الفصل الثالث عشر

قانون التوقيع الإلكتروني وضرورته لدعم

نمو التجارة الإلكترونية

تزداد أهمية التجارة الإلكترونية عبر الإنترنت واستخداماتها يوماً بعد يوم. وتعتبر العقود الوسيلة الأساسية التي يستخدمها الباعة والمشترون عبر هذه الشبكة.

غير أن إبرام العقود بالأساليب الإلكترونية يثير بعض التحديات للقواعد القانونية التي استقر عليها التعامل سنين عديدة، ومنها ضرورة تعبير المتعاقدين عن إرادتهم الالتزام بالعقد عن طريق توقيعهم عليه، هذا التوقيع الذي يتم عادةً عن طريق الإمضاء، الختم أو بصمة الإصبع.

فضلاً عن ذلك، فإن إبرام العقود باستخدام الأساليب الإلكترونية يثير بعض الغموض الذي قد يقع فيه أحد المتعاقدين عن شخصية وأهلية وسلطة المتعاقد الآخر الذي يتم تبادل الرسائل الإلكترونية معه أملاً في إبرام العقد، حيث تعتبر هذه الامور أركاناً أساسية في إبرام أي عقد، وقد يؤدي عدم توافرها أو وجود عيبٍ فيها إلى بطلان العقد برمته، أو على الأقل قابليته للإبطال.

فعلى سبيل المثال، وفيما يتعلق بالأهلية، يجعل القانون جميع تصرفات المجنون والمعتوه والطفل الصغير غير المميز الذي يقل عمره عن سبع سنوات باطلةً بطلاناً مطلقاً، في حين يجعل العقود التي يبرمها القاصر الذي لم تكتمل أهليته ببلوغه سن الرشد (وهي الثامنة عشرة في أغلب قوانين العالم) قابلة للإبطال لمصلحة هذا القاصر، بحيث يستطيع استعمال هذا الخيار عند اكتمال أهليته، فكيف سيكون بإمكان المتعاقد عن طريق البريد الإلكتروني مثلاً التحقق من مدى اكتمال أهلية المتعاقد الآخر، لكي يضمن أن العقد الذي سيبرمه معه بهذا الأسلوب هو عقد صحيح لا تشوبه شائبة؟ وفضلاً عما سبق، فمن الجائز أن يقوم أحد الأشخاص باستخدام البريد الإلكتروني العائد لآخر (كما لو استطاع الحصول على كلمة السر الخاصة بحساب بريده الإلكتروني) ويتظاهر من خلاله أنه هو صاحب ذلك البريد، ولن يكون بالتالي من الممكن بسهولة على مستلم البريد التحقق من شخصية المرسل. كما أنه قد يتصرف شخص وكأنه نائبٌ عن شخص آخر أو ممثلٌ لشخصٍ اعتباري، كشركة أو مؤسسة، وأن له السلطة ليبرم العقود بالنيابة عنه، ويرسل بناءً على ذلك بريداً إلكترونياً إلى الآخرين، ويتبادل الرسائل معهم، من دون أن يكون بإمكان هؤلاء التحقق من صحة زعم ذلك الشخص، خاصةً وأنه قد يكون مستخدماً البريد الإلكتروني العائد للمؤسسة ذاتها، في حين أنه في الواقع ليس أكثر من مجرد موظف صغير فيها لا يملك من الأمر شيئاً.

إن ما ذكرناه سابقاً من أساليب للخداع يسهِّل البريد الإلكتروني استخدامها واللجوء إليها، يمكن نسبه لخاصية جهالة الهوية (**Anonymity**) المرافقة لاستخدام البريد الإلكتروني والناجمة عن عدم قدرة طرفي العلاقة على اللقاء والتماس المباشر مع بعضهم. وتسمح هذه الخاصية باستخدام الإنترنت والبريد الإلكتروني بشكل كبير جداً في أعمال الاحتيال ونهب

