الحماية الفنية والجزائية للتوقيع الالكتروني على ضوء القانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين

صحراوي مصطفى؛ طالب دكتوراه؛ الطور الثالث/حقوق؛ تخصص: علوم جنائية؛ جامعة وهران2 محمد بن احمد

البريد الالكتروني : kmsahraoui@gmail.com

ملخص :

سعيا منه إلى تكريس امن وسرية المعلومات و إضفاء الثقة على مختلف المعاملات في المجال الالكتروني ووضع الركائز الأساسية لمفرزات العالم الرقمي، اصدر المشرع الجزائري القانون 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين كتشريع مستحدث معالجا بذلك ما استجد من وسائل و أساليب لإبرام العقود.

Abstract:

In order to establish the security and confidentiality of information, to establish confidence in various transactions in the electronic field and to establish the basic pillars of the digital world, the Algerian legislator promulgated Law 15-04, which sets forth the general rules relating to electronic signature and certification as an updated legislation, thus addressing the means and methods of concluding contracts. .

مقدمة:

ادى التطور التكنولوجي الهائل في وسائل الاتصالات والمعلومات الى ظهور اساليب جديدة في ابرام العقود لم تكن معروفة منذ سنوات قليلة وصاحب هذا التطور تغيرا اخذ فيه التوقيع الالكتروني الجانب الابرز، محولا التجارة من تجارة تقليدية إلى تجارة إلكترونية[1] فلم يعد التوقيع التقليدي ملائما للمعاملات الإلكترونية، لذلك ظهر التوقيع الإلكتروني بديلا عنه. بل أصبح يعد أحد الوسائل الأساسية في تنظيم الخدمات المصرفية الإلكترونية، فالكثير منها يستند إلى التوقيع الإلكتروني في إثباتها وقبولها، إذ تستلزم عقود التجارة الإلكترونية لصحة تمامها توقيع الأطراف المتعاقدة، وذلك بهدف الحفاظ على سرية المعلومات أو الوسائل المرسلة وعدم قدرة أي شخص آخر على الاطلاع أو تعديل المعلومات. كما أنه يحدد هوية المرسل والمستقبل ويتم التأكد عن طريقه من صدق وصحة المعلومات لذلك تكتسي الحجية القانونية للتوقيع الإلكتروني أهمية بالغة في الإثبات

1/ التجارة الإلكترونية **e-commerce** من أهم التغييرات الجديدة التي دخلت حياتنا بقوة، و أصبحت تتداول في استخدام العادي لتعبر عن بعض الأنشطة الإنسانية المرتبطة بثورة تكنولوجيا المعلومات و الاتصالات. لمزيد من الاطلاع أنظر: رأفت رضوان: عالم التجارة الإلكترونية، القاهرة، المنظمة العربية للتنمية الإدارية، 1999 . ص 16.

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10

الإلكتروني وبالتالي في حقوق المتعاملين عبر الوسائط الإلكترونية، مما جعلها محل اهتمام المشرعين سواء على الصعيد الدولي أو الوطني[1].

ونظرا لأهمية التوقيع الإلكتروني في حماية معاملات الأشخاص والمؤسسات الاقتصادية عبر العالم الافتراضي حرصت التشريعات الدولية ومنها المشرع الجزائري على حماية وتأمين هذه الوسيلة (التوقيع الإلكتروني) من الاعتداءات التي تقع عليه من الغير، ولعل صدور القانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين جاء في نفس الاتجاه، وذلك من خلال توفير حماية فنية وجنائية[2] للتوقيع الإلكتروني، وهو ما يجرنا الى الاجابة عن الإشكال التالي:

ماهي النصوص القانونية والآليات الفنية التي وقعتها الدولة لحماية وتأمين التوقيع الإلكتروني؟

من خلال محورين اثنين نخصص الأول: للحماية الفنية للتوقيع الإلكتروني وهو مقسم إلى مسألتين خصصت المسألة الأولى: للتشفير كوسيلة لتأمين للتوقيع الإلكتروني والثانية: الية المصادقة على التوقيع الإلكتروني.

أما المحور الثاني: فهو معنون بالحماية الجنائية للتوقيع الالكتروني ويتضمن مسألتين: نتناول في المسألة الأولى الحماية الجنائية للتوقيع الإلكتروني في التشريعات الأجنبية والعربية، وأما المسالة الثانية نتناول فيها الحماية الجنائية للتوقيع الإلكتروني في التشريع الجزائري.

