خصوصية التوقيع الرقمي في توثيق العقود الإلكترونية

حليتيم سراح (طالب دكتوراه)
جامعة مستغانم
Sarah.halitim@univ-mosta.dz

تاريخ الإرسال: 2017/07/14 تاريخ المراجعة: 2017/11/06 تاريخ القبول: 2017/11/20

ملخص:

تهدف هذه الدراسة إلى تحديد مدى أهمية تقنيات التوقيع الرقمي في حماية المعاملات القانونية وتوثيقها، من خلال عمليات التشفير بمختلف صوره، وجاء ذلك على خلفية صدور القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين الذي نظم إجراءات التوقيع الرقمي باستعمال مفاتيح التشفير وخوارزميات إنشاء التوقيع الرقمي إضافة إلى إحاطة عملية التشفير بجهات رسمية تسمى بمؤدي خدمات التصديق الإلكتروني، وبرامج إلكترونية مخصصة لإحداث التوقيع الرقمي وللتحقق من سلامته، ما يضفي ذلك مصداقية وقوة للمحررات المنشأة عبر الدعامة الإلكترونية. ومن أجل ذلك جاءت هذه الدراسة لتوضيح مدى فعالية عمليات التوقيع الرقمي سواء التقنية منها أو الإدارية في حماية وضمان العقود الإلكترونية

الكلمات المفتاحية: التوقيع الرقمي ; التشفير ; شهادة تصديق ; مؤدي خدمات التصديق.

Abstract:

This study will set to specify the importance of electronical numeric signature to protect the treatment of laws and their rectifications from deciphering operations with different images. it was mentioned in backward of law 04-15 that is concerned signatures and electronical rectifications which organised the steps of numeric signature with the use of deciphering key and algorithms of numeric signature in addition, turning deciphering operation with principles. It was called

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368

as service electronical rectification and electronical programs that specified to occur numeric signature and to check its safety . Moreover , the value and the power to liberate the basic of electrons. For the sake of that this study came to clarify the effecacity of numeric signature operations either technic from it or administrations to protect and guarantee electronic contracts.

Key words: Numeric signature; deciphering; rectification certificate; expert in service of rectification.

مقدمة:

مع كثرة المعاملات القانونية وسرعتها ، وفي ظل التقدم التكنولوجي الذي نعيشه، كان لابد من اعتماد وسائل جديدة تتسق بين عملية إبرام التصرفات القانونية وسبل تسييرها بشكل اضمن وأسرع يتماشى والتطور التكنولوجي، وهذا من خلال استخدام الوسائل الإلكترونية لإبرام هذه التصرفات عبر الشبكة المعلوماتية. غير أنه وضمانا لحماية ولتجسيد مفهوم الخصوصية والأمن للمتعاملين عبر شبكة الانترنت وحفاظا على سرية المعلومات وهوية الأشخاص ولحماية المعاملات الإلكترونية كان لابد من اتخاذ إجراءات وقائية، تكون من خلالها بيانات التعاقد ومعلوماته في مأمن من العبث بها، عند تداولها والتي تعتبر كوسيلة تضمن حماية هذه المعلومات من التزوير وتقليده وذلك عن طريق ما يسمى "بالتوقيع الإلكتروني"، وقد نظم المشرع الجزائري أحكام التوقيع الإلكتروني في القانون 15-04، والذي عرفه على أنه "بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق"[1]. إلى جانب تنظيمه لمفاتيح التشفير والذي تعتبر كوسيلة تقنية تضمن بشكل أوسع حماية هذه المعاملات وتوثيقها بشكل أسرع، ويحتل التوقيع الرقمي أهمية كبيرة في إبرام العقود الإلكترونية لما يتمتع به من خاصية وقائية لحماية وتوثيق المعاملات الإلكترونية، وهذا بعد الحصول على شهادة التصديق الإلكترونية المسلمة من قبل جهات التوثيق الالكتروني، وعليه كيف يمكن لتقنيات التوقيع الرقمي أن تحقق ضمانا في حماية وتوثيق العقود الإلكترونية؟

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368

وسنحاول الإجابة على هذه الإشكالية من خلال التطرق إلى محورين أساسين يتعلق أولهما: بإبراز مكانة التوقيع الرقمي في إبرام العقد الإلكتروني أما المحور الثاني بمعالجة مدى فعالية التوقيع الرقمي في توثيق العقد الإلكتروني.

المحور الأول: مكانة التوقيع الرقمي في إبرام العقد الإلكتروني

إن الضرورات الحتمية التي فرضتها تكنولوجيا المعلومات أدت بالمشرع إلى تدارك ذلك في إطار إبرام العقود وهذا من خلال فتح المجال للوسائل الالكترونية في التعبير عن الإرادة والتي أحيطت بخاصية حمائية تتجسد في توقيع تلك العقود رقميا باستعمال تقنيات التشفير الإلكتروني.

