

الحماية القانونية لتأمين التوقيع الالكتروني في الصفقات العمومية في الجزائر

Legal protection of insurance electronic signature in public transactions in Algeria

د/خير الدين فايزة

كلية الحقوق – جامعة الجزائر

Khiredine.faiza@yahoo.com

تاريخ الإرسال: 2020/01/30 تاريخ القبول: 2020/06/09 تاريخ النشر: 2020/06/15

المخلص:

فرضت البيئة الالكترونية على المعاملات المدنية والتجارية وحتى الإدارية مصطلحات جديدة ذات طبيعة خاصة، فبعدما كانت تعرف التوقيع التقليدي فيها أصبحت اليوم تعرف ما يسمى التوقيع الالكتروني على مختلف العقود والمعاملات إذا تمت عبر وسائل الاتصال الحديثة والتواجد الافتراضي على شبكة الانترنت، وحتى تكون نافذة في حق المتعاقدين لبد من التوقيع عليها إلكترونيا، لهذا سعت مختلف التشريعات على تنظيمه وإقرار المبادئ الأساسية حتى تكون لهذه المحررات الالكترونية قوة ثبوتية مع المحررات الورقية، خاصة مع انتشاره الواسع فلبد من حمايته حتى يدعم ثقة التعامل به، خاصة وأن التوقيع يهدف بصفة عامة إلى استقرار المراكز القانونية للأفراد وحماية حقوقهم المكتسبة، لأنه من أهم الأسس التي تقوم عليها التصرفات القانونية، خاصة الصفقات العمومية.

الكلمات المفتاحية: التوقيع الالكتروني، التفسير الالكتروني، الحماية الالكترونية، آليات حماية التوقيع الالكتروني، المصادقة الالكترونية.

Abstract:

The electronic environment imposed on civil, commercial and even administrative transactions new terms of a special nature, after it the traditional signature in it, today it knows what is called the electronic signature on the various contracts and transactions if it is done through modern means of communication and virtual presence on the internet, and in order to be effective in the right of the contractors, it must be signed electronically. This is why various legislations sought to regulate it and approve the basic principles so that these electronic edition have a strong force with its spread. White vilbd of protection so that it supports the confidence of dealing, because it is the most important foundation of legal action, especially public transactions.

Keywords: electronic signature, electronic authentication, electronic signature protection, electronic signature protection mechanisms.

مقدمة:

ساهمت وسائل الاتصال الحديثة في نزع الصفة المادية للصفقة العمومية، بعدما أصبحت تتم بطريقة الكترونية بواسطة البوابة الالكترونية للصفقات العمومية، فأصبح التوقيع الالكتروني مظهر من مظاهر التطور التكنولوجي الذي يتماشى وطبيعة التعاملات التي تتم في الفضاء الرقمي خاصة لما يضيفه من ثقة على المتعاملين في قدرته على التحديد الدقيق لهوية الشخص والتعبير عن إرادته في الوسط الالكتروني¹.

وإستيفاء لمتطلبات الحماية² أقر المشرع الجزائري³ آليات تقنية وقانونية لحماية التوقيع الالكتروني في المعاملات المدنية بصفة عامة والصفقات العمومية بصفة خاصة، من خلال القانون رقم 04-15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين لتعزيز الثقة لدى المتعاملين به، من مخاطر التجارة واستقرار الدور الوظيفي المنوط بها من أي اختراق أو تحايل إلكتروني، وذلك من خلال إقرار عملية التشفير كإجراء تقني لحماية البيانات الالكترونية، وكذا العمل على تنظيم مهام جهة التوثيق الالكتروني وتجسيد مسؤوليتها قصد تحقيق الأمان القانوني للمتعاملين في المجال الالكتروني خاصة بالنسبة للعقود الإدارية – صفقات العمومية⁴.

ومن أجل التطرق لهذا الموضوع ارتأينا للطرح الإشكالية التالية: **كيف ساهمت المنظومة القانونية في وضع آلياتها من أجل حماية التوقيع الالكتروني على الصفقات العمومية؟**

وللإجابة على هذه الإشكالية قسمنا موضوعنا إلى ثلاث مباحث متتالية:

المبحث الأول: التشفير كآلية للحماية التوقيع الالكتروني على الصفقات العمومية

نظرا لأهمية التوقيع الالكتروني وسرعة انتشاره بات من الضروري إيجاد آليات قانونية من أجل حمايته من التزوير والتعدي على محتواه في التعامل به خاصة في الصفقات العمومية لأنه يعد كآلية من الآليات لحمايته.

المطلب الأول: مفهوم التشفير

¹ - المرسوم الرئاسي 10-236 المؤرخ في 2010/10/07 يتضمن تنظيم الصفقات العمومية، الجريدة الرسمية رقم 58 لسنة 2010/10/07 المعدل بالمرسوم الرئاسي 15/247 المؤرخ في 16 ديسمبر 2015 المتضمن الصفقات العمومية وتفويضات المرفق العام، الجريدة الرسمية العدد 50 المؤرخة في 20 سبتمبر 2015.

² - O.Moreteau, L'estoppel Et La Protection De La Cofinance Légitime, Thèse Université Jean Moulim, Lyon Iii, 1990.P24.