---

1 / تنص المادة 1/6 من القانون اليونسيترال بشأن التوقيعات الإلكترونية على أنه << عندما يشترط القانون وجود توقيع من شخص، يعد ذلك الشرط مستونيا في رسالة البيانات إذا استخدم توقيع الإلكتروني موثوقا به بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله رسالة البيانات في ضوء كل الظروف بما في ذلك أي انفاق ذي صلة>>.

كما نصت المادة (2/327) من القانون المدني الجزائري على أنه <<و يعتد بالتوقيع الإلكتروني وفقا للشروط المذكورة في المادة 323 مكرر/1>> يكون بذلك قد ساوى في الحجية بين التوقيع الإلكتروني و الوقيع التقليدي وفق للأحكام المقررة في القانون المدني و في نفس الوقت اشترط المشرع الجزائري للاعتداء بالتوقيع الإلكتروني و منحه الحجية الكاملة، أن تتوافر فيه الشروط المنصوص عليها في المادة 323 مكرر1، و تتمثل تلك الشروط في إمكانية التأكد من هوية الشخص المصدر للتوقيع و أن يكون هذا التوقيع معدا و محفوظ في ظروف تضمن سلامته.

2 / و الحماية الجنائية **la protection pénal** للتوقيع الإلكتروني يقصد بها تأمين هذا التوقيع من الاعتداء عليه بجريمة و الحفاظ عليه باصباغ حماية المشرع الجنائي بنصوص تجريمية لملاحظة الجاني المعلوماتي و مساءلته جنائيا عن الفعل المستند إليه بعقوبات رادعة.

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10

المحور الاول: الحماية الفنية للتوقيع الإلكتروني

عرف المشرع الجزائري التوقيع الالكتروني من خلال المادة 2فقرة 1 من القانون04/15 المتعلق بالتوقيع والتصديق الالكترونيين انه "بيانات في شكل الكتروني مرفقة او مرتبطة منطقيا ببيانات الكترونية اخرى تستعمل كوسيلة توثيق"[1]

ولا شك ان أمن هذه البيانات و تأمين عملية التوقيع الإلكتروني و التحقق من شخصية المتعاقدين و تأمين سلامة عملية تداول البيانات لإتمام الصفقة التجارية الالكترونية يحتاج الى وسيلة حماية فنية بالدرجة الاولى سيتم توضيحها بالتعرض الى مفهوم تشفير البيانات و التوقيع الإلكتروني المنصوص عليها في القانون 04/15 السالف الذكر كمسألة أولى، ثم إن شيوع التعاملات الإلكترونية يتوقف على قدرة ما تتمتع به من أمان وثقة لدى مستخدمي وسائل و تقنيات الاتصال الحديثة، و لما كانت المستندات الإلكترونية بما فيها العقود تتم عن بعد بين أطراف قد يجهل بعضهم البعض و هو الأمر الذي يتطلب توفير الضمانات ووسائل تكفل تحديد هوية المتعاقدين، و تضمن التعبير عن إرادتهم على نحو صحيح و بطريقة يمكن معها نسبة التصرف إلى صاحبه، مما تطلب معه إيجاد حلول تقنية لاسيما في ظل تنامي القرصنة الإلكترونية و إساءة استخدام أسماء الغير و توقيعاتهم في أنشطة غير مشروعة عبر الأنترنت[2] فظهرت الحاجة إلى وجود طرف ثالث محايد موثوق به يتأكد بطريقة خاصة من صحة وجدية صدور التواقيع الإلكترونية، وكذا الإرادة التعاقدية الإلكترونية ممن تنسب إليه، وبعدها عن الغش و الاختيال، ويتمثل هذا الطرف الثالث المحايد في أفراد أو شركات أو جهات مستقلة محايدة تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الإلكترونية، يطلق عليها اسم سلطات التوثيق أو مقدمي خدمات التصديق[3] وهو ما سيتم التطرق اليه في المسألة الثانية من هذا المحور الثاني.

المسألة الأولى: حماية التوقيع الإلكتروني عن طريق التشفير

ظهر التشفير كتقنية لتأمين التوقيع الإلكتروني والمعاملات الإلكترونية، ذلك أنه إجراء يؤدي إلى الثقة والأمان، فهو يقوم أساسا على استخدام أدوات وأساليب لتحويل المعلومات وإخفاء محتوياتها للحيلولة دون تعديلها أو

---

[1]/ قانون رقم 15-04 مؤرخ في 01 فبراير 2015 ، يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين ج.ر ، عدد 06 صادر في 2015/02/10.

2 / لزهر بن سعيد، النظام القانوني للعقود التجارة الإلكترونية، دار هومة الجزائر، 2012 ص 170-171.

