمُها مقدمُ خدماتِ التصديقِ الإلكترونيِّ

تمهيدٌ وتقسيمٌ:

اقتصر المشرِّعُ المصريُّ على تقديمه خدمة إصدار شهادة التصديق الإلكتروني فقط، مع إمكانية تقديم خدماتٍ أخرى في مجال التوقيع الإلكتروني، لم ينص على الخدمات الأخرى المتعلقة بالتوقيع الإلكتروني سواءً في القانون أو اللائحة التنفيذية، بل ترك الأمر كله في تحديد هذه الخدمات والقواعد المطبقة عليها لهيئة تنمية صناعة تكنولوجيا المعلومات.

أما اللائحة الأوربية لم تقتصرْ على تقديم خدمة إصدار شهادات التصديق على التوقيع الإلكتروني، بل أصبحت اللائحة تغطي الخدمات الثقة الأخرى، وهي خدمة التحقق من التوقيعات الإلكترونية والأختام الإلكترونية، تقديم خدمة

البريد الإلكتروني، خدمة ختم الوقت الإلكتروني، خدمة الحفظ المؤهلة للتوقيعات والأختام الإلكترونية، و حيث لا تفرض اللائحة التزامًا عامًا على مقدم خدمات الثقة بتقديم جميع خدمات الثقة الموجودة، بل يمكنه تقديم خدمة واحدة أو أكثر من خدمات الثقة، حيث تقتصر دور اللائحة على إنشاء النظام القانوني المطبق على خدمات الثقة المؤهلة والتى تنطبق على خدمات الثقة غير المؤهلة.

وبناءً على اللائحة الأوربية نظمت اللوائح الصادرة من الوكالة الوطنية لأمن نظم المعلومات ANSSI[١٣٩٠] بصفتها الجهة المسئولة في فرنسا عن

التحقق من امتثال مقدم خدمات الثقة المؤهلين والخدمات التى يقدموها لمتطلبات لائحة [eIDAS][١٣٩١]، و سوف نتناول ذلك من خلال مطلبين: نخصَّصُ الأولَ للخدمات الأخرى التى يقدمها مقدم خدمة الثقة في اللائحة الاوربية، ونكرَّسُ الثاني للخدمات الأخرى التى تقدمها جهات التصديق الإلكتروني في القانون المصري.

المطلبُ الأولُ

الخدمات الأخرى التي يقدمها مقدم خدمة الثقة في اللائحة الأوربية

وسوف نتناول ذلك من خلال أربعةِ فروعٍ: نخصَّصُ الأولَ لخدمة التحقق المؤهلة من التوقيعات الإلكترونية والأختام الإلكترونية، ونكرسُ الثاني لتقديم خدمة البريد الإلكتروني المؤهل، ونبينُ في الثالث خدمة ختم الوقت الإلكتروني المؤهلة، ونوضح في الرابع خدمة الحفظ للتوقيعات والأختام الإلكترونية المؤهلة.

الفرع الأول

خدمةُ التحققِ من التوقيعاتِ الإلكترونيةِ و الأختامِ الإلكترونيةِ المؤهلةِ

إنَّ تقديم خدمة التحقق المؤهلة للتوقيعات الإلكترونية المؤهلة، من المفترض أن تستوفي المتطلبات الواردة بالمادتين(٣٢ و٣٣)، وجديرٌ بالذكر بالرغم من أن اللائحة الأوربية تعزِّزُ المصادقة وعرض خدمات التحقق من صحة التوقيعات الإلكترونية المؤهلة، إلا أنها لا تفرضُ أي التزامٍ على طرف المستخدم للتحقق من التوقيع وكذلك لا تنصُّ على مسئوليةٍ خاصةٍ في هذه الخدمة في حالة عدم التحقق من صحة التوقيع الإلكتروني.

حيث نصَّت المادة ٣٣ في الفقرة الأولى من اللائحة [eIDAS] على أنَّ خدمة التحقق من التوقيعات الإلكترونية و الأختام الإلكترونية المؤهلة، لا يمكن تقديمها إلا من قبل مقدم خدمة ثقة مؤهل، و يشترط عند تقديمه خدمات التحقق أن تكون متوافقةً مع المتطلبات المحددة في اللائحة لتحقيق اليقين القانوني فيما يتعلق بصحة التوقيعات الإلكترونية المؤهلة و الأختام الإلكترونية المؤهلة وذلك على النحو المحدد في لائحة [eIDAS].

(١٣٩٠) Agence Nationale de la Sécurité des Systèmes d'Information.

(١٣٩١) مقدمو خدمة الثقة المؤهلون و معايير تقييم الامتثال للوائح eIDAS، الإصدار الحالي ٢٠١٧.متاح على الموقع الأتي: http://www.ssi.gouv.fr تاريخ الدخول ٢٠٢٠/٤/٧.

يجب على مقدم خدمة الثقة المؤهل الذي يقدم خدمات الثقة المؤهلة، استخدام نظمٍ ومنتجاتٍ موثوقةٍ، المحمية ضد التعديل لضمان أمن وموثوقية العمليات، ولتخزين البيانات من خدمة التحقق من صحة التوقيعات الإلكترونية والأختام الإلكترونية، وأن يكون لديه خطة إنهاء العمل لخدمة التحقق من صحة التوقيعات الإلكترونية والأختام الإلكترونية [١٣٩٢].

يجب أن يثبتَ مقدمُ خدمةِ التحققِ من الصحةِ التوقيعَ أو الختمَ الإلكترونيَّ المؤهلَ أنه قام بتنفيذ الإجراءات الفنية والتنظيمية لتقليل المخاطر على التطبيق المستخدم للتحقق، وأن يخضع تطبيق التحقق من صحة التوقيع أو الختم لشهادة الأمان من المستوى الأول (CSPN)[١٣٩٣] وفقًا لهدف الأمان الذي تمَّ التحققُ منه بواسطة ANSSI، و أن تثبت عملية التحقق من أن الشهادة التى يستند إليها التوقيع أو الختم، في وقت التوقيع أو إنشاء الختم، شهادة توقيع إلكترونية مؤهلة أو شهادة ختم إلكترونية مؤهلة؛ وإذا تم إصدار الشهادة المؤهلة من قبل مقدم خدمة ثقة مؤهل وكانت صالحة وقت التوقيع أو إنشاء الختم؛ يتطلب هذا الشرط معرفة تاريخ ووقت إنشاء التوقيع الإلكتروني المؤهل أو الختم الإلكتروني المؤهل حتى تتمكن من التحقق من أن الشهادة كانت في فترة صلاحيتها، وعدم إبطال الشهادة، و أن مقدم الخدمة الذي أصدر الشهادة كان موجودًا بالفعل في القائمة الموثوقة.

ويجب أن تشهد عملية التحقق من صحة مجموعة البيانات الفريدة التي تمثل الموقع في الشهادة بشكلٍ صحيحٍ، و إذا تم استخدام اسم مستعار في وقت التوقيع، فيجب التحقق من وجوده وتحديد الهوية، والإشارة التى تتعلق باستخدام اسم مستعار في تقرير التحقق.

يجب على مقدم هذه الخدمة تزويد أطراف المستخدمين بنتيجة عملية التحقق، بطريقة آلية وموثوقة وفَّعالة وتحمل التوقيع الإلكتروني المتقدم أو الختم الإلكتروني المتقدم لمقدم الخدمة الذي يقدم خدمة التحقق المؤهلة [١٣٩٤]، لأنَّ نتيجة عملية التحقق التى يتم تقديمها من خلال تقرير التحقق تسمح بالدراسة التفصيلية للقرارات المتخذة خلال مرحلة التحقق وتبرير حالة التحقق، يجب أن تسمح PSCo[١٣٩٥]، بالوصول إلى خدمة التحقق من صحة التوقيع أو الختم، وتزويد أطراف المستخدم بتقرير التحقق هذا بطريقةٍ آليةٍ، من أجل ضمان التفسير الصحيح لتقرير التحقق، يجب على PSCo أيضًا نشر سياسة التحقق الخاصة بها للتوقيعات الإلكترونية المؤهلة أو الأختام الإلكترونية المؤهلة.

ويجب الاحتفاظُ بجميع المعلومات ذات الصلة، التى أرسلها مقدم الطلب أو تم جمعها إلكترونيًا للتحقق من صحة التوقيع الإلكتروني أو الختم الإلكتروني، لمدة سبع سنوات بما في ذلك على الأقل تاريخ ووقت التحقق من التوقيع أو

[١٣٩٢] انظر: المادة (٢٤) من اللائحة الأوربية.