³ - يعد المرسوم 10-236 المؤرخ في 2010/10/07 الجريدة الرسمية رقم 58 لسنة 2010/10/07 كأول بادرة للتعامل الالكتروني من خلال المادتين 174 و173 والقرار الوزاري الصادر في 17 نوفمبر 2013 المتعلق بالبوابة الالكترونية للصفقات العمومية، وبعدها التنظيم رقم 15-247 المتعلق بالصفقات العمومية وتفويضات المرفق العام أين فرضت ظاهرة العولمة والتطور التكنولوجي على العقود الإدارية وبالأخص الصفقات العمومية التعاقد بوسائط الكترونية.

⁴ - فايزة خير الدين، استحداث المعاملات الالكترونية كمبدأ للمبدأ الشفافية في عملية إبرام الصفقات العمومية في الجزائر، مجلة قضايا معرفية، جامعة الجلفة، الجزائر، المجلد الأول، العدد الثالث، جوان 2019، ص24 وما يليها.

تسعى مختلف الأنظمة القانونية الالكترونية¹ لآلية التشفير حتى تضمن سلامة المعلومات الالكترونية عن طريق الرسائل المعتمدة للسيطرة على كافة أنواع ومصادر التعدي عليها، مثل التلف والضياع والاستخدام غير قانوني وهذا حماية للتأمين كافة الموارد المستخدمة في معالجة المعلومات الالكترونية².

فأغلب الدول المتقدمة في التعامل الالكتروني التي اعتمدت على التشفير كأفضل تقنية لحماية البيانات والمعلومات والصفقات المرسله عبر الشبكات المفتوحة من أي تعديل أو تعبير غير مرغوب فيه³ لضمان سريتها من أي اختراق لها، وتتصدر تقنيات التشفير⁴ الوسائل والأدوات المبتكرة في مجال توفير الأمن وسلامة وسرية المعلومات خاصة في مجال الصفقات العمومية.

ونتيجة للتطور المعاملات عرفت المادة 27 من قانون 90/1170 تعديلا آخر في 18 يونيو 2001 يقضي "بإجازة تصدير وسائل التشفير التي تؤمن وظيفة السرية لرسالة المعلوماتية"، ومن أشهر التوصيات أقرها البرلمان الأوروبي بتاريخ 2000/06/22 التي ترمي إلى إلغاء القيود القائمة على تبادل تقنيات ومنتجات التشفير فيما بين الدول الأوروبية الأعضاء⁵.

فالتشفير يقوم بدور مهم لأنه يحول المعلومات إلى رموز غير مفهومة من العامة، بحيث لا يستطيع الأشخاص غير المرخص لهم الاطلاع على المعلومات أو فهمها، وتتم إعادة تحويل المعلومات إلى صياغتها الأصلية، باستخدام المفتاح المناسب للفك الشفرة، وهذا ما يضمن سرية التوقيع الالكتروني، ويوفر الوسيلة لضمان الثقة والأمان للمعلومات عبر شبكة الانترنت⁶.

¹ - نهلة عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، عمان، الأردن، الطبعة الثانية، 2010، ص 46.
- أشرف السعيد أحمد، القرصنة الالكترونية، مطابع الشرطة، القاهرة، 2013، ص 12.
- بشرى حسن الحمداني، القرصنة الالكترونية أسلحة الحرب الحديثة، دار أسامة، عمان، الأردن، الطبعة الأولى، 2014، ص 13.

² - خالد مصطفى فهمي، النظام القانوني للتوقيع الالكتروني في ضوء التشريعات العربية والاتفاقيات الدولية، دار الجامعة الجديدة، 2007، ص 100 وما يليها.

- محمد دباس الحميد، حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، الأردن، 2007، ص 34.
- فيصل سعيد الغريب، التوقيع الالكتروني وحجته في الإثبات، المنظمة العربية للتنمية الإدارية، 2005، ص 240.
- Jeffrey F, Rayport Et Jaurorski Bernard, commerce electronique (traduit de l'américain port) francine nézina, johanne champoux et elisabeth rochette, edition cheneliere/ mcgram-hill, montréal – toronto, 2003, p. 56.

³ - Dimitriou Philippe, « l'application du droit de la cryptologie en matière de sécurité des réseaux informatique » d.e. afac des sciences juridique, politiques et sociales, ecole doctorale n°74, université de lille, 2002, p:9.

⁴ - خالد إبراهيم ممدوح، إبرام العقد الالكتروني، دار الفكر الجامعي، الإسكندرية، 2006، ص 199.
⁵ - « Toutes prestations visant a transformer a l'aide de convention secrets des information ou signaux claires en information ou signaux inintelligibles ou a réaliser l'opération inverse grâce a des moyens matériels ou logiciels conçus a cet effet »

⁶ - أشرف السعيد أحمد، المرجع السابق، ص 160.
- حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية، 2000، ص 45.

وحتى يقوم التشفير بمهامه لبد من مفاتيح تعد كأدوات الكترونية، من أجل حماية التوقيع الالكتروني نجد منها **مفتاح التشفير العام**، ومفتاح التشفير الخاص ومفتاح التشفير الجذري التي تسهل في التحقق من شخصية المحرر الالكتروني وسلامة التوقيع الالكتروني¹.