3 / ابراهيم الدسوقي أبو الليل، التوقيع الإلكتروني و مدى أهميته في الإثبات «دراسة مقارنة» -مجلة الحقوق، جامعة الكويت، العدد03 سنة2005 ص 125-126.

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10

استخدامها الغير مشروع[1] وعليه سوف نتطرق إلى مفهوم تشفير البيانات والتوقيع الإلكتروني أولا ثم إلى العلة من التشفير الإلكتروني.

أولا: مفهوم تشفير البيانات والتوقيع الإلكتروني

التشفير هو تغير في الشكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من الاطلاع الغير عليها أو ما تعديلها أو تغييرها[2].

ومن هنا يتضح أن التشفير عملية تؤدي تحويل المعلومات إلى رموز غير مفهومة بحيث لا يمكن لغير المرخص لهم بالاطلاع عليها او فهمها إلا إذا تم إعادة تحويلها إلى صفتها الأصلية عن طريق استخدام المفتاح المناسب لفك الشفرة[3]و بالرجوع إلى قانون رقم 15-04 نجد المشرع الجزائري لم يتبنى تعريفا للتشفير[4] و اكتفى بتحديد أنواعه و النص عليه كلما اقتضت ضرورة استخدامه، وهذا موقف محمود من غير المشرع الجزائري لأن عملية التعريف ليست مهمة المشرع يقدر ماهي مهمة الفقه، ولكي يقوم التشفير بوظيفته المتمثلة في حفظ و تأمين التوقيع الإلكتروني لابد من احترام من الضوابط التي يقوم عليها و قبلها معرفة طرق التشفير فيما يلي:

أ- طرق التشفير

التشفير[5] كوسيلة لتأمين التوقيع الإلكتروني والوثيقة الإلكترونية يمكن أن يتم بطريقتين: الأولى تسمى بالتشفير المماثل (السيميتري) أما الثانية فتسمى التشفير اللامماثل.

---

1 / عبد الفتاح بيومي حجازي، التجارة الإلكترونية و حمايتها القانونية، دار الفكر الجامعي، الإسكندرية ص 204.

2 / هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، ورقة بحثية مقدمة إلى مؤتمر أعمال المصرفية الإلكترونية بين الشريعة و القانون، جامعة الإمارات العربية المتحدة، مرجع سابق، ص 590.

3 /سمير حامد عبد العزيز جمال، التعاقد عبر تقنيات الاتصال الحديثة (دراسة مقارنة) دار النهضة العربية، مصر، 2001 ص 217-218.

4 /حيث نص المشرع الجزائري في الفقرة الثامنة و التاسعة من المادة الثانية من القانون 15- 04 المتعلق بالتوقيع و تصديق الإلكتروني على مفتاح التشفير العام و الخاص و أعطى تعريف لكل منهما.

5 / إن نظام التشفير هو أحد فروع العلوم الرياضية، و لقد كان في الزمن الماضي يستخدم لأغراض حكومية و عسكرية فقط. أما حاليا فقد اهتدت استخداماته وأصبح يدخل في كثير من نظم المعلومات و الشبكات، هذا و قد مر التشفير بمراحل عديدة من التطور و مازال هذا النظام فب تطور مستمر حتى الآن. أنظر: محمد أمين الرومي، النظام القانوني في التوقيع الإلكتروني، دار الكتب القانونية، مصر2008مرجع سابق، ص 32.

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10

الطريقة الاولى:التشفير المماثل أو السيميتري la cryptographie symétrique

يعني ذلك أن مصدر الرسالة والمرسل إليه يستخدمان نفس مفتاح التشفير لفك رموز الرسالة وقبل ارسال الرسائل المشفرة يتم ارسال مفتاح التشفير إلى المرسل إليه بطريقة آمنة ليستطيع فك الشفرة ثم تطور إلى نظام Asymétriqueوهي وسيلة تتيح استخدام العديد من الأرقام المعقدة يتعذر تزويرها[1].

والمشرع الجزائري لم ينص على هاته الطريقة في القانون15-04 و هذا دليل على سعة اطلاعه على مزايا و عيوب هذه الطرق بحيث جعلته يتبنى الطرق الأكثر أمنا[2].

الطريقة الثانية: التشفير اللامماثل أو بطريقة المفتاح العام La cryptographie Asymétrique

هناك طريقة أخرى لتشفير التوقيع الإلكتروني الرقمي هي نظام التشفير بطريقة المفتاح العام وهي سلسلة من الهندسة العكسية **algorithme** و هي تستخدم مفتاحين مختلفين واحد للتشفير و الآخر لفك التشفير و يتمتع المفتاحان بخاصة هام، هي أنه لو عرف أحدها هاذين المفتاحين لا يمكن معرفة المفتاح الآخر حسابيا و كل مفتاح منهما سواء المفتاح العام[3] أو الخاص[4] يحمل علامة رياضية لا يمكن معرفتها إلا من جانب صاحبها [5].