[١٣٩٣] Certification de Sécurité de Premier Niveau.

[١٣٩٤] انظر: المادة ٣٣ الفقرة الثانية من اللائحة الأوربية.

[١٣٩٥] مزود خدمة موثوق به. Prestataire de Services de Confiance.

الختم الإلكتروني المؤهل،البيانات المقدمة من مقدم الطلب للتحقق من صحة التوقيع أو الختم، و هوية مقدم طلب الخدمة، و التقرير الذي يحتوى على نتيجة المصادقة على التوقيع أو الختم الإلكتروني المؤهل.

الفرعُ الثاني

تقديمُ خدمةِ البريدِ الإلكترونيَّ المؤهلِ

يجبُ أنْ تتوافقَ خدمةُ التسليم الإلكترونية المسجلة مع تعريف اللائحة [eIDAS]، كما هو محدد في المادة الثالثة البند ٣٦ على أنها "خدمةٌ تتيح نقل البيانات بين أطرافٍ ثلاثةٍ بالوسائل الإلكترونية، والتى تقدم أدلة تتعلق بمعالجة البيانات المرسلة، بما في ذلك دليل على الإرسال والاستلام، والذي يحمي البيانات المرسلة ضد خطر الضياع أو السرقة أو التغيير أو أي تعديل غير مصرح به "، و بالتالى تعتبر هذه الخدمة الإلكترونية تقريبًا مساوية للتسليم المادي أو الورقي المسجل الذي عرفناه عقودًا في العالم البريدي، وهذا يعني أنها خدمة إلكترونية تجعل من الممكن تحقيق اليقين القانوني، بأن البياناتِ الإلكترونيةَ التى تم إرسالها واستقبالها بطريقةٍ ما، تحدد وقت و تاريخ إرسال واستلام هذه البيانات(١٣٩٦).

يجب امتثال مقدم خدمة التوصيل الإلكترونية المؤهلة للائحة [eIDAS]، المتعلقة باستخدام نظمٍ ومنتجاتٍ موثوقةٍ، ولأمن وموثوقية العمليات، وتخزين المعلومات المسلمة والمتلقية عن طريق البريد الإلكتروني المسجل؛ لاستمرارية الخدمة بعد توقف نشاط التسليم الإلكتروني المسجل(١٣٩٧)، وعند تقديم الخدمة من قبل واحد أو أكثر من مقدمي خدمات الثقة المؤهلين، يتم تحديد هوية المرسل بدرجةٍ عاليةٍ من الثقة، وتحديد هوية المستلم قبل تقديم البيانات، وتأمين إرسال البيانات واستلامها عن طريق توقيع إلكتروني متقدم أو عن طريق ختم إلكتروني متقدم من مزود خدمة ثقة مؤهل لاستبعاد أي إمكانيةٍ لتعديل البيانات، و إخطار المرسل والمستلم للبيانات بأي تعديل للبيانات اللازمة لإرسالها أو استقبالها، مع بيان تاريخ ووقت إرسال البيانات واستلامها وأي تعديل عليها عن طريق ختم زمني إلكتروني مؤهل(١٣٩٨).

وفقًا لتعريف لائحة [eIDAS] لخدمة التسليم الإلكتروني المسجل، أنها هذه الخدمة للمرسل دليلًا على الإرسال والاستلام بطريقة آلية وموثوقة فعالة، يجب أن تحدد الشروط العامة لاستخدام خدمة التوصيل الإلكترونية المؤهلة وطرق إثبات هذا الدليل، و بالتالى يجب أن تضمن خدمة التسليم المسجلة الإلكترونية المؤهلة تحديد هوية المرسل

(١٣٩٦) انظر: Sur la question de l'envoi recommandé électronique en droit belge, voy. notamment E. MONTERO, « Du recommandé traditionnel au recommandé électronique : vers une sécurité et une force probante renforcées » *in Lecommerce électronique : de la théorie à la pratique*, Cahiers du CRID, n° 23, Bruxelles, Bruylant, 2003, pp. 69 à 99 ; O. VAN CUTSEM, « L'évolution technologique et le monde postal. La validité juridique du courrier recommandé électronique en Belgique », C.J., n°3/2003, pp. 43 à 48. En droit français, voy. E. Caprioli, Signature électronique et dématérialisation, LexisNexis, 2014, pp.175 et s.

(١٣٩٧) انظر: المادة (٤٣) من اللائحة الأوربية.

(١٣٩٨) انظر: المادة (١/٤٤) من اللائحة الأوربية.

بدرجةٍ عاليةٍ من الثقة للتحقق من الهوية، تنطبق المتطلبات المحددة في معيار تقييم امتثال مقدم خدمات إصدار الشهادات المؤهلة للتوقيع الإلكتروني والختم الإلكتروني ومصادقة موقع الويب للائحة eIDAS، على التسليم الإلكتروني المسجل مع إجراء التغييرات اللازمة، بعد التحقق من الهوية يمكن لمزود خدمة التسليم المسجل الإلكتروني المؤهل تعيين وسيلة تحديد هوية المرسل، والتى يمكن استخدامها للمصادقة مع كلَّ شحنةٍ، و يجب أن تكون آلية المصادقة المستخدمة ديناميكية، وأن تخضع وسائل تحديد الهوية على الأقل لشهادة الأمان من المستوى الأول (CSPN)، وأن تكون وسائل تحديد الهوية تحت التحكم الحصري للمستخدم، وتنفيذ ضوابط الأمان بحيث يكون من غير المحتمل وجود أنشطة ضارة مثل محاولات فك التشفير، يمكن أن تضر بآليات المصادقة.

وإذا كانت وسيلة تحديد الهوية تعتمد على استخدام شهادة توقيع أو ختم إلكتروني، فيجب أن تكون هذه الشهادة مؤهلة، وذلك للحفاظ على النزاهة المستمدة من تعريف هذه الخدمة، ويجوز إصدار وسيلة المصادقة هذه من قبل هيئة غير مزود خدمة التوصيل الإلكتروني المؤهل المسجل؛ وإذا لم تقم PSCo بتعيين وسيلة تحديد هوية للمرسل، فيجب إجراء التحقق من الهوية مع كل شحنة وفقًا للشروط الموضحة في أعلاه.

ويجب أيضًا أن تضمن هذه الخدمة تحديد هوية المستلم قبل تقديم البيانات، الغرض من هذا الالتزام هو التأكد من أن الشخص الذي يطلع على العنصر المسجل هو من يدَّعي أنه له الحق في تلك المعرفة، في حالة التوكيل نعتقد أنه لا ينبغي فقط التحقق من هوية الشخص الذي يطلع على المسجل ولكن أيضًا التحقق من صحة و نزاهة التوكيل وكونه مقبول من قبل مستلم البريد المسجل إلكترونيًا[١٣٩٩].

يجب أن يحتفظ مقدم خدمة التوصيل الإلكتروني المؤهل لمدة لا تقل عن سبع سنوات بعد تاريخ إرسال واستقبال البيانات وبجميع المعلومات ذات الصلة المتعلقة بالبيانات التي تم تسليمها واستلامها، ولا سيما لغرض التمكن من تقديم دليلٍ في المحكمة، وتحدد PSCo في شروط الاستخدام العامة والخاصة بها فترة الاحتفاظ المطبقة فعليًا؛ والبيانات التى سيتم الاحتفاظ بها هي على الأقل هوية مرسل البريد الإلكتروني المسجل، إثبات صحة هوية المرسل، الوثيقة موضوع طلب التسليم الإلكتروني المسجل، تاريخ ووقت إرسال البيانات واستلامها، هوية مستلم البريد الإلكتروني المسجل، إثبات صحة هوية المستلم، البيانات المتعلقة بأمن الشحنة وهي الأختام الإلكترونية.

تستفيد خدمات التوصيل الإلكترونية المؤهلة، المستوفية للشروط من الآثار القانونية المحددة في المادة (٢/٤٣) من لائحة [eIDAS][١٤٠٠]، إن البيانات المرسلة والمستلمةَ بواسطة خدمة التوصيل الإلكترونية المسجلة المؤهلة، فإنها تستفيد من افتراض سلامة البيانات، فعندما يتم إرسال هذه البيانات من قبل المرسل المحدد وعندما يتم استلامها من قبل المستلم المحدد، فأن تاريخ ووقت الإرسال والاستلام صحيح كما هو مبين بواسطة خدمة التوصيل الإلكترونية المسجلة المؤهلة، وعلى من يدَّعِى خلاف ذلك عليه الإثبات.