ونفس الأحكام تبناها المشرع الجزائري من خلال قانون 04-15 في مادته 02، في ذكرها لأنواع التشفير كوسيلة فنية للمحافظة على سرية المعلومات، الثابت منها والمتحرك باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات، إلى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك فهم لا يستطيعون فهم أي شيء².

فمن خلال ما سبق نجد أنه مهما تعددت وتنوعت التشفيرات يكمن دورها في الحماية التي تفرضها وتضمنها للتوقيع الالكتروني مما يزيد في ثقة التعامل به بين المصالح المتعاقدة على جميع المستويات وذلك من خلال عدم إمكانية استعمال التوقيع الالكتروني أو الاطلاع عليه إلا من طرف صاحبه وفق تقنيات توفرها الدولة.

المطلب الثاني: دور التشفير في حماية التوقيع الالكتروني

يعمل التشفير كوسيلة حماية على عدة مستويات منه، لهذا توجد عموما ثلاث طرق لتشفير البيانات المخزونة على أجهزة الحاسوب، إذ يمكن تشفير ملفات معينة، أو تشفير القرص الصلب بأكمله (Hard Disk).

فقد يكون التشفير على مستوى الإرسال على جميع المعلومات والبيانات بين نقطة الإرسال ونقطة الاستقبال، أو على مستوى التصفح أو التشغيل من خلال تصفح جميع الاتصالات بين نوافذ الشبكة أو أحد المواقع الموجودة عليها، وحماية البيانات أثناء استقبالها³، كما يكون التشفير على مستوى التطبيق والملفات، فمن خلال ذلك هو نظام تأميني على المعاملات الالكترونية، ويعتبر هذا النظام من أهم البرتوكولات المتعلقة بالنواحي التي ظهرت في مجال منظومة التجارة الالكترونية، حتى تتم كل المعلومات بطريقة آمنة ومضمونة⁴، فتحول التوقيع إلى رموز لا يعرف مفاتيحها إلا صاحب التوقيع.

المطلب الثالث: تقدير التشفير كآلية للحماية التوقيع الالكتروني في مجال الصفقات العمومية

-
- ¹ - سعيد السيد قنديل، التوقيع الإلكتروني، دار الجامعة الجديدة، مصر، 2006، ص 70.
 - ² - Brazell Lorna, electronic signatures, law and regulation sweet maxwell, london, 2004, p 50.
 - ³ - وسيم شفيق الحجار، الإثبات الالكتروني، المنشورات الحقوقية، بيروت، 2002، ص 198.
 - ⁴ - أشرف السعيد أحمد، المرجع السابق، ص 163.
 - ³ - إلياس ناصيف، العقود الدولية - العقد الالكتروني، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت- لبنان، 2009، ص 244.
 - ⁴ - لهذا فالتشفير يتم حتى على الرسائل الالكترونية والملفات التي يتم تداولها عبر شبكة الانترنت فوفقا للبرنامج التأمين الذي وضعه فيليب زيمرمان لحماية الوسائل الالكترونية عام 1996، يتم تشفير البيانات التي تحتويها الرسائل باستخدام أسلوب المفتاح العام، ويتميز هذا البرنامج بسهولة استخدامه، وصعوبة الهجوم عليه.
 - محمد سعيد رشدي، التعاقد بوسائل الاتصال الحديثة ومدى حجيتها في الإثبات، منشأة المعارف، الإسكندرية، 2008، ص 55.
 - سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة، دار النهضة العربية، القاهرة، 2006، ص 218.

إذا اختارت الإدارة طريقة التعاقد بوسائل الكترونية فإن عملية إدخال الصفقة حيز التنفيذ يكون بالتوقيع عليها إلكترونياً، وفي هذه الحالة يعد التشفير من الآليات التي تضمن حماية وتأمين المعلومات الالكترونية للبيانات من خلال تغيير تلك البيانات عن طريق تحويلها إلى رموز أو إشارات لحمايتها من إطلاع الغير عليها من أجل تدعيم الثقة التعامل بالتوقيع الالكتروني من جهة، وحماية مختلف البيانات والمعلومات من الضياع والتعدي عليها بالقرصنة أو التحريف أو التغير فيها.

كما يعد التشفير من الوسائل المستخدمة في حفظ البيانات والمعلومات بشكل يصعب الاطلاع عليها من قبل الغير، خاصة وأنه من الضمانات المؤتمن عليها في المجالات العسكرية إذ يستخدم في تأمين الاتصالات التي تحتوي على المعلومات والأوامر بين القادة، لكن هذا لا يمنع من وجود هيئة ثالثة وهي التصديق الالكتروني لان التشفير وحده لا يكفي من جهة أخرى¹.

المبحث الثاني: التصديق الالكتروني كآلية لحماية التوقيع الالكتروني على الصفقات العمومية

نتيجة لانتشار الواسع لعمليات التعاقد التي تتم عبر شبكة الانترنت، كان لبد من إيجاد حلول تقنية خاصة مع تنامي مخاطر القرصنة الالكترونية عبر شبكة الانترنت²، ولتفادي هذه المخاطر لبد من التصديق الالكتروني الذي يؤكد فيها صحة هوية الأطراف المتعاقدة إلكترونياً وتوقيعها، وهذه الجهات تعرف بجهات التصديق أو التوثيق الالكتروني³.