أولا: تحديد ماهية التوقيع الرقمي- التشفير الإلكتروني-

ظهر التشفير قديما بمصر عام 2000 قبل الميلاد، واستعمل التشفير كسلاح في الحروب لاسيما في الحرب العالمية الأولى، أين استعمل سنة 1917 لفك رموز برقية مرسلة من برلين إلى السفير الألماني في واشنطن، ويعتبر التوقيع الرقمي وسيلة من وسائل التوقيع الإلكتروني وهو عبارة عن بيانات رقمية متسلسلة قوية يصعب اختراقها، لاعتماده على معادلات حسابية يتم من خلالها تحويل المعاملات والاتصالات بطريقة آمنة باستخدام مفاتيح التشفير إلى نص مشفر، على نحو لا يمكن تعديل أو تغيير في أصل النص إلا لمن يحمل مفتاح التشفير.

ويحتاج التشفير الإلكتروني إلى مفتاحين أحدهما يستعمل في تشفير الرسالة من قبل صاحبها ويسمى المفتاح الخاص ويكون سريا لا يعلمه إلا صاحبه، لأما الآخر فيستعمل في فك التشفير والتأكد من صحة التوقيع ويكون معلوما للجميع ويسمى المفتاح العام، ويحتاج إلي الغير من أجل فك تشفير الرسالة الأصلية هي الرسالة المستقبلة، ولتشفير الرسالة المرسلة.

ومن هذا المنطلق يشكل التوقيع الرقمي أهمية بالغة في حماية العقود الإلكترونية من حيث مصداقيته والذي من خلاله يتم التأكد من صحة المرسل. كما أنه بموجبه تتجسد سرية المعاملات من خلال حماية هوية المستخدم وحماية البيانات من التغيير والعبث بها، ويتم نشر الثقة والأمن خلال عملية الإرسال[3]، مما يضيف على المحرر

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368

الموقع رقميا مصداقية عالية يجعل منه دليلا للإثبات نظرا لعدم قدرة أي جهة بإنكار أن التوقيع صادرا منها.

ثانيا: استناد التوقيع الرقمي على تقنيات فنية للتشفير

يستند التوقيع الرقمي إلى عمليات تقنية تمر بعدة مراحل من إنشاء التوقيع إلى التحقق من الموقع، فيتم إنشاء التوقيع من صاحب الرسالة باستخدام مفتاحه الخاص، باستخدام آليات الإنشاء التي عرفها القانون 15-04 على أنها: "جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني"، أما التحقق من التوقيع والتثبيت من صحته[4] فيكون من جانب المرسل إليه استنادا على المفتاح.[5]

وتختلف ميزات وتقنيات التوقيع الرقمي بحسب نوع التشفير، والتي تنقسم إلى ثلاث أنواع التشفير المتماثل والتشفير اللامتماثل والمزج بين الطريقتين السابقتين.

أ- التشفير المتماثل: (symétrique) وهو التشفير الذي يستخدم فيه صاحب الرسالة المفتاح الخاص ذاته لإنشاء التوقيع ولفكه بعد الاتفاق المسبق مع المرسل إليه على كلمة السر بينهما، وغالبا ما يعتمد فيه على شفرة القيصر (chiffre de césar) التي تقوم على أساس استبدال النص بأحرف تقابله وهذا بإتباع عدة مراحل للوصول إلى النص المشفر. ولابد أن تكون اللغة والخوارزمية المعتمدة معروفة وهذا لسهولة فك التشفير، ويكون تشفير الرسالة هو في حد ذاته كلمة السر الناتجة عن تحويل حروف أو أرقام أو رموز إلى عدد ثنائي وإضافة رموز أخرى لها.

مثال: إذا أراد شخص أن يرسل نصا إلى شخص آخر، فعليه إرفاق الرسالة بمفتاح وجدول للرموز إضافة إلى تحديد العدد الأقصى للرموز المستعملة module فإذا استعمل أحرف اللغة العربية فتكون القيمة هي28 إذن نستعمل 28 module وهذا لكي لا نتحصل حين تشفير الرسالة أو فكها على قيمة تجاوز عدد الأحرف المستعملة والتي لا يكون لها حرف يقابلها،

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368

1: لتشفير النص الأصلي وفق خوارزمية القيصر: يقوم المرسل بكتابة الرسالة وإتباع الخطوات التالية باستعمال module**28** من اجل الحصول على خارج القسمة، الذي يطرح مجموع النص الأصلي مع كلمة السر لكي لا تتجاوز النص المشفر قيمة (ي) في الرموز الذي يقابله العدد 28 فالمعادلة وفق خوارزمية القيصر تكون كالتالي:

تشفير النص Cr (T) = (النص T+ مفتاح C) module 28

Cr (T) Cryptage d'un texte = (T texte+ C clé) module 28

مثال تطبيقي عن التشفير الإلكتروني

الرسالة: نلتقي غدا

المفتاح : 10

تشفير النص Cr (T) = (النص T+ مفتاح C) modulo 28

28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
ي	و	ه	ن	م	ل	ك	ق	ف	غ	ع	ظ	ط	ض	ص	ش	س	ز	ر	ذ	د	خ	ح	ج	ث	ت	ب	أ

أولا : تشفير النص الأصلي									
النص T:	ن(25)	ل(23)	ت(3)	ق(21)	ي(28)	غ(19)	ذ(9)	ا(1)	النص الاصلي بعد تحويله الى رموز
(النص T+ مفتاح C)	35	33	13	31	38	29	19	11	نضيف الرمز المقابل للنص الاصلي الى المفتاح وهو 10
modulo 28	7	5	13	3	10	1	19	11	نقوم بطرح 28 من كل عدد يتجاوزه، اما الاعداد الاصغر من 28 فتبقى كما هي.
النص المشفر Cr (T)	خ	ج	ش	ت	ر	ا	غ	ز	نقوم بتحويل الرموز الى الرقم المقابل لها في الجدول

بعد التشفير سيستقبل المرسل إليه النص المشفر التالي: "خ ج ش ت ر ا غ ز كما ه".

ثانيا: فك التشفير تطبق الخوارزمية العكسية على النحو التالي:

فـك التشـفير $Dc(C)$ =(النص المشـفرCr -المفتـاحC) =module28 Tالـنص الأصلي

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368

Dc(C)=(26+Cr-C)module28=T Décrypter d'un *texte*

(وفق جدول فك التشفير التالي)

فك التشفير Dc (C) =(النص المشفر Cr -المفتاح C) module 28 = Tالنص الاصلي
Décrypter d'un texte Dc (C) = (26+ Cr -C) module 28 = T

ثانيا : فك تشفير النص									
النص المشفر Cr	خ (7)	ج (5)	ش (13)	ت(3)	ر(10)	ا(1)	غ(19)	ز(11)	النص المشفر بعد تحويله إلى رموز
28+النص المشفر Cr	35	33	41	31	38	29	47	39	نضيف الرمز المقابل للنص المشفر إلى المفتاح وهو 10
(28+النص المشفر Cr)- المفتاح C	25	23	31	21	28	19	37	29	نطرح المفتاح من القيمة المحصل عليها من إضافة الرمز المقابل للنص المشفر إلى المفتاح
modulo 28	25	23	3	21	28	19	9	1	نقوم بطرح 28 من كل عدد يتجاوزه، اما الاعداد الاصغر من 28 فتبقى كما هي.
النص الأصلي	ن	ل	ت	ق	ي	غ	ذ	ا	نقوم بتحويل الرموز الى الرقم المقابل لها في الجدول

وبعد عملية فك التشفير سيتحصل المرسل إليه على النص التالي:

"ن ل ت ق ي غ ذ ا" = **نلتقي غدا** *وهذا هو النص الأصلي الذي كتبه أحمد.*

غير أن هذه النوع من التشفير يشكلا خطرا على المعاملات القانونية لاسيما في مسألة تبادل المفتاح السري الخاص الأمر الذي أدى إلى تراجعه وظهور التشفير اللامتماثل.

ب- طريقة التشفير اللامتماثل: (asymétrique) يستعمل في التشفير اللامتماثل مفتاحين مفتاح عام ومفتاح خاص المفتاح الخاص الذي يملكه شخص واحد يستخدم لتشفير الرسالة وفك شفرتها ، أما المفتاح العام الذي يفك شفرة الرسالة التي شفرها المفتاح الخاص، يمكن أن يستخدم في تشفير رسائل مالك المفتاح الخاص لكن لا يمكن للمفتاح العام أن يفك شفرة رسالة مشفرة بالمفتاح العام، ويستند التشفير اللامتماثل على إرسال الرسالة المشفرة بالمفتاح الخاص إلى المرسل إليه مرفقة بالمفتاح

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368

العام، من خلال هذا الأخير يتم التحقق من هوية الموقع وتشفير الرسالة المرسلة[6]، وهذا باستخدام برامج حاسوبية متخصصة[7].

وتجب الإشارة أن المرسل إليه إذا أراد أن يرد على الرسالة أن يكتب النص ويشفره باستخدام المفتاح العام للمرسل والذي لا يمكن لحاملي هذا المفتاح فك تشفيرها إلا بالمفتاح الخاص.