[١٣٩٩] انظر: D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et lesservices de confiance (eIDAS) : analyse approfondie»,op.cit.p.30.

[١٤٠٠] انظر: المادة ٤٣ من اللائحة الاوربية.

وجديرٌ بالذكر إنه يمكن لمقدم خدمة التسليم الإلكترونية المسجلة المؤهلة وفقا للقانون البلجيكي ٢١لسنة ٢٠١٦، بناءً على طلب المرسل إرسال بريده المسجل في شكلٍ إلكترونيٍّ مع ضمان تلقي المستلم له في ظرفٍ في شكلٍ ورقيٍّ، ويعد هذا التسليم من قبل عامل البريد وإذا قرر المزود تقديم خدمة توصيل مختلطة مسجلة فإنه يقوم بإرسال البند المسجل الإلكتروني المؤهل إلى مقدم الخدمة البريدية، في موعد أقصاه يوم العمل التالي للإيداع من قبل مرسل العنصر المسجل الإلكتروني المؤهل، وإبلاغ المرسل بالتاريخ الذي تم إيداع الشحنة فعليًا لدى مزود الخدمة هذا، حتى يتمكن هذا المرسل من التحقق من احترام الموعد النهائي في يوم العمل التالي، وجديرٌ بالذكر أنَّ تقديمَ هذه الخدمة لا تغطيها اللائحة الأوربية [١٤٠١]، ويجب أن يمتلك مقدم الخدمة البريدية ترخيصًا خصصته BIPT [١٤٠٢] بموجب أحكام القانون.

الفرع الثالث

خدمة ختم الوقت الإلكتروني المؤهلة

يتم تعريفُ ختم الوقت الإلكتروني في المادة (٣٣/٣) من للائحة [eIDAS] على أنها "بياناتٌ في النموذج التى تجمع بين البيانات الأخرى في شكلٍ إلكترونيٍّ في وقتٍ معينٍ وتؤسس دليلاً على أن البيانات الأخيرة كانت موجودةً في ذلك الوقت "، و كما عرفت أيضا ختم الوقت الإلكتروني المؤهل" يعني الطابع الزمني الإلكتروني الذي يلبي المتطلبات المنصوص عليها في المادة ٤٢".

يكون استخدام خدمة الوقت الإلكترونية للبيانات مفيدًا غالبًا سواءً لأسبابٍ قانونيةٍ أم لا، ويمكن استخدام هذه الخدمة في المستندات الإلكترونية مثل العقود والالتزامات من جانب واحد، ووثائق إقامة الدعاوى، وما إلى ذلك، لكنها تسمح بذلك أيضًا تحديد التاريخ للوصول إلى الوثيقة، وإرسال الوثيقة، وأختام الصفقة، نظرًا لأهمية هذا النوع من الخدمة في سياق المعاملات الإلكترونية، وجد المشرِّعُ الأوربيُّ أن هذه الخدمةَ مفيدةٌ، مثل خدمات الثقة الأخرى، فخصص قسمًا لها من ناحية تحديد الآثار القانونية المرتبطة بهذه الطوابع الزمنية الإلكترونية، ومن ناحيةٍ أخرى تحديد متطلبات الاختام الزمنية الإلكترونية المؤهلة [١٤٠٣].

[١٤٠١] انظر: C. VERDURE, « Règlement eIDAS : quelles nouveautés en matière d'horodatage et de recommandé électroniques ? » *in* L'identification électronique et les services de confiance depuis le règlement eIDAS, sous la direction de H. JACQUEMIN, Collection du Crids, Bruxelles, Larcier, Mars 2016, pp. 203 et s.

[١٤٠٢] المعهد البليجكي للخدمات البريدية والإتصالات.هو المنظم الفيدرالي المسؤول عن سوق الاتصالات الإلكترونية ، والسوق البريدي ، والطيف الكهرومغناطيسي للترددات الراديوية والبث الإذاعي والتلفزيوني في العاصمة بروكسل.تأسس المعهد البلجيكي للخدمات البريدية والاتصالات في عام ١٩٩١ كمؤسسة شبه حكومية،وتم وضعه الخاص بموجب قانون الصادرفي١٧ يناير ٢٠٠٣.

[١٤٠٣] انظر: La notion doit s'entendre au sens large dans la mesure où le service permet de déterminer de manière précise tant la date que l'heure. La définition utilise d'ailleurs à dessein le terme « instant » et non celui de « date ». Sur cette notion et ce service, voy. E. Caprioli, *Signature électronique et dématérialisation*, LexisNexis, 2014, pp.169 et s.

إن معايير تقييم الامتثال لمتطلبات اللائحة [eIDAS]على تقديم خدمة ختم الوقت الإلكتروني المؤهل، والتى تنطبق على جميع مقدمي خدمات الثقة المؤهلين، و هي التى تتضمن استخدام نظم ومنتجات موثوقة لأمن وموثوقية العمليات، لتخزين البيانات من خدمة ختم الوقت الإلكترونية، وخطة توقف الأعمال لخدمة ختم الوقت الإلكتروني(١٤٠٤)، و أن يربط التاريخ والوقت بالبيانات بحيث يستبعد بشكل معقول إمكانية تعديل البيانات التى لا يمكن الكشف عنها، أنه يستند إلى ساعةٍ دقيقةٍ مرتبطة بالتوقيت العالمي المنسق، يتم التوقيع عليه عن طريق توقيعٍ إلكترونيٍّ متقدمٍ أو مختومٍ عن طريق ختمٍ إلكترونيٍّ متقدمٍ لمقدم خدمة الثقة المؤهل(١٤٠٥).

وأن يتم إنشاء الارتباط بين التاريخ والوقت والبيانات عن طريق وحدة ختم الوقت التى تتكون من تطبيق ختم الوقت ووحدة التشفير النمطية؛ وإذا كان تطبيق ختم الوقت محميًا في البيئة الآمنة لوحدة التشفير النمطية، فيجب أن يكون تطبيق ختم الوقت على الأقل خاضعًا لشهادة أمان من المستوى الأول (CSPN) وفقًا لهدف الأمان والذي يتم التحقق من قبل ANSSI، ويجب أن يكون تطبيق ختم الوقت معتمدًا وفقًا للمعايير العامة ووفقا لملف تعريف الحماية، ونظام ختم الوقت [PP_HORODAT](١٤٠٦).

إذا كان تطبيق ختم الوقت غير محمي في البيئة الآمنة لوحدة التشفير النمطية، فيجب على PSHE(١٤٠٧) توضيح تنفيذ التدابير التقنية والتنظيمية القائمة للحد من المخاطر على وحدة ختم الوقت، ويجب بأن يخضع تطبيق ختم الوقت لشهادة أمان من المستوى الأول (CSPN) وفقًا لهدف الأمان الذي يتم التحقق منه بواسطة ANSSI.

يجب أن تحتفظ PSHE لمدة لا تقل عن سبع سنوات بعد الانتهاء من كل خدمة ختم الوقت، لكل المعلومات ذات الصلة المتعلقة بالبيانات التى تم تسليمها واستلامها، حتى تكون قادرةً على تقديم أدلة العدالة، وتحدد PSHE في شروطها العامة للاستخدام مدة الحفظ المطبقة بالفعل.

الاستفادة من الآثار القانونية المحددة في المادة ٤١ من اللائحة [eIDAS](١٤٠٨)، أي أنَّ الختم الزمني الإلكتروني المؤهل يستفيد من افتراض دقة التاريخ والوقت الذي تشير إليه، وسلامة البيانات التى يرتبط بها هذا التاريخ والوقت، ولكنها قابلة لإثبات العكس، ولكن الاستفادة من هذا الأثر القانوني يجب أن تستوفي خدمة ختم الوقت الإلكتروني المؤهلة ثلاثة متطلباتٍ: الأول أن تربط التاريخ والوقت بالبيانات، حتى تستبعد بشكلٍ معقولٍ إمكانية تعديل البيانات التي لا يمكن الكشف عنها، يقع هذا الشرط للحفاظ على النزاهة، والتى تتعلق ببيانات الوقت والتى تجعل من الممكن التحقق من التاريخ والبيانات المؤرخة مثل العقد، والثاني أن تستند خدمة ختم الوقت إلى ساعةٍ دقيقةٍ مرتبطةٍ بالتوقيت

(١٤٠٤) انظر: المادة (٢/٢٤) من اللائحة الاوربية.