المطلب الأول: الجهة المختصة بإصدار شهادة التصديق الالكتروني

من أجل تأمين وإضفاء الحماية القانونية للتوقيع الالكتروني لبد من فرض بنود تعكس شروط تؤكد صحة التوقيع الالكتروني وإيجاد طرف ثالث هو جهة التصديق الالكتروني .

فهما اختلف الفقه والقانون في اصطلاح تسميتها فهي "الجهة المختصة بإصدار شهادات التصديق الالكتروني" التي تقدم خدمات أمنية في التجارة الالكترونية، لتثبت صحة حقيقة معينة متعلقة بموضوع التبادل الالكتروني لتوثيق هوية الأشخاص المستخدمين لهذا التوقيع الرقمي، وكذلك نسبة المفتاح العام المستخدم إلى صاحبه⁴، والتأكد من السلطة المختصة بإصداره⁵.

¹ - إن التشفير يعد أيضا ك تقنية للحماية الحسابات الشخصية من القرصنة والمخترقين للأنظمة المعلوماتية فهو من أحسن التقنيات للضمان الحماية وإبعاد الخطر الذي يقع على المواقع الالكترونية والأنظمة المعلوماتية والبرامج والبطاقات الائتمانية.

² - محمد سعيد رشيد، المرجع السابق، ص58.

³ - سمير حامد عبد العزيز الجمال، المرجع السابق، ص221.

⁴ - لينا إبراهيم يوسف حسان، التوثيق الالكتروني ومسؤولية الجهات المختصة به، دار الراية للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2009، ص40 وما يليها.

⁵ - سماح عبد الواحد التهامي، التعاقد عبر الانترنت، دراسة مقارنة، دار الكتب القانونية، مصر، 2008، ص 416.

عرف المشرع الفرنسي من خلال المادة الأولى الفقرة 11 من المرسوم 2001/272 باستخدامه مصطلح مزود خدمات التصديق الإلكتروني بأنه "كل شخص يصدر شهادات الكترونية أو يقدم خدمات التوثيق الإلكتروني الأخرى المتعلقة بالتوقيع الإلكتروني"¹.

أما المتصفح للمنظومة² القانونية والتنظيمية في الجزائر نجد المرسوم التنفيذي رقم 162-07 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية طبقا للمادة 03 حيث سماها بمؤدي خدمات التصديق الإلكتروني وهي سلطة ضبط البريد والمواصلات طبقا للمادة 10 من قانون 03-2000، ثم جاء قانون 04-15 والمحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني فسمها المشرع بمؤدي خدمات التصديق الإلكتروني طبقا للمادة 02 فقرة 12 بنصها على "أنه كل شخص طبيعي أو معنوي، يقوم بمنح شهادات التصديق الإلكتروني الموصوفة ويقدم خدمات أخرى في مجال التصديق الإلكتروني"³.

فهذه الجهة هي التي تتولى منح شهادات التصديق الإلكتروني في حالة ما إذا تم توقيع الصفقة بطريقة الكترونية، حتى تضمن صحتها وتدخل الصفقة حيز التنفيذ.

المطلب الثاني: دور جهات التصديق الإلكتروني في حماية التوقيع الإلكتروني

تلعب هذه الجهة دورا مهما في حمايته التوقيع الإلكتروني وتدعيم ثقة التعامل به وذلك من خلال:

- **منح شهادة التصديق الإلكتروني** من أهم الأهداف والصلاحيات التي تقوم بها مزود خدمات التصديق الإلكتروني بإصدار شهادة التوثيق التي ترتبط بهوية موقعها وفق الشروط القانونية حتى تصدر وثيقة شهادة التصديق الإلكتروني.

وعرفها المشرع الجزائري⁴ في المادة الثانية الفقرة 7 من قانون 04-15 بأنها "وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقع".

¹ - منح التوجيه الأوروبي رقم 1999/93 للدول الاتحاد الأوروبي بإنشاء أنظمة طوعية من أجل إعطاء اعتماد لمزاولة نشاط التصديق الإلكتروني طبقا لنص المادة 3 الفقرة 2، من أجل إضفاء الشفافية وفق هذا التوجيه.

- Article 3 paragraphe 2 de directive 1999/93/ce du parlement européen et du conseil, du 13 /12/1999, sur un cadre communautaire pour les signatures électroniques (J O N°1013 du 19/01/2000 p.00012-0020).

- Article 9 paragraphe 2 Décret n° 2001-272 du 30/03/2001 pris pour l'application de l'article 1316-4 du Cod civil et relatif à la signature électronique.

² - أزرو محمد رضا، النظام القانوني لمزود خدمات التصديق الإلكتروني "دراسة مقارنة"، مجلة العلوم القانونية والإدارية والسياسية لكلية الحقوق والعلوم السياسية جامعة أبي بكر بلقايد- تلمسان، العدد 14، سنة 2012، ص 126.

³ - المادة 02 الفقرة 12 من قانون التوقيع الإلكتروني رقم 04-15 المؤرخ في 01 أبريل 2015 والمحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني، ج.ر.ج. عدد 6 صادرة بتاريخ 10 أبريل 2015 ص.6.

- خالد إبراهيم ممدوح، إبرام العقد الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006، ص.195.