وقد تبنى المشرع الجزائري من خلال القانون 15-04 هذه الطريقة وذلك في نص المادة الثانية فقرة 8 و9 حيث عرف في الفقرة 8 من المادة الثانية مفتاح التشفير الخاص بأنه «عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الإلكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي».

---

1 / هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الأنترنت، دار النهضة العربية، القاهرة 2000، ص 76 و ما يليها.

2 / أهم عيوب هذه الطريقة تكمن في عملية تبادل المفتاح السري، أي أن الرسالة يستطيع فك شفرتها شخص آخر غير المرسل إليه، و ذلك بمجرد علمه أو حصوله على المفتاح السري مما أدى إلى عدم توافر الثقة في هذا النوع و هو ما أدى إلى تراجع استخدامه. أنظر سمير حامد عبد العزيز جمال، مرجع سابق، ص 219،220.

3 / المفتاح العام هو أيضا يتكون من مجموعة الرموز و الأرقام التي يتم تبليغها للمرسل إليه يتمكن من فك شفرة الرسالة التي تم تشفيرها بالمفتاح الخاص، و لكنه يختلف عن المفتاح الخاص في أنه يكون معروفا لطرفين أو أكثر و هو ما تعرض له المشرع الجزائري في المادة الثانية فقرة 09 من القانون 15-04.

4 / يتكون المفتاح الخاص من مجموعة من الرموز و الأرقام و التي يمكن تخزينها على بطاقة إلكترونية، و يكون هذا المفتاح معروفا لطرف واحد فقط و هو المرسل و الذي يظل متحفظا بسريته، و يستخدم هذا المفتاح لتشفير الرسالة و فك شفرتها: أنظر: عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظام القانونية المقارنة، مرجع سابق، ص 31-32.

5 / عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص 197.

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10

أما الفقرة التاسعة من نفس المادة المذكورة أعلاه فقد عرض فيها مفتاح التشفير العمومي(العام) بقوله: «هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني، وتدرج في شهادة التصديق الإلكتروني».

وتعد هذه الطريقة حسب رأي البعض[1] أكثر أمانا من الطريقة السابقة لأنه من يقع بحوزته المفتاح العام فلا يقع في علمه المفتاح الخاص، وبالتالي عدم إمكانية فك شفرة الرسالة وهذه الخاصية دفعت المشرع الجزائري إلى تبنيه في القانون 15-04 المتعلق بالتوقيع الإلكتروني والتصديق الإلكترونين.

ب- **ضوابط التشفير:** للتشفير ضوابطه وقواعده المتمثلة في الآتي[2]:

القاعدة الأولى: إباحة تشفير البيانات والمعلومات التي يتم تدوينها أو التعامل فيها من خلال الوسائط الإلكترونية وقد أحال مشروع قانون التجارة الإلكترونية المصري إلى اللائحة التنفيذية[3] الخاصة في شأن تحديد القواعد الخاصة بتشفير المستندات والبيانات الإلكترونية خاصة فيما يتعلق بتشفير التوقيع الإلكتروني وبطاقات الائتمان التي تتم نقلها أو تخزينها عبر وسائط إلكترونية.

القاعدة الثانية: احترام سرية البيانات المشفرة والاعتراف بحق أصحابها في الخصوصية لذلك جرم الاعتداء عليها، وهذه البيانات تعتبر خاصة بصاحبها لا يجوز خصم سريتها إلا بناء على تصريح كتابي منه[4].

القاعدة الثالثة: استخدام التشفير كوسيلة معتمد بها قانونيا في شأن تحرير البيانات والمعلومات بواسطة الجهات المختصة وفقا للائحة التنفيذية[5].

---

1 /من بينهم: سمير حامد عبد العزيز جمال في مرجع السابق، ص 220-221.

2 / هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، مرجع سابق، ص 591.

3 / اللائحة صدرت بالقرار رقم 09 لسنة 2005 الصادر في 15 ماي 2005، لمزيد من الاطلاع أنظر: محمد أمين الرومي، مرجع سابق، ص 31 و ما يليها.