الأموال. لا تقتصر أساليب الخداع السابقة الذكر بالطبع على التعاقد باستخدام الأساليب الإلكترونية، إذ أنها قد تستخدم في كل عقدٍ، ومهما كانت أساليب إبرامه، غير أن استخدام الوسائل الإلكترونية في التعاقد يزيل من أيدي المتعاقدين بعضاً من الظروف والقرائن التي قد تساعدهم في اكتشاف الاحتيال والتزوير، وفي تجنب العيوب التي قد تنتاب العقود والناجمة عن شخصية المتعاقد الآخر أو أهليته أو سلطته في التعاقد، ومن هذه الظروف الاحتكاك والتماس المباشر بين الأطراف، التأكد من شخصيات الأطراف ومن أعمارهم بالاطلاع على هوياتهم، فضلاً عن وجود الشهود والتوقيع على مستندٍ مكتوبٍ، يدون عليه كل واحد من المتعاقدين المعلومات الكاملة عن شخصيته. استطاع التقدم التكنولوجي أن يقدم للإنسان وسائل وأدوات وتقنيات تؤدي وظائف التوقيع وتنوب عن اللقاء المباشر بين أطراف العقد، بحيث أنها تساعد المتعاقد على تجاوز تلك المخاطر للوصول إلى التحقق الكامل من شخصية وأهلية ذلك الإنسان الذي يتم تبادل البريد الإلكتروني معه للوصول إلى إبرام عقدٍ سليمٍ لا شائبة فيه، وسنحاول إعطاء لمحة موجزة عن بعض هذه التقنيات، والتنظيم القانوني لها في هذا البحث.

التقنيات التي تؤدي وظائف التوقيع التقليدي في بيئة التجارة الإلكترونية: أتاح التطور التكنولوجي عدداً من الوسائل التي قد يكون من الممكن استخدامها كبديلٍ عن التوقيع في البيئة الإلكترونية، بحيث نحصل على ما يمكن تسميته بالتوقيع الإلكتروني.

ومن هذه الوسائل: بصمة الأصبع الرقمية، صورة رقمية عن شبكية العين أو تقنية التعرف الصوتي (وهما وسيلتان مما يمكن تسميته بالبيومتركس، وهي خصائص بيولوجية خاصة في جسم الإنسان، لا تتكرر من شخص إلى آخر أبداً.)، استخدام رقمٍ أو كلمة سر، صورة عن التوقيع

اليدوي التقليدي موضوعة على رسالة إلكترونية، مجرد كتابة الشخص لاسمه في نهاية الرسالة، وأخيراً ما يسمى بتقنية المفتاح العمومي.

تختلف هذه الوسائل طبعاً عن بعضها البعض من حيث درجة الموثوقية والأمان التي تؤمنها لمستخدميها. وإذا كانت تقنية المفتاح العمومي تقدم لمستخدميها أعلى درجات الموثوقية والأمان باستخدامها، كما سنرى لاحقاً، فإن البيومتركس أو الخصائص الذاتية الشخصية تليها من حيث درجة الأمان التي تؤمنها، فهذه الخصائص الشخصية يستحيل انتحالها واستعمالها من شخص آخر غير صاحبها، ويتطلب استخدامها بالطبع أخذ عينةٍ من خصائص الشخص قبل أن يكون من الممكن استخدام هذه التقنية كتوقيعٍ إلكتروني. ويلي البيومتركس من حيث الأهمية والموثوقية، اتخاذ كلمة سر معينة أو رقم بطاقة الاعتماد. وتأتي فيما بعد عملية وضع صورةٍ عن التوقيع التقليدي في أسفل الرسالة، أو مجرد كتابة الاسم أسفل الرسالة، في آخر قائمة الوسائل الممكن استخدامها كتوقيع إلكتروني.

و بناءً على ما ذكرناه يمكننا تعريف التوقيع الإلكتروني "بأنه أية حروفٍ أو رموز أو أرقام يعبر عنها بالأساليب الإلكترونية، موضوعة ومتبناة من قبل شخصٍ ما، مع توافر نية توثيق كتابةٍ معينة لديه.

التوقيع الإلكتروني باستخدام تقنية المفتاح العمومي:

يعتبر التوقيع الإلكتروني باستخدام تقنية المفتاح العمومي، أو ما يمكن تسميته بالتوقيع الرقمي، أحد أهم الوسائل لتأمين الأمان والموثوقية في بيئة الإنترنت والتجارة الإلكترونية، إذ أن التوقيع الرقمي باستخدام هذه التقنية يعتبر وسيلةً كبيرة الفعالية لتحقيق الثقة بين شخصين لا يعرف أحدهما الآخر، ويشجعهما بالتالي على الإقدام على التعامل مع بعضهما تجارياً.