⁴ - قبل صدور قانون 04-15 كان اختصاص ومنح الترخيص لمزاولة خدمات التصديق الإلكتروني من صلاحيات سلطة ضبط البريد والمواصلات السلكية واللاسلكية تطبيقا للمادة 02 من المرسوم التنفيذي رقم 162-07 المؤرخ في 30/05/2007 يعدل ويتم المرسوم التنفيذي رقم 01-123 المؤرخ 09/05/2001 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج.ر.ج. عدد 37 المؤرخ في 07 ماي 2007، ص.13.

كما أضافت المادة 15 شروطا خاصة لشهادة التصديق الالكتروني الموصوفة شهادة تتوفر فيها الشروط التالية:

- أن تمنح من طرف ثالث موثوق أو من قبل مؤدي خدمات التصديق الالكتروني طبقا لسياسة التصديق الالكتروني الموافق عليها.

- أن تمنح للموقع دون سواء..."، من خلال هذه المادة أوكل مهمة التصديق وفق ما جاءت به المادة الثانية الفقرة 11 للشخص معنوي توكل له مهمة منح شهادات التصديق الالكتروني الذي يقدم خدمات التصديق الالكتروني ويقدم خدمات أخرى في هذا المجال وفق المادة 2 الفقرة 12، في حين المادة 15 ألزمت من يقوم بإصدار شهادات التصديق الموصوفة بمطابقتها للشروط المحدد في هذه المادة.

وفي الأخير فإن هذه الوثيقة التي تعكس الكترونية التوقيع الالكتروني وصحته من خلال مطابقة البيانات مع الموقع تصدر عن مزود خدمات التصديق الالكتروني¹، وتتعدد هذه الشهادات وتتنوع حسب درجات موثوقيتها إلا أن المشرع الجزائري وفق المادة 15 من قانون 04-15 اقتصر فقط على شهادة التصديق الالكتروني البسيطة والموصوفة، ومن بين الشهادات الموجودة في المعاملات المدنية والتجارية نجد شهادة الإذن، شهادات المعاملة، شهادة التوقيع الرقمي.

ولكي تكون لشهادة التصديق الالكتروني قوة قانونية وتكون موصوفة، لبد أن تحتوي على بيانات إلزامية، وفي حالة تخلفها يفقدها قيمتها القانونية².

- تحديد هوية مزود خدمات التصديق الالكتروني والسلطة المختصة تتجسد أهمية تحديد جهات التوثيق إلى زيادة الثقة والائتمان القانوني، وهذا ما نصت عليه المادة 15 الفقرة ب بنصها "تحدد هوية الطرف الثالث الموثوق أو مؤدي خدمات التصديق الالكتروني وكذا البلاد الذي يقيم فيه".

- تحديد تاريخ سريانها وانتهائها نصت للمادة 15 فقرة ح من قانون 04-15 لبد من الإشارة إلى بداية ونهاية مدة صلاحية شهادة التصديق الالكتروني"، فإذا انتهت مدة صلاحية هذه الشهادة فعلى جهات التصديق الالكتروني أن تقوم بنشر قائمة الشهادات المنتهية الصلاحية حتى تعفى من مسؤوليتها.

المبحث الثالث: الحماية القضائية للتوقيع الالكتروني على الصفقات العمومية

نظرا لأهمية التوقيع الالكتروني وانتشاره الواسع خاصة مع تطور التجارة الالكترونية العابرة للحدود، مما يجعله عرضة للتعدي عن طريق القرصنة أو التعدي على البيانات الالكترونية أو إتلافها، لهذا وحتى يكون له حجية في الإثبات لبد أن يكون محل حماية جزائية وفق ما يقتضيه القانون.

خاصة لما يتعلق الأمر بالصفقات العمومية التي تحتوي أضخم المبالغ المالية، والتي تهدف إلى تحقيق المصلحة العامة فلبد من حماية توقيع على الصفقة العمومية إذا تمت بطريقة الكترونية.

¹- لينا إبراهيم يوسف حسان، المرجع السابق، ص75.

²- إلياس ناصف، المرجع السابق، ص265.

المطلب الأول: الجريمة المعلوماتية والتوقيع الالكتروني

نظرا للانتشار الواسع للتعامل عبر شبكة الانترنت، ظهر ما يعرف بالقرصنة أو التعدي على البيانات أو المعلومات الالكترونية وعلى الرموز والأرقام والبيانات التي تعكس حجية التوقيع الالكتروني من خلالها¹.

نجد المشرع الفرنسي² عرفها من خلال القانون 1988/19 تضمن بعض الجرائم الالكترونية المعلوماتية وأقر بأنها "أي جريمة يكون متطلبا لاقترافها أن تتوفر لدى فاعلها معرفة تقنية الحاسب" أو "هي أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبيه أو هي كل سلوك إجرامي بمساعدة الحاسب الآلي أو تحدث في محيطه".

فمن خلال هذا التعريف فإن الجريمة الالكترونية تقوم على التعدي أو الاختراق لأحد أنظمتها المعلوماتية أو استهداف لبياناتها وبرامج تطبيقه من خلال الاستيلاء على محتوى الإجراء المعلوماتي.