ثالثا: المزج بين التشفير المتماثل والتشفير اللامتماثل: يمكن للمرسل والمرسل إليه أن يستخدما كلا النظامين في التشفير وهذا بتشفير الرسالة المرسلة بمفتاح متماثل (المفتاح السري) ثم بعدها يتم تشفير المفتاح المتماثل بالمفتاح العام للشخص المرسل إليه الرسالة ويرسل المفتاح المشفر والرسالة المشفرة إلى المرسل إليه الذي يقوم بفك شفرة المفتاح بمفتاحه الخاص ليتحصل على المفتاح السري الذي شفرت به الرسالة الأصلية.[8] فتشفر الرسالة بالمفتاحين عبر عدة مراحل:

1- كتابة النص الأصلي وتشفيره بالمفتاح العام للمرسل إليه، حتى لا يتمكن لأي شخص آخر فك تشفيرها من غيره.

2- تشفر ذات الرسالة مرة أخرى باستخدام المفتاح الخاص للمرسل وهذا بغرض التأكد من مرسلها وقابلية فكها باستخدام المفتاح العام للمرسل.

3- إرسال الرسالة إلى المرسل إليه عبر الوسائل الالكترونية.

4- وصول الرسالة إلى المرسل إليه المشفرة بالمفتاح المتماثل والمفتاح المتماثل المشفر بالمفتاح العام للمرسل إليه.

5- يقوم المرسل إليه بفك تشفير باستخدام المفتاح العام للمرسل فيتحصل على رسالة مشفرة بمفتاحه العام فيقوم بفكها باستخدام المفتاح السري الخاص به الذي يكون معلوما لديه.[9]

وتعتبر هذه الطريقة أكثرها أمانا نظرا لدورها الفعال في تحقيق سرية الرسالة وإمكانية التحقق من صاحبها، نظرا لان فك الرسالة يحتاج للمفتاح الخاص للمرسل إليه حتى بعد فك تشفيرها بالمفتاح العام للمرسل.

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368

المحور الثاني: مدى فعالية التوقيع الرقمي في توثيق العقد الإلكتروني

أولا: فعالية التوقيع الرقمي من حيث إجراءاته الرسمية.

إن ارتباط التوقيع الرقمي بتقنيات التشفير الإلكتروني بمختلف أنواعه يحمي المحرر الإلكتروني من العبث به، لكن ونظرا لتطور برامج الهاكرز والقرصنة الإلكترونية أصبح بالإمكان اختراق الرسائل والمعاملات المشفرة نظرا لقدراتهم وخبراتهم العالية في هذا المجال، لذا كان لابد من إحاطة عمليات التشفير الإلكتروني بإجراءات رسمية تضمن خصوصية المعاملات القانونية وأطراف التعاقد.

1- ارتباط عملية التوقيع الرقمي بهيئات رسمية:

يرتبط التوقيع الإلكتروني بهيئات رسمية تتعلق "بجهات التوثيق الإلكتروني" والتي تشكل الطرق الثالث في العلاقة القانونية تعمل كوسيط بين المتعاملين في المعاملات الإلكترونية، وقد عرفه قانون الاونسترال النموذجي قد انه" **شخصا يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية**"[10].

وقد عرفته المادة 12/2 من القانون 15-04 على أنه: "شخص طبيعي أومعنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني"، فيقوم بمنح شهادات التصديق الإلكتروني إلى أصحابها بناءا على طلبه وبعد التأكد من صحة وتكامل بيانات الإنشاء مع بيانات التحقق من التوقيع والتحقق من معلوماته الشخصية وهويته[11]، إما عبر إرسال المستندات الإثباتية بالبريد أو الإنترنت أو بالهاتف.

وفي إطار ذلك تعمل جهات التصديق على التنسيق بين عمليتي إنشاء التوقيع الإلكتروني والتدقيق في هذا التوقيع، من خلال البيانات والرموز والأنظمة المعلوماتية المستعملة بغرض وضع التوقيع والتأكد منه فمن حيث البيانات فلها دور في تقديم الرموز ومفاتيح التشفير لاسيما الشفرة الخاصة من أجل إنشاء التوقيع وتوظيف تلك البيانات والرموز لاسيما الشفرة العامة في التحقق من صحة التوقيع الإلكتروني[12]،

2- الاعتماد على شهادة التصديق الإلكتروني في عملية التوقيع الرقمي:

شهادة التصديق الإلكتروني عبارة عن وثيقة إلكترونية تعدها السلطة المختصة المخول لها ذلك، يثبت من خلالها الصلة بين بيانات التحقق من التوقيع الإلكتروني

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368

والموقع، تقدم إلى شخص طبيعي أو معنوي بواسطة مؤدي خدمات التصديق الإلكتروني. تتضمن هذه الشهادة أساسا ما يثبت أنها ممنوحة على أساس أنها شهادة تصديق إلكترونية، وهي بطاقة لها رمز تعريفي نظرا لخصوصيتها وتحديد صلاحيتها بمدة بداية ونهاية، وتحديد السلطة التي منحت الشهادة وكذا البلد المقيم به، إلى جانب معلومات الموقع وصفته الخاصة عند الاقتضاء[13]، فبمجرد حصول الشخص على شهادة التصديق فيتم نشر مفتاحه العام على الانترنت الذي يكون له نسخة منه داخل الشهادة الى جانب المفتاح الخاص ويسلم هذا الأخير في وسيلة آمنة يتم حفظه برقم سري خاص فقط بالمستخدم.