ولكن ما هي آلية عمل التوقيع الرقمي، وكيف تؤدي هذه الآلية إلى إنشاء الثقة بين الأطراف عن طريق استخدامه؟

تبدأ العملية بكتابة الرسالة التي يراد إرسالها، سواء أكانت الكتابة ضمن برنامج البريد الإلكتروني مباشرةً، أو كانت على ملف خاص تتم الكتابة عليه ويتم إلحاقه في ما بعد بالبريد الإلكتروني ليرسل معه. وبعد أن تتم عملية الكتابة، يتم توقيعها رقمياً، وذلك بأن يتم إدخالها إلى برنامج تشفير يقوم بتطبيق معادلة رياضية عليها، تقوم بتحويلها إلى صيغة تبدو غير مفهومة وغير قابلة للقراءة. ولكي تتم عملية التشفير هذه لا بد من استخدام منشئ هذه الرسالة لما يسمى بمفتاحه الخاص، وهذا المفتاح هو مجموعة من الأعداد الضخمة التي يتم الحصول عليها باستخدام سلسلة من الصيغ الرياضية المطبقة على أعداد أولية. ومن ثم يقوم المنشئ بإرسال الرسالة فيما بعد. عندما تصل الرسالة إلى المرسل إليه لا بد له لكي يستطيع قراءتها من معرفة المفتاح العام لمرسلها، حيث يقوم مستلم الرسالة بإدخال الرسالة إلى برنامج تشفيرٍ موافقٍ لذلك الذي أدخلها المرسل إليه، مستخدماً المفتاح العام العائد للمرسل، والذي يعتبر مترابطاً مع مفتاحه الخاص، فتتم عملية التعرف على شخصية المنشئ، والتأكد بالتالي من أن الرسالة لم يتم العبث بها بعد أن تم توقيعها، ويتم بعد ذلك تحويلها مرة أخرى إلى صيغة مقروءة يفهمها مستلم الرسالة الإلكترونية .

مما سبق نرى أن التوقيع الرقمي يتطلب وجود مفتاحين، الأول يسمى بالمفتاح الخاص، والذي يستخدمه المرسل لكي يوقع على رسالته الإلكترونية أو على الوثيقة المرفقة بها، حيث أنه من المفترض به أن يحتفظ بهذا المفتاح سرياً، وأن لا يعلم به أحد لأنه مرتبط بشخصه كلياً، أما المفتاح الآخر وهو المفتاح العام فإن الموقع يعطيه إلى الآخرين، ويمكن أن يعلن عنه

وأن يضعه على منشوراته ومطبوعاته، لكي يكون بالإمكان استخدامه لفك تشفير الرسائل والوثائق التي سيرسلها إليهم.

وتواجهنا الآن مشكلة تتلخص في الكيفية التي يستطيع من خلالها الناس التحقق من أن المفتاح العام الذي بين يديهم يعود لذلك الشخص الذي يزعم أنه يملكه، فقد ينتحل شخصٌ ما شخصية آخر، ويرسل لهم المفتاح العام الذي يملكه على أنه مملوكٌ لشخصٍ آخر، فكيف يمكن التحقق من شخصية مالك هذا المفتاح؟ للتخلص من المشكلة السابقة تم ابتداع ما يسمى بسلطة التوثيق، وهي هيئة مستقلة تقدم خدماتها بوصفها طرفاً ثالثاً موثوقاً، يقوم بإصدار شهاداتٍ رقمية يستطيع من خلالها أي إنسان التعرف على المفتاح العام العائد لأيِّ شخصٍ من الأشخاص، والتعرف أيضاً على جميع المعلومات الخاصة به (طبعاً إن كان يملك مفتاحاً خاصاً به ومشتركاً لدى سلطة التصديق أيضاً) بدلاً من أن يلجأ إلى الحصول على هذا المفتاح من ذلك الشخص مباشرة. وقد سميت سلطة التوثيق هذه في قانون اليونسترال النموذجي للتجارة الإلكترونية بمقدم خدمات التوثيق، والذي عرِّف بأنه شخصٌ يصدر الشهادات (وهي رسالة بيانات أو أي سجل آخر يؤكد الارتباط بين الموقِّع وبيانات إنشاء التوقيع) ويجوز أن يقدم خدماتٍ أخرى ذات صلة بالتوقيعات الإلكترونية.