(١٤٠٥) انظر: المادة (١/٤٢) من اللائحة الاوربية.

(١٤٠٦) Profil de protection, Système d'horodatage, référence PP-SH-CCv3.1, version 1.7 du 18 juillet 2008. Disponible sur http://www.ssi.gouv.f.

(١٤٠٧) مزود خدمة ختم الوقت الإلكتروني.

Prestataire de Services d'Horodatage Electronique.

(١٤٠٨) انظر: المادة ٤١ من اللائحة الأوربية.

العالمي المنسق، لأن الهدف الأساسي من هذه الخدمة هو تقديم تاريخٍ موثوقٍ ودقيقٍ، وربطه بالوقت العالمي المنسق[١٤٠٩]، و الثالث يجب توقيع خدمة ختم الوقت باستخدام توقيع إلكتروني متقدم أو مختومة باستخدام ختم إلكتروني متقدم من مزود خدمة الثقة المؤهل، أو بطريقةٍ مكافئةٍ، و يقدم هذا الشرط مستوى من الأمان عاليًا نسبيًا في المنشأ وسلامة الخدمة، يمكن لمفهوم الطريقة المعادلة إنه في حالة استخدام طريقة غير الختم الإلكتروني المتقدم أو التوقيع الإلكتروني المتقدم يجب أن تكون مسئولية مقدم خدمة الثقة المؤهل موضحة في تقرير تقييم الامتثال، وتضمن تلك الطريقة مستوى مكافئًا من الأمن وتفي بالالتزامات المنصوص عليها في هذه القواعد [١٤١٠].

الفرعُ الرابعُ

خدمة الحفظ المؤهلة للتوقيعات المؤهلة والأختام الإلكترونية

تنص اللائحة في المادة ٣٤ على حكمٍ يتعلق بخدمة الحفظ المؤهلة للتوقيعات الإلكترونية المؤهلة، هذا يقتصر على الإشارة إلى أن خدمة الحفظ المؤهلة للتوقيعات الإلكترونية المؤهلة لا يمكن تقديمها إلا من مقدم خدمة ثقة مؤهل، و باستخدام الإجراءات والتقنيات لزيادة موثوقية التوقيعات الإلكترونية المؤهلة لما بعد فترة الصلاحية التكنولوجية.

يمكن وصف هذه المادة بأنها "التصرف الجنيني" للأرشفة الإلكترونية على هذا النحو، هناك من يقول أن اللائحة تنسق القواعد العامة المتعلقة بخدمة الحفظ الإلكتروني، كما فعلت للتوقيع والختم الإلكتروني والأختام الزمنية والبريد المسجل، إلا إنه يوجد العديد من الأسئلة التى يجب حلّها في سياق الأرشفة الإلكترونية حيث إنها كثيرةٌ ومتنوعةٌ، حيث كان الهدف من اللائحة هو فقط إنشاء معادل إلكتروني للإيداع الورقي وبالتالى تحديد الظروف التى يمكن أن يتم فيها الإيداع في شكلٍ إلكترونيٍّ، دون لمس القواعد الموضوعية، نأسف لذلك لأنَّ المشرِّعَ الأوربيَّ أتيحت له فرصة لم يغتنمها [١٤١١].

تسمح خدمات الحفظ المؤهلة للتوقيعات الإلكترونية المؤهلة والأختام الإلكترونية المؤهلة التى ينفذها مزود خدمة موثوق به ومتوافق مع المتطلبات المحددة في اللائحة [eIDAS]، والتى تتضمن استخدام نظمٍ ومنتجاتٍ موثوقةٍ، وأمن

[١٤٠٩] التوقيت العالمي المنسق، هو مقياس زمني تم اعتماده كأساس للوقت المدني الدولي من قبل غالبية دول العالم، إنه مقياس زمني بين "الوقت الذري الدولي" الذي مستقر ولكن غير متصل بدوران الأرض، والتوقيت العالمي (UT) ، المرتبط مباشرة بتدوير وبالتالي الأرض متغيرة ببطء يشير مصطلح "منسق" إلى أن التوقيت العالمي المنسق هو في الواقع مطابقًا للوقت الذري الدولي، حيث يتمتع بالاستقرار والدقة لأقرب عدد صحيح من الثواني، مما يسمح لها بالالتزام بالتوقيت العالمي في غضون ٠.٩ ثانية، منشور على الموقع الاتي: http://fr.wikipedia.org/wiki/Temps_universel_coordonn%C3%A9

[١٤١٠] انظر: D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l’identification électronique et lesservices de confiance (eIDAS) : analyse approfondie »,op.cit.p.34.

[١٤١١] انظر: Pour un aperçu de ces nombreuses questions, voy. notamment « L’archivage électronique et le droit », ouvrage collectif sous la direction de M. DEMOULIN, Collection du CRIDS, Larcier, Mai 2012, 198 pages ; E. Caprioli,Signature électronique et dématérialisation, LexisNexis, 2014, pp.187 et s. ; M. DEMOULIN et D. GOBERT, «L'archivage dans le commerce électronique : comment raviver la mémoire? », in M. DEMOULIN (dir.), Commerceélectronique, de la théorie à la pratique, Cahiers du CRID, 2003, n° 23, pp. 101 à 130.

وموثوقية العمليات، وأن تتم تخزين البيانات من الخدمة لحفظ التوقيعات الإلكترونية والأختام الإلكترونية، خطة إنهاء الأعمال لخدمة الحفاظ على التوقيعات الإلكترونية والأختام الإلكترونية[١٤١٢]، واستخدام الإجراءات والتكنولوجيات لتمديد موثوقية التوقيعات الإلكترونية المؤهلة إلى ما بعد فترة الصلاحية التكنولوجية[١٤١٣]، و التحقق من صحة وحفظ الأختام الإلكترونية المؤهلة تطبيق المادة (٣٤) مع مراعاة ما يقتضيه اختلاف الحال على التحقق من الأختام الإلكترونية المؤهلة والمحافظة عليها[١٤١٤]، و بالرجوع المادة (٣٤) المتعلقة بتقديم هذه الخدمة، تشترط عدم تقديم هذه الخدمة إلا من خلال مقدم خدمة ثقة مؤهل يستخدم الإجراءات والتقنيات لتمديد موثوقية التوقيعات الإلكترونية المؤهلة إلى ما بعد فترة الصلاحية التكنولوجية.

لضمان الحفاظ على التوقيعات والأختام الإلكترونية المؤهلة يتم التعرف على نهجين، الأول منهجيٌّ قائمٌ على حماية سلامة نظام الإيداع الإلكتروني الذي سيتم فيه الاحتفاظ بالتوقيعات المؤهلة والأختام الإلكترونية، يطبق هذا النهج المعيار الفرنسي[NF_Z42-013][١٤١٥]، و الثاني محددٌ قائمٌ على الحماية في نزاهة كل توقيعٍ مؤهلٍ أو ختمٍ إلكترونيٍّ يخضع للحفظ بشكل فردي، عن طريق تمديد منتظم للتوقيع أو الختم أو لالتقاطٍ منتظمٍ لمعلومات التحقق، وهكذا تحدد هذه اللائحة بناءً على النهج المختار، المتطلبات القابلة للتطبيق.

وأن تتوافق وحدات التشفير المستخدمة في العمليات اللازمة لخدمة الحفظ المؤهلة، ولاسيما عمليات إنشاء توقيع إلكتروني أو إنشاء ختم إلكتروني أو ختم زمني، مع القواعد المحددة لتقييم امتثال مقدمي الخدمة المؤهلين للائحة الأوربية، وأن يحتفظ مزود خدمة التخزين المؤهل لفترة مساوية على الأقل لفترة تخزين التوقيعات المؤهلة أو الأختام الإلكترونية، وجميع المعلومات ذات الصلة المتعلقة بالبيانات التى تم تسليمها واستلامها، حتى تتمكن من تقديم الأدلة في المحكمة، و أن يحدد مزود خدمة الحفظ المؤهل في شروط الاستخدام العامة فترة الحفظ الخاصة به، والفترة الإضافية التى يتم حفظ التوقيعات المؤهلة والأختام الإلكترونية.