ولكي يعتد بشهادة التصديق الإلكتروني لابد ان تكون صادرة عن جهات رسمية مختصة، إضافة إلى تأكيد صحتها بتأكيد صحة مصداقية البيانات الوارد فيها مع أهلية ذوي الشأن[14].

وتنقسم شهادات التصديق الإلكترونية إلى شهادات عادية وشهادات موصوفة، فشهادة التصديق الالكتروني البسيطة فهي وثيقة تنسق بين عملية التوقيع الإلكتروني والموقع وفق ماجاء به قانون التوجيه الأوروبي رقم 99-93 المؤرخ في 13 ديسمبر 1999 المتعلق بالتوقيعات الإلكترونية الذي عرفها على أنها: "بيانات في شكل إلكتروني تربط أو تتصل منطقيا ببيانات إلكترونية أخرى" من خلال يتم اثبات صلة التوقيع الإلكتروني للموقع[15].

أما شهادة التصديق الإلكترونية الموصوفة فهي تتميز بمتطلبات حددتها المادة 15 من القانون 15-04، أهمها صدورها من قبل طرف ثالث موثوق أو من قبل مؤدي خدمات تصديق إلكتروني، طبقا لسياسة التصديق الإلكتروني الموافق عليها، وان تمنح للموقع دن سواه إضافة إلى تضمنها على البيانات القانونية الواجب توافرها في شهادات التصديق حسب المادة 15 من القانون المذكور أعلاه، على غرار البيانات الواجب أن تتضمنها لاسيما تأكيد صلاحية الشهادة للاستخدام بتحديد مدة بدايتها ونهايتها، كما تبين هوية صاحبها واسمه وصحة بياناتها، بذكر اسم وعنوان الجهة التي أصدرت الشهادة ومكانها وخصوصية البطاقة باشتمالها على رمز تعريفي لصاحبها، أما من حيث التوقيع فهي تتضمن مفاتيح التشفير العمومي والخاص وبيانات

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368

متعلقة بالتحقق من التوقيع الإلكتروني التي تتوافق مع بيانات إنشاء التوقيع، والتوقيع الرقمي للجهة المصدرة للشهادة على التوقيع الإلكتروني لتأكيد صحة كل من التوقيع والهوية والرسالة. وأهم ما يمكن أن تتضمنه الشهادة هو الموقع الإلكتروني (web site) الذي يعرض فيه قائمة الشهادات الموقوفة أو الملغاة.(16)

ويشترط في شهادة التصديق أن تكون صادرة عن جهة رسمية مرخص لها داخل الدولة، أما بخصوص الشهادات الصادرة عن جهات تابعة لدول أخرى فالمشرع الجزائري اعترف بها على شرط أن تكون تلك الجهات مرخص لها في دولتها بمنح تلك التراخيص.(17)

3- مفاتيح التشفير: يشكل مفتاح التشفير الوسيلة الأساسية لتوقيع المحررات الإلكترونية، والذي ينقسم إلى مفتاح تشفير عمومي ومفتاح خاص.

أ- مفتاح التشفير العمومي: عرفته المادة 9/02 من القانون 15-04 على أنه: "سلسة من الأعداد تكون موصوفة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني، وتدرج في شهادة التصديق الإلكتروني"، ومن اجل إرسال رسالة مشفرة إلى شخص ما عبر بريده الالكتروني لابد من الحصول على الشهادة الرقمية لذلك الشخص واستخدام المفتاح العام المخزن بها لتشفير الرسالة المرسلة إليه(18).

ب- **مفتاح التشفير الخاص:** هو "عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الإلكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي."(19) كما يستخدم أيضا لفك تشفير الرسالة المرسلة لصاحب المفتاح(20)، وباعتبار أن المفتاح العام مصادق عليه من طرف سلطة رسمية معتمدة فهو يعتبر كوسيلة للتأكد من مطابقة التوقيع لمرسل الرسالة(21)، وتتم عملية تبادل مفاتيح التشفير عبر عدة وسائل لكن أفضلها أن يتم تخزينه على قرص مرن ويتم تسليمه يدويا.