أما المشرع الجزائري عرف الجريمة المعلوماتية في المادة 02 من قانون 04-09 المتضمن القواعد الخاصة من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بأنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظم الاتصالات الالكترونية، ومن خلال التعريفات السابقة تقوم هذه الجريمة على التوقيع الالكتروني على:

1- تعدي أو تحايل أو تزوير على التوقيع الالكتروني.

2- المساس بطريقة غير قانونية بأنظمة معلوماتية أو نظام اتصالات الكترونية من أجل الولوج للتوقيع الالكتروني.

3- تجريم الفعل المرتكب من خلال التعدي على الأنظمة المعلوماتية.

المطلب الثاني: موقف التشريعات من الحماية الجنائية للتوقيع الالكتروني

نظرا لأهمية التوقيع الالكتروني أصدرت غالبية الدول قوانين خاصة بالتوقيع الالكتروني تضمن له حماية قانونية وتعاقب على كل الجرائم المستحدثة فيه، ففي فرنسا عاقب المشرع في قانون العقوبات الجديد الصادر عام 1992 على التزوير في المحررات الرسمية والعرفية والتي تقع بأي طريقة كانت، وهذا دليل على فتح المجال على التعدي أو التزوير الالكتروني من خلال المواد (145-152) التي يندرج فيها ما يعرف بالتزوير المعلوماتي والتزوير بالطرق الأخرى التقليدية، فنص المادة 441 واضحا حيث

¹ - حسن بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دار النهضة العربية، القاهرة، ص 06 وما يليها.
- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، 2010، ص 52.

² - حسن بن سعيد الغافري، المرجع السابق، ص 10 وما يليها.

فتح من طرق تزوير التوقيع الالكتروني بإصلاح "أي وسيلة" وهذا دليل على إمكانية تطبيقه على التزوير المعلوماتي¹.

وعليه ف الجريمة التعدي على التوقيع الالكتروني تقوم على ركنين فيها الأول الركن المادي الذي يعكس سلوك التعدي على التوقيع الالكتروني من خلال فعل التزوير أو التقليد الالكتروني أو الدخول غير المشروع للأنظمة المعلوماتية أو قاعدة البيانات التي تخص التوقيع بحد ذاته، أما الركن الثاني فهو معنوي يعكس تعمد السلوك الإجرامي في اختراق أو التعدي على التوقيع الالكتروني أو الدخول الغير مشروع على قاعدة البيانات التي تتعلق به، فقصد الجاني متعمدا وعليه فالقصد الجنائي قائم بعنصريه العلم والإرادة، فرغم خطورة الفعل إلا أن الجاني تعمد ذلك الفعل الإجرامي².

ومن هذه الجرائم التي قررت للحماية التوقيع الالكتروني إذا تضمنته الصفة العمومية نجد:

1-جريمة تزوير التوقيع الالكتروني: لقد اعتبر الفقه تزوير التوقيع الالكتروني من أشكال الغش المعلوماتي وجريمة التزوير الالكتروني التي لها أركان خاصة بها وأثار تنعكس على العقوبة المقررة لها، ومن خلال قانون التوقيع والتصديق الالكترونيين 04-15 لم يقر فيها أو يخصص لهذه الجريمة أي أحكام تخصها، لكن هذا لا يعني أنه لا يمكن تطبيق عليها القواعد العامة فيما يخص جريمة التزوير التقليدية مادام أنها لا تتعارض والأحكام العامة³.

3-جريمة صنع أو حيازة برامج لإعداد توقيع إلكتروني مزور: وتتفرع من هذه الجريمة جريمة صناعة نظام معلوماتي لإعداد برنامج توقيع إلكتروني، أحيازة النظام أو البرامج وذلك بغرض إعداد توقيع إلكتروني دون موافقة صاحبه فمن خلال هذه الأنظمة المعلوماتية يهدف إلى التعدي على التوقيع الالكتروني.

4-جريمة الدخول بالغش على قاعدة بيانات التوقيع الالكتروني: يقصد بقاعدة البيانات التي تتعلق بالتوقيع الالكتروني البيانات المخزنة داخل الحساب الآلي أو قرص منفصل، مثل البيانات المتعلقة باسم صاحب التوقيع ومهنته وكافة بياناته الشخصية وكافة المعلومات المتعلقة بذلك التوقيع والتي يفترض سربيتها، بمجرد التحول غير مشروع يعتبر جريمة إلكترونية⁴.

5-جريمة فض مفاتيح التشفير: تقع هذه الجريمة على موضوع التجارة والضرر المحقق في المستقبل، وهو من جرائم الخطر وليس من جرائم الضرر، لكون التشفير كما سبق من الأمور الخطرة

¹-ولقد أكد التشريع الفرنسي على ذلك من خلال قانون التوقيع الالكتروني الصادر بتاريخ 2000/03/13 رقم 2000/230 في صورة تعديل للنصوص المنظمة للإثبات لتتماشى مع تقنيات المعلوماتية، ونظرا للتطور المعاملات المدنية والتجارية وحتى الإدارية وكثرة استخدام التوقيع الالكتروني أدرج هذا التعديل في نص المادة 1316 من القانون المدني باعتباره الشريعة العامة.

²- محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة، الأردن 2004، ص 233.

¹-الياس أبو عبيد، نظرية الإثبات في أصول المحاكمات المدنية والجزائية، الجزء الأول، منشورات الحلبي الحقوقية 2005 ص 181، وما يليها.