يجب على PSCo توفير إجراءات لضمان سلامة جميع العناصر المنقولة وقابليتها للاستخدام ، إما من مقدم الطلب الأصلي أو من مزود خدمة صيانة مؤهل آخر بموافقةٍ صريحةٍ من مقدم الطلب الأصلي، وأن تكون هذه العناصرُ مقروءةً ومفهومةً من قبل متلقيها، وفي شكلٍ يسمح باستغلالها الجيد، بالإضافة إلى ذلك، إذا كانت هذه العناصر تخضع لحماية السلامة عن طريق الأختام الزمنية أو الأختام الإلكترونية، فيجب أن يكون من الممكن للمستلم التحقق من هذه الأختام، التى تفترض مسبقًا أن استخدام الشهادات الإلكترونية التى يمكن الوصول إلى حالة الإبطال فيها وسلسلة الثقة وسياسة الاعتماد على سبيل المثال يمكن أن تكون الشهادة الإلكترونية التى تحدد الخدمة في القائمة الموثوقة، قد ترفض PSCo الاحتفاظ بالتوقيعات الإلكترونية أو الأختام المقدمة، إذا اعتبرت أنه من غير الممكن لها ضمان قراءتها بمرور الوقت.

(١٤١٢) انظر: المادة (٢/٢٤) من اللائحة الاوربية.

(١٤١٣) انظر: المادة (١/٣٤) من اللائحة الاوربية.

(١٤١٤) انظر: المادة (٤٠) من اللائحة الاوربية.

(١٤١٥) أن هذا المعيار المتعلق بتصميم وتشغيل أنظمة الكمبيوتر، يضمن الحفاظ على سلامة الوثائق المخزنة في هذه الأنظمة وتكاملها.

يمكن لـ PSCo اختيار ضمان للحفاظ على التوقيعات والأختام الإلكترونية المؤهلة، وذلك من خلال استخدام الأرشفة الإلكترونية، مما يجعل من الممكن ضمان سلامة التوقيعات المؤهلة والأختام الإلكترونية المؤرشفة، أو بالرجوع على أساسٍ منتظمٍ إلى توسيع التوقيعات والأختام الإلكترونية المؤهلة أو إلى تخزين المعلومات، التى تتيح بعد فترة الصلاحية التكنولوجية، التحقق من صحة هذه التوقيعات والأختام الإلكترونية.

قد تستخدم PSCo تقنياتٍ أخرى، بشرط أن توضح أنها تستجيب لمستوى من الأمن مشابه لما سبق، أيًّا ما كانت الطريقة المختارة يجب أن تضمن PSCo الحفاظ على الوثيقة التى هي موضوع التوقيع أو الختم الإلكتروني، في ظل نفس شروط حماية السلامة، ولا سيما للتخفيف من خطر إضعاف الوظيفة التى تربط الوثيقة بالتوقيع أو الختم.

قبل تقديم خدمة الحفظ يجب إخضاع التوقيع المؤهل أو الختم الإلكتروني للمصادقة من قبل مقدم خدمة الحفظ المؤهل، مع تلبية المتطلبات المطبقة على خدمات التحقق المؤهلة، كما هو موضح في معايير تقييم امتثال مقدم خدمات التحقق المؤهلة للتوقيعات الإلكترونية المؤهلة والأختام الإلكترونية المؤهلة للائحة eIDAS، و يمكن لمزود خدمة الحفظ المؤهل الاعتماد على مزود خدمة التحقق المؤهل لإجراء هذه العملية، في هذه الحالة يجب التحقق من التوقيع المتقدم أو الختم الإلكتروني المتقدم مثبتًا بواسطة مزود خدمة التحقق المؤهل في تقرير التحقق، قبل تقديم التوقيع الإلكتروني المؤهل أو الختم الإلكتروني المؤهل، يجب حفظ نتيجة التحقق مع التوقيع أو الختم الإلكتروني المؤهل.

وجديرٌ بالذكر قد لا تطبق PSCo هذه المصادقة في هذه الحالة، يجب عليه التأكد من أن مستخدمي الخدمة على علمٍ جيدٍ بهذا القيد والمخاطر الناجمة عن عدم التحقق الأول من موثوقية التوقيعات المؤهلة والأختام الإلكترونية المحفوظة، ويجب أن يكون PSCo قادرًا أيضًا على الاحتفاظ بالإضافة إلى التوقيعات والأختام الإلكترونية المؤهلة وفي نفس ظروف الحفاظ على السلامة بجميع العناصر الإضافية التى يرسلها مقدم الطلب والمساعدة في إثبات صحة التوقيع أو الختم الإلكتروني المؤهل الذي يتم الاحتفاظ به.

يجب أن يستوفي التحقق من صحة التوقيع المؤهل أو الختم الإلكتروني المتطلبات المطبقة على خدمات التحقق المؤهلة، كما هو موضحٌ في معايير تقييم امتثال مقدم خدمات التحقق المؤهلة للتوقيعات الإلكترونية المؤهلة والأختام الإلكترونية المؤهلة للائحة eIDAS، وأن يكون شكل التوقيعات المؤهلة والأختام الإلكترونية التي تكون موضوع هذا التحقق، أحد تلك المنصوص عليها في المعايير المشار إليها في قرار تنفيذ الاتحاد الأوربي[١٤١٦].

يجوز لـ PSCo كبديلٍ للتحقق من التوقيعات أو الأختام الإلكترونية المؤهلة المحفوظة، توفير المعلومات اللازمة للتحقق من صحتها، مثل القائمة الموثوقة، والمعلومات التى تتعلق بحالة الإلغاء، في هذه الحالة يجب أن يضمن سلامة هذه العناصر وقابليتها للاستخدام مع مستوى من التأكيد يساوي على الأقل المستوى الذي تسمح به آلية التحقق.

[١٤١٦] لجنة تنفيذ القرار (الاتحاد الأوربي) رقم ١٥٠٦لسنة ٢٠١٥ المؤرخ ٨ سبتمبر ٢٠١٥ الذي يحدد مواصفات أتساق التوقيعات الإلكترونية المتقدمة والأختام الإلكترونية المتقدمة التي يجب أن تعترف بها هيئات القطاع العام المشار إليها في المادة ٢٧ (٥) وفي المادة ٣٧ (٥) من لائحة [eIDAs].

المطلبُ الثاني
الخدماتُ الأخرى التي تقدمُها جهاتُ التصديق الإلكترونيَّ
في القانونِ المصريَّ

حيث تشترط هيئة تنمية صناعة تكنولوجيا المعلومات في التراخيص الصادرة للشركات عدم تقديم خدمات أخرى غير نشاط التصديق على التوقيع الإلكتروني بدون الحصول على ترخيصٍ من الهيئة، بالرجوع إلى الترخيص الصادر لجهات التصديق الإلكتروني تضمن تقديم خدمة إصدار أدوات وتثبيت التوقيعات الالكترونية و خدمة حفظ مفاتيح الشفرة الخاصة المصدرة لمستخدم الخدمة، وإلى تعديل اللائحة التنفيذية لقانون التوقيع الإلكتروني رقم ٣٦١لسنة ٢٠٢٠ التى تتضمن إضافة خدمتى الختم الإلكترونى والبصمة الزمنية، و بالتالى سوف نقسم هذا المطلب إلى ثلاثةِ فروعٍ: نخصصُ الأولَ خدمة إصدار أدوات وتثبيت التوقيعات الالكترونية، ونكرسُ الثاني لخدمة حفظ مفاتيح الشفرة الخاصة المصدرة لمستخدم الخدمة، ونوضحُ في الثالثِ خدمة الختم الإلكترونى والبصمة الزمنية.

الفرعُ الأولُ
خدمةُ إصدارِ أدواتِ وتثبيتِ التوقيعاتِ الإلكترونيةِ

من الخدمات التى يقدمها مقدمو خدمات التصديق الإلكتروني والتى نصَّت عليها المادة ٤٧ من الترخيص رقم ١٠٣ لسنة ٢٠٠٦ الصادر من هيئة صناعة تكنولوجيا المعلومات ما يُسمى بخدمة إصدار أدوات إنشاء و تثبيت التوقيع الإلكتروني و التي تتمثل بإصدار البطاقة الذكية و القاريء.

حيث عرفت المادة(٢٠/١) من اللائحة التنفيذية لقانون التوقيع الإلكتروني ١٥ لسنة ٢٠٠٤ التى تم تعديلها بموجب القرار ٣٦١لسنة ٢٠٢٠ التى تضمنت تغير مسمى البطاقة الذكية لتصبح مسمى أداة التوقيع الإلكتروني بأنه: "وسيطٌ إلكترونيٌّ مؤَّمنٌ يستخدم في عملية إنشاء وتثبيت التوقيع الإلكتروني على المحرر الإلكتروني، ويشمل هذا التعريف الكروت الذكية و الشرائح الإلكترونية المنفصلة أو غيرها من وسائط أو أنظمة تتطابق معه من حيث تحقيق الوظائف المطلوبة، وفقًا للمعايير التقنية والفنية المحددة في هذه اللائحة".