3- برمجيات التشفير: وهي الآليات المعدة لإعداد التوقيع الإلكتروني تكون عبارة عن جهاز وبرامج إلكترونية معلوماتية تستعمل خصيصا إما لتطبيق بيانات إنشاء التوقيع الإلكتروني أو تطبيق بيانات للتحقق من الصلة بين التوقيع الإلكتروني والموقع، ويلزم أن تكون برامج التشفير سريعة نظرا للتزامن بين الجلستين، وقد

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368

عرفت شركة IBM باختصاصها في تطوير نظام التشفير الإلكتروني والذي شهد انتشارا واسعا في السوق لما يتميز به لضمان حماية مفاتيح التشفير الذي يصل طوله إلى حوالي 128 بت Bits وهذا ما يحقق قوة التشفير الإلكتروني[22].

ثانيا: فعالية التوقيع الرقمي من حيث توثيق المحرر الإلكتروني.

إن المحرر الالكتروني شانه شان المحرر الكتابي في إثبات ما ورد فيه فبالرجوع إلى المادة 323 مكرر1 من القانون المدني والتي جاء فيها: "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها"[23].

1- توثيق مضمون العقد: من خلال خاصية التوقيع الإلكتروني على المحررات الإلكترونية فهي تضيف عليها طابع السرية نظرا إلى اعتبار أن ما دون بداخلها خاضع لتقنيات التشفير التي تجعل النص سريا ومضمونا لا يمكن الإطلاع عليه إلا من أطراف التعامل لاسيما إذا كان التشفير باستعمال المفتاح السري. هذا وتجب الإشارة إلى أن التوقيع الإلكتروني يمكن من التعرف على الشخص مرسل الرسالة وأنها صادرة بإرادته ولا يمكنه بذلك إنكار ماورد منه،

2- توثيق أهلية وإرادة أطراف التعاقد: يعتبر التوقيع الرقمي ميزة شخصية تعكس معلومات وبيانات الموقع من خلال توقيعه للعقد المبرم إلكترونيا، ومن خلاله يمكن الكشف عن اسمه ولقبه وتوقيعه من خلال الرموز أو الأرقام الخاصة المستخدمة في التشفير والمنظمة في شهادات التصديق الإلكترونية، فهو بذلك يعبر عن شخصية الموقع وهويته، ما يترتب عنه صعوبة تزوير أو تقليد أو استعمال التوقيع الرقمي من غيره الموقع، ومن خلال توقيع السند الإلكتروني بتقنيات التشفير بواسطة الدعامة الإلكترونية فيتم إبرام العقد والذي هو حجة على إرادة وموافقة الموقع على ما ورد في السند من التزامات وحقوق الأمر الذي لا يمكن معه إنكار إرادته في ذلك، وثبوتا لحضوره الشخصي وقت إدخال الرقم السري، وبالرجوع إلى القانون 04/15 فقد جاء فيه أن "الموقع هو شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني ويتصرف

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368

لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله"[24]، ويرتبط التوقيع الرقمي بالموقع نفسه ولا يمكن استخدام مفتاحه الخاص من قبل الغير.

ومن أجل ذلك قد حدد القانون النموذجي للتوقيع الإلكتروني ضوابط لأطراف التعاقد الإلكتروني في استخدام التوقيع الإلكتروني، فمن حيث الموقع عليه أن يستخدم توقيعه في الحدود المسموح بها قانون وفي حالة تعرض بيانات إنشاء توقيعه لما يثير الشبهة عليه أن يقوم بإخطار بذلك.وقبل ذلك كله لابد أن تكون البيانات الشخصية الصادرة في بطاقة التصديق الإلكترونية صحيحة، وأي إخلال منه يترتب عليه المسؤولية المدنية.

أما من جانب المرسل إليه فله التأكد من صحة وموثوقية التوقيع الإلكتروني والتأكد من مصدر الرسالة وصلاحية شهادة تصديقه في إنشاء التوقيع وأنها سارية المفعول وأن يبذل جهده في التأكد من هوية مرسل الرسالة وفي حالة عدم قيامه بذلك فيتحمل تبعة الأضرار الناجمة عن ذلك[25].

4- **مدى تحقيق التوقيع الإلكتروني لمزايا التوقيع العادي:** لكي يتم الاعتراف والأخذ بالتوقيع الإلكتروني لابد أن تتوافر فيه وظائف وخصائص التوقيع على الورق من تحديد لهوية الموقع والتعبير عن إرادته على نحو يثبت الصلة بين الموقع والتوقيع ويكون التوقيع التقليدي على شكل إمضاء[26]، ختم أو بصمة وينفرد التوقيع الكتروني من جهته بعدة صور وأشكال أهمها التوقيع الرقمي، فقد اشترط المشرع الجزائري للأخذ بالعقود سواء أكانت رسمية أم عرفية أن تكون موقعة، ويعتبر التوقيع بمثابة شكلية أساسية ضرورية لإثبات صحة ما ورد في المحرر وليكون حجة على من وقعه ولا يمكن إنكاره، ويختلف التوقيع على المحررات الورقية بحسب نوع المحرر فإذا كان رسميا فيجب أن يكون تحت إشراف ضابط عمومي والأطراف والشهود عند الاقتضاء[27]، وهذا ما جاءت به المادة 324 مكرر2 من القانون المدني: "توقع العقود الرسمية من قبل الأطراف والشهود عند الاقتضاء، ويؤشر الضابط العمومي على ذلك في آخر العقد، أما العقود العرفية فلا تكون ذات حجة إلا إذا كانت موقعة وتحتوي على تاريخ ثابت.