⁴- عبد الفتاح بيومي، المرجع السابق، ص 228.

-بوعمره أسيا، النظام القانوني لقواعد البيانات، رسالة ماجستير، جامعة الجزائر، 2005، ص 90 وما يليها.

التي يكون فيها مساسا بسلامة الدولة وأمنها القومي، لان عملية الكشف عن مفاتيح الشفرة أو فض المعلومات المشفرة في غير الأحوال المصرح بها قانونا يعد مساسا بسلامتها¹.

الخاتمة:

في ظل غياب النصوص القانونية الخاصة بتأمين وحماية التوقيع الالكتروني خاصة في مجال الصفقات العمومية، هذا لا يمنع من الاعتماد على القواعد العامة عند وجود توقيع الكترونيا للأطراف المتعاقدة، إذا تمت الصفقة العمومية بطريقة إلكترونية أن تضمن له حماية قانونية دولية ومحلية، من أجل ضمان التعامل به واستقرار المعاملات الالكترونية، مما أدى بالعديد من الدول الاعتراف بالتوقيع الالكتروني وأضفت عليه حجية قانونية متساوية والتوقيع التقليدي في الإثبات، حيث جعلته محصن بنصوص قانونية تشريعية وتنظيمية، من أجل إمكانية الأخذ به كحجة ودليل لإثبات والوصول إلى حلول فعلية أو جزئية من أجل توفير بنية قانونية تكفل حماية كاملة للحقوق الأطراف المتعاقدة عبر شبكة التواصل -الانترنت.

وحتى تزيد ثقة التعامل بالتوقيع الالكتروني كان لبد من إيجاد آليات ووسائل تقنية لحماية هذا التوقيع من أي مخاطر يتعرض لها التوقيع الالكتروني خاصة في مجال الصفقات العمومية كالتشفير أو بتدخل طرف ثالث كجهة التصديق الالكتروني وفرض عليه حماية جزائية من خلال تجريم التعدي على التوقيع الالكتروني لهذا نقترح التوصيات التالية:

1- على المشرع الجزائري ضرورة مواكبة التطورات وإدخال تعديلات على قانون التجارة الالكترونية وجعله أكثر دقة من حيث المصطلحات التي تنظم التوقيع الالكتروني وضمان حمايته، وتفعيل نظام عقابي خاص بحماية التوقيع الالكتروني لتفادي النقص التشريعي القائم في هذا المجال واستبعاد تطبيق النصوص التقليدية على التوقيع الالكتروني .

2- نتيجة لانتشار الواسع للتعامل بالتوقيع الالكتروني لبد من تأطيره وفق حماية قانونية متطورة على أحدث الوسائل تماشيا مع تطور وسائل الاتصال الحديثة خاصة مع انعدام الوعي بين الأشخاص سواء كانوا طبيعيين أو معنويين بمخاطر التعامل الالكتروني خاصة المواقع المقلدة أو المشبوهة لتفادي الوقوع في مصيدة المواقع المقرصنة (مصيدة الهاكر) .

¹ - عبد الفتاح بيومي، المرجع السابق، ص 228 وما يليها.

3- غياب ثقافة الثقة والتعامل بالتوقيع الالكتروني في الجزائر خاصة وأنه ولا قضية موجودة على مستوى القضاء مما يدل على عدم ثقة التعامل به وما زالت تعمل بالنصوص تقليدية من جهة، وتخوف الإدارات والمتعاملين معها من التزوير والتحايل خاصة مع الانتشار الواسع لانتزعت وتحايل المتعاملين معها مما يفتح فجوة للفساد الالكتروني والمحسوبية في اختيار المتعاملين المتعاقدين مع المصلحة المتعاقدة.

4- ضرورة التفصيل في قانون 04-15 من خلال إصدار تنظيمات بما يتماشى على مستوى الدولي خاصة مع فتح مجال الاستعمال وتوسيع مجال الصفقات العمومية خاصة مع وجود متعاملين أجانب الذين يتقنون في التوقيع الالكتروني، مما يستلزم تفعيل التعاون في مجال مكافحة جرائم الالكترونية وتسليم المجرم المعلوماتي والعمل على تبادل الخبرات الالكترونية خاصة لما يتعلق الأمر بالصفقات العمومية لأنه يسهل في عملية إتمام الإجراءات الشروع في عملية التنفيذ.

قائمة المصادر والمراجع:

أولا /قائمة المصادر:

أ- النصوص القانونية

1- قانون التوقيع الالكتروني رقم 04-15 المؤرخ في 01 أفريل 2015 والمحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني، ج.ر.ج. عدد 6 صادرة بتاريخ 10 أفريل 2015 ص6.

2- المرسوم الرئاسي 10-236 المؤرخ في 2010/10/07 يتضمن تنظيم الصفقات العمومية، الجريدة الرسمية رقم 58 لسنة 2010/10/07.

3- المرسوم الرئاسي 15/247 المؤرخ في 16 ديسمبر 2015 المتضمن الصفقات العمومية وتفويضات المرفق العام، الجريدة الرسمية العدد 50 المؤرخة في 20 سبتمبر 2015.

4- المرسوم التنفيذي رقم 01-123 المؤرخ 2001/05/09 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج.ر.ج. عدد 37 المؤرخ في 07 ماي 2007، 13.