4 / أما المشرع الجزائري فقد عاقب في نص المادة 68 من القانون رقم 15 -04 كل من يقوم بحيازة أو إنشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير قد تراوحت العقوبة بين تلك التالية للحرية و الغرامة المالية أو بإحدى تلك العقوبتين سواء أكان الفاعل شخصا طبيعيا أما إذا كان معنويا فإن الغرامة تضاعف حسب المادة 75 من نفس القانون.

5 / و قد أقر ذلك المشرع الجزائري في المادة 14 من القانون 15-04 على أن التأكد من مطابقة الآلية المؤقتة لإنشاء التوقيع الإلكتروني يتم من طرف الهيئة الوطنية المكلفة باعتماد آليات إنشاء التوقيع الإلكتروني، و سبب ذلك يكمن في أن عملية التشفير ترتبط بمعلومات هامة و سرية سواء تعلق الأمر بالتجارة الإلكترونية أو بالأسرار الخاصة بالأفراد أو بالدولة. أنظر: عبد الفتاح بيومي حجازي، التجارة الإلكترونية و حمايتها القانونية، المرجع السابق، ص 208.

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10

ثانيا: العلة من التشفير

تتسم المعاملات الإلكترونية بوجود طرف غير المتعاقدين قد يكون الغير مستخدم للشبكة، و قد تكون جهة أخرى لذلك كان لابد من وسيلة للمحافظة على سرية البيانات و حمايتها لكي لا يستطيع اي شخص الاطلاع عليها غير المتعاقدين أو من يصرح له قانونا بذلك فاستخدمت وسيلة التشفير بكتابة أو أرقام أو رموز معينة بدلا من الكتابة العادية بحيث يكون المفتاح الخاص **Privatekey** بالتشفير لا يعرفه إلا أطراف العملية التجارية- و أمن الشفرة يتبع حجم مفتاحها فكلما كان طويلا كلما زاد أمن الشفرة و الشفرات التجارية الحديثة يبلغ طولها 56 بت على الأقل[1].

المسألة الثانية: المصادقة على التوقيع الإلكتروني

ظهر التوقيع الإلكتروني ليؤكد هوية المتعاقدين ويعبر عن إرادتهم في التعاقد، وقد احاطت معظم التشريعات التوقيع الإلكتروني بالحجية في الإثبات إذا ما استوفى شروط معنية تعززه وتبعث الثقة فيه، ومن هذه الشروط ضرورة أن التوقيع مصادقا عليه، مما يستلزم ضرورة وجود طرف ثالث محايد يؤكد صدور الإرادة كمن نسبت غليه عن طريق الإصدار شهادة تتضمن التوقيع الإلكتروني للشخص المراد إثبات هويته، هذا الطرف الثالث سمي بمقدم خدمات التصديق الإلكتروني.

وعليه سوف نتطرق في هذه المسألة إلى مفهوم التصديق الإلكتروني ودور جهات التصديق في تأمين التوقيع الإلكتروني كما يلي:

أولا: مفهوم التصديق الإلكتروني

التصديق الإلكتروني يعرف على أنه « وسيلة أمنة للتحقق من صحة التوقيع أو المحرر حيث يتم نسبته إلى شخص أو كيان معين[2]ومن ثم فإنه وسيلة سلامة و تأمين التعامل عبر الأنترنت سواء من حيث مضمونه ومدخله و تاريخه و أطرافه[3] على التوقيع الإلكتروني و يعرفون بأنهم « جهة أو منظمة عامة أو خاصة مستقلة

1 / Lamy, Alain ben soussan la problématique Française : colloque du 13 Mai 1998 : commerce électrique.

2 / محمد حسين منصور، الإثبات الإلكتروني، دار الفكر الجامعين الإسكندرية، 2006 ص209.

3 / عرف قانون الأونيسترال النموذجي لسنة 2001 المتعلق بالتوقيعات الإلكترونية مقدم خدمات التصديق في نص المادة الثانية الفقرة(ه) بأنه « شخص يصدر شهادات و يجوز أن يقدم خدمات أخرى ذات الصلة بتوقيعات الإلكترونية» أما التوجيه الأوروبي رقم 93 لسنة 1999 فلقد عرف هذه الجهة في المادة 02 فقرة 11 بأنها:« كل شخص طبيعي أو معنوي يصدر شهادات توثيق التوقيع الإلكتروني، أو يتولى خدمات أخرى مرتبطة بالتوقيع الإلكتروني. أنظر: خالد ممدوح ابراهيم حجية البريد الإلكتروني في الإثبات، دار الفكر الجامعي، الإسكندرية 2010، ص 208- 209.