قوانين التواقيع الإلكترونية حول العالم:

هل يتمتع التوقيع الإلكتروني بالقوة القانونية نفسها التي يتمتع بها التوقيع أو الإمضاء اليدوي التقليدي؟ وبمعنى آخر، هل تعترف القوانين في العالم بحجية التوقيع باستخدام هذه الأساليب؟ فالعديد من القوانين التقليدية تتطلب أن يكون التوقيع مكتوباً، فهل يتحقق هذا الشرط في حال استخدام التوقيع الإلكتروني؟ لحسم الخلاف حول هذه التساؤلات، ظهرت في

السنوات العشر الأخيرة العديد من القوانين حول العالم التي شرَّعت ونظمت استخدام التوقيع الإلكتروني في الإثبات. وقد نهجت العديد من الدول عند صياغة تلك التشريعات منهجاً يسمى بالحياد التكنولوجي (**Technological Neutrality**) ، ومضمون هذا المنهج أن قانون التوقيع الإلكتروني لا يجب أن ينص على تقنية معينة تستخدم في عملية التوقيع في بيئة التجارة الإلكترونية ، وإنما من المتوجب بدلاً من ذلك أن ينص على شروط معينة من الواجب توافرها في التوقيع لكي يكون له حجية قانوناً. قامت هيئة الأمم المتحدة للقانون التجاري الدولي (يونسترال) في عام ١٩٩٦ ، بوضع أول قانونٍ تضمَّن تنظيماً لمسألة التوقيع الإلكتروني ، حيث قامت اليونسترال بعد إدراكها لأهمية التجارة الإلكترونية ، بوضع قانونٍ نموذجٍ للتجارة الإلكترونية ، لتقوم الدول الأعضاء في الأمم المتحدة باحتذائه والاقتداء به عند قيامها بوضع تشريع ينظم هذه التجارة.

تطرق هذا القانون في المادة السابعة منه إلى مسألة التوقيع الإلكتروني ، ومدى حجيته في الإثبات في العمليات التجارية المبرمة بالأساليب الإلكترونية ، حيث نصت المادة المذكورة على أنه:

عندما يشترط القانون وجود توقيعٍ من شخصٍ، يستوفي ذلك الشرط بالنسبة إلى رسالة البيانات إذا:

أ- استخدمت طريقة لتعيين هوية ذلك الشخص والتدليل على موافقته على المعلومات الواردة في رسالة البيانات.

ب- وكانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله رسالة البيانات. أي أن هذا القانون يعطي التوقيع الإلكتروني الحجية نفسها للتوقيع التقليدي بشرط توافر شرطين:

أولهما إمكانية التعرف على الشخص الموقع وموافقته على محتوى الوثيقة الموقعة.

والآخر هو كون الطريقة المستخدمة في التوقيع للتعرف على شخصية الموقع موثوقة وآمنة. فيما بعد، وفي عام ٢٠٠١ قامت اليونسترال بإكمال المادة السابعة المذكورة بوضع تشريعٍ نموذجٍ آخر خاص بالتواقيع الإلكترونية، حيث نظم هذا التشريع مسألة التوقيع الإلكتروني ومقدم خدمات التوثيق بشكلٍ تفصيلي، إذ نصت المادة السادسة منه على أنه:

حيثما يشترط القانون وجود توقيعٍ من شخص، يعد ذلك الشرط مستوفى بالنسبة إلى رسالة البيانات إذا استخدم توقيع إلكتروني موثوق به بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله رسالة البيانات)) . وتنص الفقرة الثالثة من هذه المادة على الحالات التي يكون فيها التوقيع الإلكتروني موثوقاً به حيث تقول:

يعتبر التوقيع الإلكتروني موثوقاً به لغرض الوفاء بالشرط المشار إليه في الفقرة (١) إذا:

آ – كانت بيانات إنشاء التوقيع مرتبطة في السياق الذي تستخدم فيه، بالموقع دون أي شخص آخر .

ب – كانت بيانات إنشاء التوقيع خاضعةً وقت التوقيع، لسيطرة الموقع دون أي شخص آخر.

ج – كان أي تغيير في التوقيع الإلكتروني يجري بعد حدوث التوقيع، قابلاً للاكتشاف.

د – كان الغرض من اشتراط التوقيع قانوناً هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع وكان أي تغيير يجري في تلك المعلومات بعد التوقيع قابلاً للاكتشاف)) .