5- المرسوم التنفيذي رقم 07-162 المؤرخ في 2007/05/30 يعدل ويتم المرسوم التنفيذي رقم 01-123 المؤرخ 2001/05/09 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج.ر.ج. عدد 37 المؤرخ في 07 ماي 2007، ص13.

-النصوص الاجنبية:

1- Directive 1999/93/ce du parlement européen et du conseil, du 13 /12/1999, sur un cadre communautaire pour les signatures électroniques (J O N°1013 du 19/01/2000 p.00012-0020) .

2-Décret n° 2001-272 du 30/03/2001 pris pour l'application de l'article 1316-4 du Cod civil et relatif à la signature électronique.

ثانيا/ قائمة المراجع:

أ-الكتب:

- 1- أشرف السعيد أحمد، القرصنة الالكترونية، مطابع الشرطة، القاهرة، 2013.
- 2- إلياس ناصيف، العقود الدولية –العقد الالكتروني، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت- لبنان، 2009.
- 3- اليأس أبو عبيد، نظرية الإثبات في أصول المحاكمات المدنية والجزائية، الجزء الأول، منشورات الحلبي الحقوقية 2005.
- 4- بشرى حسن الحمداني، القرصنة الالكترونية أسلحة الحرب الحديثة، دار أسامة، عمان، الأردن، الطبعة الأولى، 2014.
- 5- حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية، 2000.
- 6- حسن بن سعيد الغافري، السياسية الجنائية في مواجهة جرائم الانترنت، دار النهضة العربية، القاهرة، 2014.
- 7- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، 2010.
- 8- خالد مصطفى فهمي، النظام القانوني للتوقيع الالكتروني في ضوء التشريعات العربية والاتفاقيات الدولية، دار الجامعة الجديدة، 2007 .
- 10- خالد إبراهيم ممدوح، إبرام العقد الالكتروني، دار الفكر الجامعي، الإسكندرية، 2006.
- 11- سماح عبد الواحد التهامي، التعاقد عبر الانترنت، دراسة مقارنة، دار الكتب القانونية، مصر، 2008.
- 12- سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة، دار النهضة العربية، القاهرة، 2006.
- 13- سعيد السيد قنديل، التوقيع الإلكتروني، دار الجامعة الجديدة، مصر، 2006، ص 70.
- 14- فيصل سعيد الغريب، التوقيع الالكتروني وحجته في الإثبات، المنظمة العربية للتنمية الإدارية، 2005 .
- 15- ليلى إبراهيم يوسف حسان، التوثيق الالكتروني ومسؤولية الجهات المختصة به، دار الراية للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2009.

الحماية القانونية لتأمين التوقيع الالكتروني في الصفقات العمومية في الجزائر

16- محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة، الأردن، 2004.

17- محمد دباس الحميد، حماية أنظمة المعلومات ، دار الحامد للنشر والتوزيع، الأردن، 2007.

18- محمد سعيد رشدي، التعاقد بوسائل الاتصال الحديثة ومدى حجيتها في الإثبات، منشأة المعارف، الإسكندرية، 2008.

19- نهلة عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، عمان، الأردن، الطبعة الثانية، 2010 .

20- وسيم شفيق الحجار، الإثبات الالكتروني، المنشورات الحقوقية، بيروت، 2002.

ب-الرسائل الجامعية:

1-بوعمره أسيا، النظام القانوني لقواعد البيانات، رسالة ماجستير، كلية الحقوق بن عكنون، جامعة الجزائر، 2005.

د-المقالات:

1- أزرو محمد رضا، النظام القانوني لمزود خدمات التصديق الالكتروني "دراسة مقارنة"، مجلة العلوم القانونية والإدارية والسياسية لكلية الحقوق والعلوم السياسية جامعة أبي بكر بلقايد- تلمسان، العدد 14، سنة 2012، ص120 إلى غاية ص 145.

2-فايزة خير الدين، استحداث المعاملات الالكترونية كمبدأ للمبدأ الشفافية في عملية إبرام الصفقات العمومية في الجزائر، مجلة قضايا معرفية، جامعة الجلفة، الجزائر، المجلد الأول، العدد الثالث، جوان 2019، ص24 إلى غاية ص47.

ه-المدخلات والملتقيات

1-فايزة خير الدين، التوقيع والتصديق الالكترونيين، ملتقى وطني حول تأثير الرقمنة على المفاهيم التقليدية للمعاملات المدنية والتجارية (بين مستجدات التشريع وصعوبة التطبيق)، كلية الحقوق سعيد حمدين، جامعة الجزائر 1، يومي 22-23 أكتوبر 2019.

ثانيا: المراجع باللغة الأجنبية

1-O.Moreteau,l'estoppel et la protection de la cofinance legitime, these, universite jean moulim, lyon iii ,1990,p24.

2-Jeffrey F.Rayport Et Jaurorski Bernard , commerce electronique (traduit de l'américain port) francine nézina, johanne champoux et elisabéth rochette, edition cheneliere/ mcgram-hill, montréal – toronto, 2003.

3-Dimitriou Philippe, «l'application du droit de la cryptologie en matière de sécurité des réseaux informatique » d.e.afac des sciences juridique, politiques et sociaux, ecole doctorale n°74, université de lille, 2002.