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10

محايدة تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الإلكترونية مصدرة بذلك شهادة إلكترونية. ونرمز لهذه الجهة باختصار برمز(PSC)

Prestataires de Services de Certification

تتدخل هذه الجهة بناء على طلب شخصين أو أكثر بهدف إنشاء و حفظ و إثبات الرسائل الإلكترونية[1]، أما عن المشرع الجزائري فإنه هو الآخر عرف بهذه الجهة و سماها بمؤدي خدمات التصديق[2] و بذلك إصداره قانونا يفصل فيه كل هاته المسائل و يشرحها و هو القانون رقم 15-04 الذي يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونين، بحيث أورد في نص المادة الثانية فقرة 12 من نفس القانون تعريفا لمؤدي خدمات التصديق و عرفه على أنه «كل شخص طبيعي أو معنوي يقوم بمنح شهاد تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني»[3].

ويعمل مقدمي خدمات التصديق على توثيق التوقيع الإلكتروني مصدره بذلك شهادة تبين بأن التوقيع الإلكتروني هو توقيع صحيح وصادر ممن نسب غليه، وأن يستوفي الشروط والضوابط المطلوبة فيه[4] كما تؤكد أن البيانات الموقع عليها هي بيانات صحيحة، ولم يتم التلاعب فيها سواء بالتعديل أو التغيير أو الحذف أو الإضافة وتسمى هذه الشهادة شهادة التصديق الإلكترونية[5].

1 / لزهر بن سعيد، النظام القانوني للعقود التجارة الإلكترونية، دار هومة، الجزائر 2012، ص 172.

2 / اعترف المشرع بمؤدي خدمات التصديق بداية في نص المادة 3 مكرر من المرسوم التنفيذي 162/07 الصادر في 30 ماي 2007 و المتعلق بنظام استغلال الشبكات بما فيها السلكية الكهربائية و على مختلف المواصلات السلكية و اللاسلكية يعدل و يتمم المرسوم التنفيذي رقم 01/ 123 المؤرخ في 09 مايو 2001 و كذا المادة 08 من القانون رقم 03/2000 الجريدة الرسمية العدد 48 لسنة 2000.

3/ الجديد في المصادقة الإلكترونية بالنسبة للتشريع الجزائري في استحداث ثلاث سلطات للتصديق الإلكتروني بموجب القانون 15- 04 السالف الذكر و فصل أحكامها في الباب الثالث عنونه بسلطات التصديق الإلكتروني تتمثل في السلطة الوطنية و السلطة الحكومية، و كذا السلطة الاقتصادية للتصديق الإلكتروني وحدد لكل واحدة من هذه السلطات مهام تتكامل فيما بينها تضمن ترقية استعمال التوقيع و التصديق الإلكترونين و تطورهما.

4 / خالد ممدوح ابراهيم، أمن المعلومات الإلكترونية، دار الجامعية، الإسكندرية، 2008، ص117.

5 / عرفها القانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001 بأنها« رسالة بيانات أو سجلا آخر يؤكدان الارتباط بين الموقع و بيانات إنشاء التوقيع.

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10

عرف المشرع الجزائري شهادة التصديق الإلكتروني في المادة 02 فقرة 07 من القانون 15-04 بأنها « وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني و الموقع»، و هي على نوعين شهادة المصادقة الإلكترونية العادية[1] و شهادة المصادقة الإلكترونية الموصوفة[2].

ثانيا: دور جهات التصديق الإلكتروني في تأمين التوقيع الإلكتروني

إن دور جهات التوثيق يتمثل في التأكد من صحة التوقيع الإلكتروني، و من سلامته، كما يتمثل في تحديد هوية المتعاملين في المعاملة الإلكترونية، ومن أهليتهم القانونية للتعامل و التعاقد، كما تعمل أيضا على التحقق من مضمون هذا التعامل وسلامته و حريته[3]، كما تقوم هذه الجهات بإصدار المفاتيح الإلكترونية سواء المفتاح الخاص الذي بمقتضاه يتم تشفير التعاملات الإلكترونية أو المفتاح العام الذي يتم بواسطته فك التشفير، بل و الأكثر من ذلك فإن من ضمن المهام التي تقوم بها جهات التصديق أيضا هو تعقب المواقع التجارية عبر الأنترنت، حيث تجرى عليها وعن جديتها فإذا تبين لها عدم أمن أحد المواقع فإنها تقوم بتوجيه رسائل تحضيرية للمتعاملين توضح فيها عدم مصادقة الموقع[4] و من ثم فإن هذه الجهات تقوم بدور فعال في ضمان التوقيعات الإلكترونية و الاعتراف بها قانونا.