وفي عام ٢٠٠١ أيضاً أصدر الاتحاد الأوروبي توجيهاً حول التواقيع الإلكترونية، حيث ميز هذا التوجيه بين التوقيع الإلكتروني البسيط والتوقيع الإلكتروني المتقدم. ويتطلب التوجيه الأوروبي في التوقيع الإلكتروني المتقدم عدداً من الشروط الخاصة بضمان الأمان والموثوقية، والتي لا تعتبر مطلوبةً بالنسبة لذلك البسيط. وبالمقابل فقد أعطى للتوقيع المتقدم مزيةً أكبر من حيث الاعتراف الكامل بحجيته أمام القضاء، بالمقارنة مع حجية التوقيع الإلكتروني البسيط. والتوقيع الإلكتروني المتقدم يتطلب: رابطةً قويةً بين التوقيع والموقِّع، قدرةً على التعرف على شخصية الموقع، إنشاء التوقيع باستخدام وسائل تقع تحت سيطرة الموقع الوحيدة، وأخيراً قدرة مستلم الرسالة على التحقق منها وعلى اكتشاف حدوث أي تعديلات على الرسالة أو الوثيقة الرئيسة المرسلة من الموقع.

أما في الولايات المتحدة الأميركية فقد أصدر الكونغرس الأميركي في عام ٢٠٠٠ قانوناً موحداً للتوقيع الإلكتروني يسري في الولايات جميعها، وقد نص هذا القانون بأنه لا يمكن تجريد التوقيع من آثاره القانونية أو حجيته لمجرد أنه جاء بالشكل الإلكتروني، وأنه إذا تطلب القانون وجود توقيع، فإن وجود توقيع إلكتروني يجعل هذا المطلب محققاً. إنَّ هذا القانون لم يشترط توافر خصائص معينة في التوقيع لكي يكون له حجية قانونية، وبالتالي فإن استخدام أيٍ من الوسائل التي ذكرناها أعلاه كتوقيع إلكتروني يعتبر موفياً بالمتطلبات القانونية للتوقيع. خاصية الحياد التكنولوجي في تشريعات التواقيع الإلكترونية حول العالم.

بعد أن استعرضنا بعض التشريعات المتعلقة بالتواقيع الإلكترونية حول العالم، ورأينا ما فيها من اختلافات لناحية الحياد التكنولوجي، أصبح بإمكاننا أن نصنف القوانين حول العالم من هذه الناحية، ضمن فئاتٍ ثلاث:

١- قوانينٌ ذكرت صراحةً في صلب تشريعاتها الخاصة بالتواقيع الإلكترونية، أن تقنية المفتاح العمومي يجب أن تستخدم في عملية التوقيع الإلكتروني، ومن الدول التي أخذت بهذا النهج ألمانيا، فهي أخذت بعين الاعتبار التكنولوجيا المتوافرة حالياً، مفضلةً إمكانية اللجوء إلى تعديل القانون في المستقبل في حال تطور التكنولوجيا، على أن يكون القانون عاماً غير محدد.

٢- قوانينٌ أخرى أخذت بمعيارٍ متدرج من حيث قوة التوقيع الإلكتروني في الإثبات، حيث أن هذه القوانين أخذت بمبدأ الحياد التكنولوجي ضمن حدود وشروط، فقد فرقت هذه القوانين في المعاملة بين الأشكال المتعددة للتواقيع الإلكترونية، فهي وإن كانت اعترفت بأن للتوقيع بالشكل الإلكتروني حجية في الإثبات، إلا أنها أعطت هذا التوقيع الإلكتروني قوةً كاملةً إذا ما توافرت شروط خاصةٌ بهذا التوقيع، ولا تتوافر هذه الشروط فعلياً في ظل التطور التقني الحالي، إلا في تقنية المفتاح العمومي. ويدخل ضمن هذه الفئة، توجيه الإتحاد الأوروبي، وقانونا الأمم المتحدة النموذج.

٣- قوانينٌ كانت شديدة السماحية، بحيث أنها كانت محايدة تكنولوجياً بشكل كامل، وقوانين أغلب الدول في العالم تندرج تحت هذه الفئة، ومنها الولايات المتحدة الأميركية.