حيث أن هذه الخدمة تتمثل في قيام جهة التصديق بإصدار بطاقةٍ إلكترونيةٍ، تحتوي على بياناتٍ خاصةٍ بالموقع وحدَه دون غيره، وهي بيانات إنشاء التوقيع الإلكتروني ويتم تثبيته على المحرر الإلكتروني بطريقة فنية بحيث تحافظ على سرية البيانات المدونة عليها كون هذه البطاقة غير قابلة للاستنساخ، ومحمية برقمٍ سريٍّ وذلك كما ورد في البند (٤/١) من الشروط والموصفات الفنية الواردة ضمن أحكام كراسة الشروط و المتطلبات الخاصة بمنح الترخيص تقديم خدمات التوقيع الإلكتروني.

لخطورة وأهمية هذه الخدمة المقدمة من قبل الجهات المرخَّصِ لها فإنَّ هناك مجموعةً من الشروط لابدَّ من توافرها في الأدوات المستخدمة بإنشاء و تثبيت التوقيعات الإلكترونية والتى ورد ذكرها ضمن أحكام المادة ٤٧ من الترخيص

رقم ١٠٣ الصادر من الهيئة وكذلك الواردة باللائحة التنفيذية وهي ذات الشروط المطلوب توافرها في منظومة تكوين بيانات إنشاء التوقيع الإلكتروني[١٤١٧].

الفرعُ الثاني

خدمة حفظ مفاتيح الشفرة الخاصة المصدرة لمستخدم الخدمة

من الخدمات أيضا التى يقدمها مقدمو خدمات التصديق الإلكتروني التى نصَّت عليها المادة ٤٩ من الترخيص رقم ١٠٣ لسنة ٢٠٠٦ الصادر من هيئة تنمية صناعة تكنولوجيا المعلومات هي خدمة حفظ مفاتيح الشفرة الخاصة لمستخدم الخدمة، و للتعرف على هذه الخدمة التى تقدمها جهات التصديق الإلكتروني يلزم معرفة مفهوم مفتاح الشفرة الخاص الذى نصَّت عليه المادة (١٧/١) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري رقم ١٥ لسنة ٢٠٠٤ التى تم تعديلها بموجب القرار ٣٦١لسنة ٢٠٢٠ بأنه عبارة عن " أداء إلكترونية خاصة بصاحبها، تنشأ بواسطة عمليةٍ حسابيةٍ خاصةٍ، ويتم الاحتفاظ بها على أداة إنشاء التوقيع الإلكتروني، تستخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية".

حيث يتضح من هذا التعريف أن المفتاح الشفري الخاص هو الوسيلة التي تستعمل لوضع التوقيع الإلكتروني للشخص الموقع على المحرر الإلكتروني على أنَّ المفتاح الشفري الخاص في حيازة الموقع نفسه وأن يكون تحت سيطرته وهذا ما نصَّت علية المادة (١١) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري، و يتضح من هذا النص أن اللائحة التنفيذية لقانون التوقيع الإلكتروني اشترطت أن تكون أداة إنشاء التوقيع الإلكتروني تحت سيطرة الموقع وحده دون غيره وتحت حيازته، إلا أنه يجوز لصاحب المفتاح الشفري الخاص أن يسند إلى جهة تصديقٍ إلكترونيٍّ مرخصٍ لها بتقديم خدمات التصديق الإلكتروني بحفظ مفتاح الشفري الخاص، وذلك بناءً على طلبٍ مقدمٍ منه بموجب عقدٍ مستقلٍ يتم إبرامه بينه وبين تلك الجهة، و وهذا ما نصت علية المادة (١٣/ ز) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري التى تم تعديلها بموجب القرار ٣٦١لسنة ٢٠٢٠.

حيث لا يجوز للجهة المرخص لها إبرام هذا العقد إلا بعد اعتماد نموذج هذا العقد من هيئة تنمية صناعة تكنولوجيا المعلومات وهذا ما نصت علية المادة (١٤) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري، وأيضا المادة ٤٩ من الترخيص رقم ١٠٣ لسنة ٢٠٠٦الصادر من هيئة صناعة تكنولوجيا المعلومات.

حيث يجوز لجهة التصديق المرخص لها بتقديم خدمات التصديق الإلكتروني بناءً على طلبٍ من الشخص مالك مفتاح الشفرة الخاصة أن تحتفظ بهذا المفتاح بموجب عقدٍ مستقلٍ يتم إبرامه بين جهة التصديق و الموقع و لكن بشرطٍ هو اعتماد نموذج هذا العقد قبل إبرامه من هيئة تنمية صناعة تكنولوجيا المعلومات، ونظرًا لخطورة وأهمية المفتاح الشفري الخاص فإنَّ الترخيصَ ١٠٣ لسنة ٢٠٠٦ وضع شروطًا والتزاماتٍ على جهة التصديق الإلكتروني عند تقديمها خدمة حفظ المفتاح الشفري الخاص وهي.

([١٤١٧]) انظر: المادة الثانية من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري التى تم تعديلها بموجب القرار رقم ٣٦١لسنة ٢٠٢٠.

أن تحتفظ بالمفتاح الخاص بالمستخدم بالطريقة التى لا تسمح بفكَّ شفرة المفتاح، عدم إفشاء أي معلوماتٍ قد تؤدي إلى التوصل للمفتاح الشفري الخاص، و أن لا يتم الاحتفاظ أو نسخ المفتاح الشفري الخاص أو أي معلوماتٍ تؤدي إليه إلا لدى المرخَّصِ له[١٤١٨].

حيث نحد أنَّ خدمةَ حفظِ مفتاحِ الشفرةِ الخاص من الخدمات المهمة، لأنها تحتوي على بيانات إنشاء التوقيع الإلكتروني الذي لا يكون معروفًا إلا لصاحبه فقط حيثُ أنَّ أي تسريبٍ أو إفشاءِ أي معلوماتٍ عنه تؤدي إلى معرفة فكَّ شفرةِ المفتاحِ الخاصَّ، مما يؤدي إلي كشفِ بياناتِ التوقيع الإلكتروني بالتالي الإضرار بصاحب مفتاح الشفرة الخاص، ولذلك وضعت اللائحة و الترخيص الصادر لمقدمي خدمات التصديق الالكتروني شروطًا والتزاماتٍ عند تقديمها خدمة حفظ مفتاح الشفرة الخاص وضعت العقوبات عند مخالفة ذلك.

ولكن حيث يؤخذ على المشرَّع المصريَّ أنه لم ينظمْ هذه الخدمة التي يقدمها مقدمو خدمات التصديق تنظيمًا كافيًا، حيث لم يوضح في قانون التوقيع الإلكتروني أو اللائحة التنفيذية ،مدة الحفظ أو المعايير التقنية الفنية التى تضمن عملية الحفظ، حيث نصَّ القانون فقط عدم إبرام مقدم الخدمة العقد مع العملاء إلا بعد اعتماد نموذج العقد من الهيئة، وحيث ترك لمجلس إدارتها وضع القواعد والضوابط في هذا الشأن التى تضمن حقوق ذوي الشأن، حيث كان يجب على المشرَّعِ النص عليها في القانون، حتى يكون التزام مقدم خدمات التصديق بالمعايير التقنية والفنية التى تضمن عملية الحفظ التى تكون مصدرها القانون، لضمان حقوق العملاء الذين يتعاقدون مع مقدم خدمات التصديق لحفظ مفتاح الشفرة الخاص لما له من أهميةٍ بالغةٍ في تحديدِ هويةِ الموقع في المعاملات الإلكترونية التى تتم عن بعد.