كما تعتبر شهادة التصديق الإلكترونية أهم وسيلة تقدمها الجهات المختصة في إصدارها لتأمين المعاملة الإلكترونية بين المتعاملين، ذلك أنها تحتوي على البينات الصحيحة الموثقة من طرف هذه الجهة والمتعلقة بصاحب التوقيع الإلكتروني.

حيث بإمكانها التأكد من شخصية المرسل وتشهد بصحة البيانات المدونة بالمحرر وعدم قابليتها للتعديل، هذا من شأنه أن يمنح الأمان والثقة للمتعاملين عبر الأنترنت، نظرا لخطورة هذه الشهادة سواء كان ذلك من حيث طبيعة البيانات الشخصية والسرية التي تحتويها، أو من حيث حجيتها القانونية في الإثبات، حيث يجوز لصاحب الحق أن يحتج بهذه الشهادة في حالة التعدي على حق من حقوقه[5]

---

1 / أنظر المادة 2 ق 7 من القانون 15- 04.

2/ أنظر المادة 15 من القانون 15- 04.

3 / مصطفى أبي مندور موسى، الجوانب القانونية لخدمات التوثيق الإلكتروني، دار النهضة العربية، القاهرة، دون تاريخ السنة ، ص 23.

4 / ابراهيم الدسوقي أبو الليل، التوقيع الإلكتروني و مدى أهميته في الإثبات (دراسة مقارنة)، مجلة الحقوق، جامعة الكويت، العدد 03 سنة 2005، ص 125.

5 / و للإشارة فإن شهادات التصديق تتعد و تختلف بحسب استخداماتها و الغرض منها، فإلى جانب شهادة التصديق التوقيع الرقمي مثلا توجد شهادات مصادقة أخرى، مثل شهادة توثيق تاريخ الإصدار التي توثق تاريخ و وقت إصدار التوقيع الرقمي، حيث يقوم صاحب الشهادة بعد التوقيع عليها بإرسالها إلى جهة التوثيق، هذا و توجد أيضا شهادة الإذن و بمقتضاها يتم تقديم معلومات إضافية عن صاحبها مثل عمله و مؤهلاته، و

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10

المحور الثاني: الحماية الجنائية للتوقيع الإلكتروني

التوقيع الرقمي أو الإلكتروني هو عبارة عن جزء صغير مستقر من بيانات يضاف إلى رسالة إلكترونية كالبريد الإلكتروني أو العقد الإلكتروني[1] فمفهوم التوقيع الإلكتروني يعد مفهوما جديدا لحداثة

القوانين الصادرة بشأنه[2] ولكن هذه القوانين وإن كانت اشتملت على تعريفات متباينة للتوقيع الإلكتروني إلا أنها تنظر بنفس الأهمية إلى مسألة حماية هذه الوسيلة جنائيا لأنه أي التوقيع الإلكتروني يرتبط أساسا بالوسيلة التقنية المستعملة وبقدرتها على الحفاظ على سرية وأمن المعلومات من الأخطار المتمثلة في مسألة أمن وسرية البيانات على شبكة الأنترنت وتعرضها للاختراق والسطو والتعديل والتزوير، وعليه سوف نحاول توضيح صور هذه الحماية الجنائية للتوقيع الإلكتروني في التشريع الجزائري.

الحماية الجنائية للتوقيع الإلكتروني في القانون الجزائري

تماشيا مع التطور التكنولوجي في مجال الاتصالات و انتشار استخدام النظم المعلوماتية، أصدر المشرع الجزائري نصوص قانونية بموجب ق ع ج 15-04 تحت عنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات و الاستعمال للإعلام الآلي من خلاله جرم كل أنواع الاعتداءات التي تستهدف الدخول غير المشرع لأنظمة المعلوماتية تغيير أو اتلاف المعطيات محدد بذلك الأفعال و السلوكيات التي تدخل ضمن مجال هذا النوع الجديد من الجرائم و التي يمكن اعتبارها كحماية للتوقيع الإلكتروني باعتباره بيانات إلكترونية[3] و إن كانت حماية

التراخيص التي يملكها و من هنا تظهر أهمية هذه الشهادات، و مدى خطورة المعلومات التي تتضمنها و التي يعتمد عليه الغير و على أساسها يحدد تعاملاته. أنظر: خالد ممدوح ابراهيم، إبرام العقد الإلكتروني، دار الجامعة، مصر، 2007، ص 252.

1 / يونس عرب، التعاقد و الدفع الإلكتروني. تحديات النظاميين الضريبي و الجمركي، جزء من أوراق عمل برنامج الندوات المخصصة حول التجارة الكترونية، الخرطوم، معهد التدريب و الاصلاح القانوني 2002 م ص 02.