إنَّ هاتين الفئتين الأخيرتين أخذتا بعين الاعتبار إمكانية التطور التكنولوجي في المستقبل، وضرورة أن يكون القانون شاملاً ومطبقاً على تلك التقنيات المستقبلية التي قد تستخدم في عملية التوقيع الإلكتروني. فأي المناهج القانونية هي الأولى بالاتباع، فيما إذا أرادت بلادنا سنَّ قانونٍ خاص ينظم استخدام التواقيع الإلكترونية؟ إن الغاية من سن قانونٍ للتوقيع الإلكتروني هي ضمان الأمان والموثوقية للمتعاملين بالتجارة الإلكترونية،

وبالتالي فإن القانون الأسلم هو ذلك الذي ينص على ضرورة توافر شروطٍ معينة في التوقيع الإلكتروني لكي يكون من الممكن الاعتراف بحجيته في الإثبات، فالناس لن تتعامل بالتوقيعات الإلكترونية إلا إذا شعرت بأنها تحقق لها المستوى ذاته من الثقة الذي تحصل عليه عندما تجتمع مع بعضها شخصياً.

وبناءً عليه، فإن الدول التي أخذت بالمعيار المتسامح، واعترفت لجميع التواقيع الإلكترونية، ومهما كان الشكل الذي جاءت فيه، بالقوة الكاملة في الإثبات لن تدعم التجارة الإلكترونية، إذ أنها لن تحقق الغاية من سنِّها وإصدارها، فالتوقيع الإلكتروني وفقاً لها لا يطمئن نفوس المتعاملين به.

أما القوانين التي نصت على استخدام وسيلةٍ معينة كتوقيع إلكتروني، فهي كذلك لا تخلو من النقد، إذ أنها ضيَّقت كثيراً، وقد تسبب في المستقبل إعاقة التكنولوجيا في حال ابتداع تقنيات جديدةٍ للتوقيع، حيث أن عملية التطور التكنولوجي دائماً أسرع بكثير من عملية التطور التشريعي، والتي تأخذ عادةً زمناً ليس بالقصير. أما المنهج الذي اتبعه الاتحاد الأوروبي فهو يعتبر الأمثل والأصلح للاتباع، فهو وإن كان لم يتطلب استخدام تقنية بعينها، غير أنه وضع شروطاً معينة لا بد من توافرها في التقنية المستخدمة في عملية التوقيع، لكي تصنف بأنها توقيع إلكتروني متقدم، ولكي نعطيها قوةً كاملة في الإثبات، وهذه الشروط في الواقع الحالي، لا تتوافر إلا في تقنية المفتاح العمومي، أو ما يسمى بالتوقيع الرقمي، أي كأن الاتحاد الأوروبي قد دعا إلى استخدام هذه التقنية بشكلٍ ضمني، إلا أنه ترك الباب مفتوحاً على مصراعيه لأي تقنية قد يتمكن العلم من استحداثها مستقبلاً، طالما تحقق الشروط التي تطلبها.

إن الوظائف التي يؤديها التوقيع التقليدي عادةً تتمثل بما يلي:

التوقيع هو وسيلة للتحقق من شخصية الموقع، ولمعرفة الموقِّع بالأثر

القانوني الذي سيترتب على عملية توقيعه، ومن أجل التحقق من إقرار الموقِّع وموافقته على محتوى الوثيقة الموقعة منه، وأخيراً فهو وسيلةٌ تحرم الموقع من القدرة على الرجوع عن الوثيقة الموقع عليها، وعن الالتزام الوارد بها بعد إتمام عملية التوقيع. وفعلاً، فإنه إذا ما قمنا بمقارنة هذه الوظائف وحاولنا تطبيقها على تقنية المفتاح العمومي، فإننا نجد أن هذه التقنية تقوم بهذه الوظائف كاملةً، مما يضفي على عملية التعاقد في بيئة التجارة الإلكترونية باستخدامها ضماناً وأماناً وثقةً كاملين في نفوس المتعاقدين. وفضلاً عن ذلك، فإنه يمكننا اعتبار التوقيع الإلكتروني باستخدام هذه التقنية أكثر ثقةً واعتباراً من التوقيع اليدوي التقليدي، ولا بد من إعطائه بناءً على ذلك قوة ووزناً أكبر، فهو لا يدلنا فقط على شخصية الموقع، وإنما يؤكد لنا أيضاً بأن الوثيقة لم تحرَّف بعد أن تم توقيعها، وهو ما لا يستطيع التوقيع اليدوي التقليدي تحقيقه.