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368

ولقد اعتد المشرع الجزائري بالتوقيع الإلكتروني في إثبات العقد بنفس شروط توقيع المحرر العرفي وجاء بذلك في الفقرة الثانية من المادة 327 من القانون المدني[28]: "ويعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر أعلاه"، فمتى كانت التوقيع الإلكتروني سليما وأمكن من خلاله التعرف على هوية صاحبه وكان محفوظا في ظروف تضمن سلامته فيعتبر التوقيع الإلكتروني كالتوقيع على الورق هو نفس ما جاءت به المادة 1316 من القانون المدني الفرنسي[29].

وتجب الإشارة إلى أن التوقيع الإلكتروني الذي يعادل في قوته الثبوتية قوة التوقيع العادي هو التوقيع الموصوف سواء كان شخصا طبيعيا أو معنويا وهذا ماجاءت به المادة 08 من القانون 15-04 بقولها: "يعتبر التوقيع الإلكتروني الموصوف وحده مماثلا للتوقيع المكتوب، سواء كان لشخص طبيعي أو معنوي". فيشترط في التوقيع أن يكون قد نشأ بناءا على شهادة تصديق إلكتروني موصوفة، وأن يكون بالإمكان التأكد من تحديد هوية الموقع، ومصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني، وأن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع إضافة إلى أن يكون مرتبطا بالبيانات الخاصة به بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات[30].

ومع ذلك فإنه قد أكدت المادة 9 من القانون 15-04على فعالية التوقيع الإلكترونية باعتباره كدليل إثبات أمام القضاء وهذا بنصها: "بغض النظر عن أحكام المادة 08 أعلاه، لا يمكن تجريد التوقيع الإلكتروني من فعاليته القانونية أو رفضه كدليل أمام القضاء بسبب: 1- شكله الإلكتروني، أو،

2- أنه لا يعتمد على شهادة تصديق إلكتروني موصوفة، أو،

3- أنه لم يتم إنشاؤه بواسطة آلية مؤمنة لإنشاء التوقيع الإلكتروني".

خاتمة:

إن التوقيع الرقمي باعتباره صورة من صور التوقيع الالكتروني يعد طريقا آمنا لحماية المعاملات القانونية المبرمة عبر الشبكة العنكبوتية، كما انه يعد وسيلة لإثبات التصرف ومصدر التصرف فهو يتم بمعية جهة التصديق المصدرة لشهادة التصديق الالكترونية المستخدمة في التوقيع الالكتروني، ويُمكن مستقبل الرسالة

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368

من التحقق من هوية مرسل الرسالة باستخدام مفاتيح التشفير وهو بذلك يعد وسيلة اضمن تهدف لمواكبة التطورات التكنولوجية في مجال إبرام التصرفات القانونية، ما يفرض من الناحية العملية تعميم استعمال شهادات التصديق الالكترونية لسهولة إبرام التصرفات القانونية على وجه يضمن حمايتها وحماية مصالح الأطراف المتعاملة، ومن هذا المنطلق فيمكن اعتماد آليات التوقيع الرقمي كضمان أوفر وأسرع في سبيل حماية المعاملات القانونية وهذا بالنظر إلى خصائصه القانونية والفنية الفعالة.

الهوامش:

(1)- المادة 02 من القانون 15- 04 المؤرخ في 2015/02/01 المتعلق بالتوقيع والتصديق الإلكترونيين.

(2)- M. Guével , LE DEVELOPPEMENT DE LA SIGNATURE ELECTRONIQUE. Master2 recherche droit des affaires. Université Paris3 Nord.2010- 2011. p16.

(3)- طلال حسن أمين، الأرقم قاسم، مأمون عادل مأمون، محمد عبد المنعم، احمد على محمد، التوقيع الالكتروني، تقرير في مقرر أمن المعلومات والشبكات كلية العلوم والتقنيات جامعة أم درمان الإسلامية. ص12.

(4)- عرف القانون 15- 04 آلية التحقق من التوقيع الإلكتروني على أنها: "جهاز أو برنامج معلوماتي معد لتطبيق بيانات التحقق من التوقيع الإلكتروني".