الفرعُ الثالثُ

تقديمُ خدمةِ الختمِ الإلكترونيِ والبصمةِ الزمنيةِ

أجرت وزارة الاتصالات وتكنولوجيا المعلومات تعديلاتٍ على اللائحة التنفيذية لقانون التوقيع الإلكترونى تتضمن إضافة خدمتى الختم الإلكترونى والبصمة الزمنية إلى اللائحة؛ وذلك بموجب القرار رقم ٣٦١لسنة ٢٠٢٠ الذى أصدره وزير الاتصالات وتكنولوجيا المعلومات بتعديل بعض أحكام اللائحة التنفيذية للقانون رقم ١٥ لعام ٢٠٠٤ الخاص بتنظيم التوقيع الإلكترونى وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

وجديرٌ بالذكر أنَّ هذه التعديلات التى تم اجراؤها فى بنود اللائحة تأتى فى إطار الحرص على نشر استخدام تكنولوجيا التوقيع الإلكترونى للأفراد والمؤسسات بما يتواكب مع التطورات التكنولوجية في هذا المجال؛ وأنَّ التعديلاتِ تسهم في دفعِ عملياتِ التحولِ الرقميَّ، ورفع كفاءة العمل الإدارى والارتقاء بالخدمات الحكومية، وكذلك توسيع أنشطة الشركات العاملة بهذا المجال خلال الفترة المقبلة.

[١٤١٨] انظر: المادة ٤٩ من الترخيص ١٠٣ لسنة ٢٠٠٦، الصادر من هيئة تنمية صناعة تكنولوجيا المعلومات.

لقد تضمن التعديلُ إضافة بعضِ التعريفاتِ وعددًا من المصطلحات المستخدمة فى هذا المجال وفقًا للمعايير المتبعة عالميًا، حيث نصت المادة الأولى على تعريف المصطلحات المتعلقة بتقديم خدمة الختم الإلكترونى وذلك علي النحو التالى:

– الختم الإلكترونى Electronic seal بأنه: "توقيعٌ إلكترونىٌّ يسمح بتحديد – الشخص الاعتبارى – مُنشيء الختم ويميزه عن غيره"، و منشئ الختم بأنه: "الشخص الاعتبارى الحائز على بيانات إنشاء الختم الالكترونى واستخدامه"، وبيانات إنشاء الختم الإلكترونى بأنها: "عناصر متفردة خاصة بمُنشئ الختم الإلكترونى وتميزه عن غيره، ومنها على الأخص مفاتيح الشفرة الخاصة به، والتى تُستخدم فى إنشاء الختم الإلكترونى"، و شهادة الختم الإلكترونى بأنها: "الشهادة التى تصدر من الجهة المرخص لها بالتصديق، وتثبت الارتباط بين منشئ الختم وبيانات إنشاء الختم الإلكترونى".

حيثُ أنَّ تقديمَ خدمة الختم الإلكترونى electronic seal الذى يسمح بتحديد الشخص الاعتبارى أو مُنشئ الختم ويميزه عن غيره بما يتيح توسيع استخدام تطبيقات التوقيع الالكترونى من قبل الجهات والمؤسسات المختلفة، و للحصول على خدمة الختم الإلكتروني للشخص الإعتباري يجب على الممثل القانوني للشركة تقديم أصول المستندات والوثائق للإطلاع عليها وهي على النحو الآتى: صورةٌ من المستخرج الرسمي للسجَّل التجاري أو قرار الإنشاءأو الإشهار، صورةٌ من البطاقة الضريبية، صورةٌ صحيفةِ الاستثمارِ أو الشركاتِ أو عقدِ الشركةِ، صورةُ إثباتِ الشخصيةِ للمديرِ المسئولِ.

كما تضمنت التعديلاتُ أيضًا إضافةَ خدمةِ البصمةِ الزمنيةِ الالكترونيةِ Time Stamp والتى تربط التاريخ والوقت بالمحرر الإلكتروني بطريقةٍ تمنع إمكانية تغيير البيانات دون اكتشافها، والاستناد إلى مصدرٍ زمنىٍّ دقيقٍ معتمدٍ من السلطة الجذرية العليا للتصديق الإلكترونى، ويُجرى إنشاءه بواسطة السلطة الجذرية العليا أو من إحدى الجهات المرخَّصِ لها من قِبلِ هيئةِ تنميةِ صناعةِ تكنولوجيا المعلومات وفقًا للضوابط الفنية والتقنية المنصوصِ عليها فى اللائحة.

حيث عَّرفت اللائحةُ التنفيذيةُ رقم ٣٦١لسنة ٢٠٢٠ في المادة (١٣/١) البصمةَ الزمنيةَ الالكترونيةَ Time Stamp بانها: "ما يوضع على محرر الكترونى ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها والتى تربط تلك البيانات بوقتٍ محددٍ لإثباتِ وجودِ هذا المحررِ الإلكترونىَّ فى ذلك الوقت"، بالتالى فإنَّ تقديمَ خدمةِ البصمة الزمنية الالكترونية، تستخدم في إثباتِ سلامةِ البيانات وارتباطها بالوقت والتاريخ، و يشترط لإثبات البصمة الزمنية الإلكترونية الشروط والضوابط الآتية: أن تربط التاريخ والوقت بالمحرر الإلكتروني بطريقة تمنع إمكانية تغيير البيانات دون اكتشافها، و أن يستند إلى مصدرٍ زمنيٍّ دقيقٍ معتمدٍ من السلطة الجذرية العليا للتصديق الإلكترونى.

يمكن أنْ تقدمَ هيئةُ تنميةِ صناعةِ تكنولوجيا المعلومات، بناءً على طلب كلَّ ذى شأنٍ، خدمةَ الفحصِ والتحققِ من صحة بيانات إنشاء التوقيع الإلكترونى والختم الإلكترونى نظير مقابلٍ يحدد فئاته مجلس إدارة الهيئة، ويجوز للهيئة أن

تعهد للغير بتقديم هذه الخدمة تحت إشرافها، وفى جميع الأحوال تصدر الهيئة شهادة فحص بيانات إنشاء التوقيع الإلكتروني[١٤١٩].

يمكن أن تقدم الهيئة أيضًا بناءً على طلب كل ذى شأن، خدمة فحص التوقيع الإلكتروني، الختم الإلكتروني، البصمة الزمنية الإلكترونية، نظيرَ مقابلٍ يحددُ فئاتهِ مجلسَ إدارةِ الهيئةِ، وتتحققُ الهيئةُ فى سبيلِ القيامِ بذلك من سلامة شهادة التصديق الإلكترونى وتوافقها مع بيانات إنشاء التوقيع الإلكترونى أو الختم الإلكتروني، و إمكان تحديد مضمون المحرر الإلكترونى محل الفحص بدقةٍ، و سهولة العلم بشخص الموقع أو منشىء الختم، و توافر الشروط الواردة فى المادة (٤) من هذه اللائحة؛ وذلك لفحص البصمة الزمنية الإلكترونية.

أما بخصوص شروط ومتطلبات منح تراخيص تقديم خدمات التصديق الإلكتروني، طبقًا لتعديل لإئحة قانون التوقيع الإلكتروني رقم ٣٦١لسنة ٢٠٢٠ ، فإنه جاري اعتمادها من هيئة تنمية صناعة تكنووجيا المعلومات.

الخاتمةُ:

بعد أن انتهينا – بفضلِ اللهِ وحمدهِ – من إنجاز هذا البحثِ يبدو لنا من العرضِ السابقِ لخدمات التصديق الإلكتروني، أنَّه من أبرزِ الموضوعاتِ القانونيةِ المستحدثةِ، والتي تثيرُ العديدَ من المشكلات، و الاختلافات الفقهية والقضائية.

وقد قمنا بتقسيم هذا البحث إلى مبحثين، قد تناولنا فى المبحثِ الأولِ خدمةَ إصدارِ شهادةِ التصديقِ الإلكترونيِ، مما لا شكَّ فيه أنَّ شهادةَ التصديقِ الإلكترونيَّ التى يصدرُها مقدمُ خدماتِ التصديق الإلكتروني لها دور فعَّالٌ في إبرامِ المعاملات التى تتم عبر وسائلِ الاتصال الحديثة وخاصةً في مجال الإثبات، قد يكون لها قوة المستندات الرسمية في الإثبات، ولذلك اعتني المشرعون في الإيضاح المقصود بشهادة التصديق وبياناتها، و ضع شروطَ إصدارِ شهادةِ التصديق الإلكتروني، ثم تناولنا بعد ذلك موقف المشرَّع المصريَّ و اللائحة الأوربية من حجَّية شهادةِ التصديق الإلكتروني الوطنية، وحجية شهادة التصديق الإلكتروني الأجنبية.

ثم تناولنا في المبحث الثانى الخدمات الأخرى التي يقدمها مقدمو خدمات التصديق الإلكتروني، حيث لم تقتصرْ اللائحة الأوربية على تقديم خدمة إصدار شهادات التصديق علي التوقيع الإلكتروني، بل أصبحت اللائحة تغطي خدمات الثقة الأخرى، وهي خدمة التحقق من التوقيعات الإلكترونية والأختام الإلكترونية، تقديم خدمة البريد الإلكتروني، خدمة ختم الوقت الإلكتروني، خدمة الحفظ المؤهلة للتوقيعات والأختام الإلكترونية، ثم عرضنا الخدمات الأخرى التى يقدمها مقدمو خدمات التصديق الإلكتروني في قانون التوقيع الإلكتروني المصري واللائحة التنفيذية لقانون التوقيع الإلكتروني التى تم تعديلها بموجب القرار ٣٦١لسنة ٢٠٢٠، الذي تضمن إضافة خدمتى الختم الإلكتروني والبصمة الزمنية.

التوصياتُ:

[١٤١٩] انظر: المادة السابعة من اللائحة التنفيذية لقانون التوقيع الإلكتروني، التي تم تعديلها بموجب القرار رقم ٣٦١ لسنة ٢٠٢٠.

١- يجب على المشرِّع المصريَّ أن ينظمَ الخدماتِ التى يقوم بها مقدمُ خدمات التصديق أكثرَ تنظيمًا في القانون أو اللائحة التنفيذية، وذلك للمحافظة على حقوقِ والتزاماتِ كلَّ طرفٍ من أطرافِ خدماتِ التصديق،حيث اقتصر فى القانون واللائحة على تنظيم خدمة إصدار شهادات التصديق الإلكتروني، بالرغم من قيام المشرِّع المصريَّ بتعديل اللائحة التنفيذية لقانون التوقيع الإلكتروني رقم ١٠٩لسنة ٢٠٠٥بموجب القرار رقم ٣٦١لسنة ٢٠٢٠، تتضمن إضافة خدمتى الختم الإلكتروني والبصمة الزمنية إلى اللائحة؛ الا أنَّه كان يجب أن يتضمن فى هذا التعديل الخدمات الآخرى المتعلقة بالتصديق الإلكتروني، مثل خدمات التشفير حيثُ أنَّ له أهميةً بالغةً في حمايةِ المعاملاتِ الإلكترونية وضمان سريتها، وكذلك وخدمة الحفظ الإلكتروني لأنَّ تقديمَ خدمةِ الحفظِ الإلكتروني لها أهميةٌ بالغةٌ في حمايةِ المحرَّرِ الإلكترونيَّ، من التزويرِ، أوالتقليدِ، أو الاصطناعِ أو غيرِ ذلك من صورِ التلاعبِ.

٢- نأملُ من المشرعَّ المصريَّ تعديلَ قانونِ التوقيعِ الإلكترونيَّ بما يتواكبُ مع التطوراتِ التكنولوجية في هذا المجالِ، حيث أدركَ المشرَّعُ الأوربيُّ هذا النقصَ في التوجيهِ الأوربيَّ ١٩٩٩/٩٣وسارعَ في إلغاءِ هذا التوجيهِ واعتمادِ اللائحةِ الأوربيةِ رقم ٩١٠لسنة٢٠١٤.

قائمة المراجع

أولًا – مراجع العربية:

د. إبراهيم الدسوقي أبو الليل، توثيق المعاملات الإلكترونية ومسئولية جهة التوثيق تجاه الغير المضرور، بحث مقدم في مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي، في الفترة من ٩-١١ربيع الأول ١٤٢٤هـ الموافق ٢٠٠٣/١٢/١٠م.

د. ألاء أحمد محمد الحاج علي، التنظيم القانوني لجهات التصديق التوقيع الإلكتروني، رسالة ماجستير، جامعة النجاح الوطنية،فلسطين،٢٠١٣. د. أيمن سعد سليم، التوقيع الإلكتروني، دار النهضة العربية، القاهرة، ٢٠١٣.

د. أمير فرج يوسف ،التوقيع الإلكتروني والحجية القانونية للتوقيع الإلكتروني في كافة المعاملات الإلكترونية، مكتبة الوفاء القانونية، الاسكندرية ،٢٠١١. د. أمير فرج يوسف،التوقيع الإلكتروني، دار المطبوعات الجامعية،٢٠٠٨. د. تامر محمد سليمان الدمياطي، إثبات العقد الإلكتروني عبر الإنترنت دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٠٨. د. حسن محمد بودي، التعاقد عبر الإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٩. د. خالد ممدوح إبراهيم، التوقيع الإلكتروني، دار الجامعة الجديدة للطباعة والنشر، الاسكندرية، ٢٠١٠.

د. خالد مصطفي فهمي، إبرام العقد الإلكتروني في ضوء التشريعات العربية والمنظمات الدولية، دار الجامعة الجديدة،الاسكندرية،٢٠٠٧. د. سامح عبد الواحد التهامي، التعاقد عبر الإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٨.

د. سهى يحيى الصباحين، التوقيع الإلكتروني وحجيته في الإثبات، رسالة دكتوراه، جامعة عمان العربية للدراسات العليا، الاردن،٢٠٠٥ .

د. عباس العبودي، تحديات الاثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ٢٠١٠.

د. عبد الفتاح بيومي حجازي، مقدمه في التجارة الإلكترونية، دار الفكر الجامعي، الاسكندرية، سنة ٢٠٠٣.

د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الكتب القانونية، القاهرة، ٢٠٠٧.

د. عبد الفتاح بيومي حجازي، إثبات المعاملات الإلكترونية عبر الإنترنت، دار الكتب القانونية، القاهرة،٢٠٠٩.

د.علاء حسين مطلق التميمي، الجهة المختصة بإصدار شهادة التصديق الإلكتروني، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١١ . د.عبير ميخائيل الصفدي، النظام القانوني لجهات التوثيق الإلكتروني، رسالة ماجستير، جامعة الشرق الأوسط للدراسات العليا، فلسطين،٢٠٠٩. د. غني ريسان جادر الساعدي، د.اكرم تحسين محمد حسن، النظام القانوني لشهادة التوثيق الإلكتروني، دراسة مقارنة، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الثاني،٢٠١٧. د. محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، الطبعة الأولي، دار الفكر الجامعي، الاسكندرية، ٢٠٠٦. د. ممدوح محمد مبروك، مدى حجية التوقيع الإلكتروني في الإثبات، دار النهضة العربية، ٢٠٠٩.

ثانيًا: المراجع الفرنسية:

1. E.MONTERO, « Définition et effets juridiques de la signature électronique en droit belge : appréciation critique », in La Preuve, Formation permanente CUP, Liège, Volume 54, mars 2002.
2. E. MONTERO, « Du recommandé traditionnel au recommandé électronique : vers une sécurité et une force probante renforcées » in Lecommerce électronique : de la théorie à la pratique, Cahiers du CRID, n° 23, Bruxelles, Bruylant, 2003.
3. E.Caprioli, Signature électronique et dématérialisation, LexisNexis, 2014.
4. MOUGENOT, La preuve, tiré à part du Répertoire Notarial, 4ème édition, Larcier, Juin 2012.
5. Georges Didier, Cadre juridique pour les signatures électroniques et les services de certification : Analyse de la loi du 9 juillet 2001.
6. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et lesservices de confiance (eIDAS) : analyse approfondie », février 2015.
7. GOBERT, " La loi belge du 21 juillet 2016 mettant en œuvre le règlement européen eIDAS et le complétant avec des règles sur l'archivage électronique : analyse approfondie".octobre,2016.
8. Luc Grynbaum, La Preuve littérale et la signature à L'Heure de la communication électronique. J.C.P., nov. 1999.
9. M. DEMOULIN, Collection du CRIDS, Larcier, Mai 2012.
10. M. DEMOULIN et D. GOBERT, «L'archivage dans le commerce électronique: comment raviver la mémoire? », in M. DEMOULIN (dir.), Commerceélectronique, de la théorie à la pratique, Cahiers du CRID, 2003.
11. P. LECOCQ et B. VANBRABANT, « La preuve du contrat conclu par voie électronique » in Le commerce électronique : un nouveau mode de contracter? Editions du jeune barreau de Liège, 2001.
12. VANBRABANT, , « La signature électronique des personnes morales », in La preuve, Liège, Formation permanente CUP, 2002.
13. O. VAN CUTSEM, « L'évolution technologique et le monde postal. La validité juridique du courrier recommandé électronique en Belgique », C.J., n°3/2003.