(5)- عبد الرسول عبد الرضا، محمد جعفر هادي، المفهوم القانوني للتوقيع الإلكتروني. مجلة المحقق الحلي للعلوم القانونية والسياسية. العدد الأول، السنة الرابعة. ص 148.

(6)- ممدوح محمد على مبروك، مدى حجية التوقيع الالكتروني في الإثبات. القاهرة مصر دار النهضة العربية. 2005. ص 18.

(7)- عبد العزيز المرسي حمود، مدى حجية المحرر الالكتروني في الإثبات في المسائل المدنية والتجارية في ضوء قواعد الإثبات النافذة. جامعة المنوفية 2005. ص ص 39- 40.

(8)- إبراهيم سليمان عبد الله، امن المعلومات الجزء الأول. مقال على شبكة الانترنت اضطلع عليه بتاريخ 2015/07/25. موقع: www.kau.edu.sa/iabdullah

(9)- الأنصاري حسن النيداني، القاضي والوسائل الالكترونية الحديثة. دار الجامعة الجديدة. الإسكندرية 2009.ص ص 20- 21.

(10)- المادة 02/هـ من القانون النموذجي بشأن التوقيعات الالكترونية الذي وضعته لجنة الأمم المتحدة للقانون التجاري الدولي (الأونيسترال) 2001.

(11)- المادة 44 من القانون 15- 04 السالف الذكر

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368

(12)- زهيرة كيسي، النظام القانوني لجهات التوثيق (التصديق) الإلكتروني.مجلة دفاتر السياسة والقانون، العدد السابع/جوان 2012. ص216.

(13)- المادة 15 من القانون 15- 04 المؤرخ في 2015/02/01 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

(14)- عبير ميخائيل الصفدي الطوال، النظام القانوني لجهات توثيق التوقيع الإلكتروني.عمان، الأردن. دار وائل للنشر، الطبعة الأولى 2010.. ص 95.

(15)- إقلولي ولد رابح صافية، القوة الثبوتية لشهادات التصديق الالكتروني في التشريع المقارن. مداخلة في الملتقى الوطني حول: الإطار القانوني للتوقيع والتصديق الإلكترونيين في الجزائر، المنظم بجامعة سوق اهراس يومي 16- 17 فيفري 2016.

(16)- عبير ميخائيل الصفدي الطوال، المرجع السابق. ص ص 101 إلى 105.

(17)- صالح أوعيسى سكوتي، التوقيع الإلكتروني بين الاستقلالية والانتقاء، دراسة مقارنة بين التشريع الجزائري والأردني. مداخلة ضمن الملتقى الوطني حول " الإطار القانوني للتوقيع والتصديق الالكترونيين في الجزائر. يومي 16و 17 فيفري 2016 بجامعة سوق أهراس، الجزائر. ص 21.

(18)- فهد الحويماني، مدير المركز الوطني للتصديق الرقمي، حياتك أسرارها في مفتاح. مجلة عالم موبايلي. العدد7 يوليو 2010 ص 13.

(19)- المادة 08/02 من القانون 15- 04 السالف الذكر

(20)- ممدوح محمد على مبروك، المرجع السابق، ص18.

(21)- فهد الحويماني، المرجع السابق ص 13.

(22)- بلال بن جامع، المشكلات الأخلاقية والقانونية المثارة حول شبكة الإنترنت. مذكرة مقدمة لنيل شهادة الماجستير في علم المكتبات، تخصص إعلام علمي وتقني. كلية العلوم الإنسانية والعلوم الاجتماعية، جامعة منتوري، قسنطينة 2005- 2006. ص 150.

(23)- القانون رقم 05- 10 مؤرخ في 20 يونيو 2005، المتضمن القانون المدني.

(24)- المادة 02/02 من القانون 04/15 السالف الذكر .

(25)- عبد الرسول عبد الرضا، محمد جعفر هادي، المفهوم القانوني للتوقيع الإلكتروني. المرجع السابق. ص 154.

(26)- غازي أبو عرابي، فياض القضاة. حجية التوقيع الإلكتروني، دراسة في التشريع الاردني. مجلة جامعة دمشق للعلوم الاقتصادية والقانونية. المجلد 30، العدد الأول 2004. ص 173.

(27)- المادة 29 من القانون 06- 02 المؤرخ في 20 فيفري 2006 المتضمن مهنة الموثق.

(28)- قانون 05- 10 المؤرخ في 20 يونيو 2005 المعدل للقانون المدني الجزائري .

(29)- Article 1316- 1 Créé par loi n o 2000- 230 du 13 mars 2000- art .1 JORAF 14 mars 2000 Abrogé par ordonnance no 2016- 131 du 10 février 2016 art.3 « L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368

papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité».

(30)- المادة 07 من القانون 15- 04 السالف الذكر.

ISSN: 2352-975X– http://elbahith.univ-batna.dz – EISSN: 2588-2368