2 / قد أصبح اعتماد للتوقيع الإلكتروني ضرورة عالمية إذ سارعت معظم التشريعات إلى الاعتراف به ما بين منظميه في قوانين خاصة كما هو عليه الحال في التشريع الفرنسي- أو المصري، أو ضمن قانون التجارة الإلكترونية مثل التشريع التونسي- أو الأردني و اختلفت كذلك المصطلحات الواردة بشأنه فالبعض يسميه المستندات الإلكترونية مثل القانون الإماراتي، و البعض يسميها رسالة بيانات كقانون الأونيسترال النموذجي، و البعض الآخر يسميه بالإمضاء الإلكتروني كما ورد في التشريع التونسي، أما المصطلح الشائع الاستعمال فهو مصطلح التوقيع الالكتروني،انظر:يمينة حوحو، عقد البيع الإلكتروني في القانون الجزائري، دار بلقيس للنشر، الطبعة الاولى2016، ص 161.

3 / يعرف التوقيع الإلكتروني العادي في المادة 2/ ف من القانون15- 04 بأنه « بيانات إلكترونية في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق» في حين عرفت المادة 7 التوقيع الإلكتروني الموصوف بأنه:« التوقيع الإلكتروني هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات التالية:

- أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة.
- أن يرتبط بالموقع دون سواه.
- أن يمكن من تحديد هوية الموقع.

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10

عامة ضمن قانون العقوبات كمرحلة أولى بعد أن اعترف به أولا في القانون رقم 05- 10 المعدل و المتمم للقانون المدني، و لكن و نظرا للأهمية و المكانة التي يتمتع بها التوقيع الإلكتروني خصه المشرع بقانون خاصا به من حيث الأحكام التي تنظمه و كذا الحماية الجنائية المرتبة على مخالفة تلك الأحكام و ذلك من خلال سن المشرع للقانون رقم 15-04 المؤرخ في 01-02-2015[1] الذي يحدد القواعد العامة للتوقيع و التصديق الإلكترونين و هي خطوة هامة تبناها المشرع الجزائري لتنظيم التوقيع الإلكتروني و إفراده بحماية خاصة تتلائم طبيعته و أهميته. وهذا ما سوف نعرض له من خلال ما يلي:

أولا: الحماية الجنائية للتوقيع الإلكتروني في إطار قانون العقوبات الجزائري

قام المشرع الجزائري بتجريم كل لأنواع الاعتداءات التي تستهدف الدخول غير المشرع للأنظمة المعلوماتية، تغييرا أو اتلاف للمعطيات، محددا الأفعال والسلوكيات التي تدخل ضمن مجال هذا النوع الجديد من الجرائم والتي تضمنها القانون رقم 15-04 والتي يمكن حصرها في الآتي:

1- جريمة الدخول أو البقاء في المنظومة عن طريق الغش المادة 394 مكرر ق ع ج تقوم هذه الجريمة بمجرد الدخول غير المرخص به وعن طريق الغش إلى المنظومة المعلوماتية، سواء مس الدخول أو البقاء كل أو جزء من المنظومة، ويكفي إثبات المحاولة لتطبيق أحكام المادة، ولا يشترط لقيام هذه الجريمة الحاق أضرار بالمنظومة المعلوماتية.

2- جريمة إدخال المعلومات في منظومة المعالجة الآلية أو إزالة أو حذف أو تعديل معطيات المنظومة المعالجة الآتية عن طريق الغش المادة 394 مكرر تقوم هذه الجريمة بمجرد ارتكاب أحد الأفعال المذكورة أعلاه بغض النظر عن المجال المستهدف سواء كانت البرامج أو المعطيات أو قاعدة بيانات للتوقيع الإلكتروني.

3- جريمة القيام عمدا أو عن طريق الغش بتصميم، توفير نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية أخرى أو حيازة أو إفشاء أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى جرائم المعلوماتية، المادة 394 مكرر2 من ق ع ج ويلاحظ كل الجرائم هي جرائم عمدية وترتكب عن طريق الغش.

4- جريمة المشاركة ضمن جماعة أو في اتفاق لغرض ارتكاب احدى الجرائم المعلوماتية المادة 354 مكرر 5 ق ع من ق ع ج وتقوم بالانتماء أو الاشتراك في جماعة أو اتفاق.

- أن يكون مصمما بواسطة آلية مؤقتة خاصة بإنشاء التوقيع الإلكتروني.
- أن يكون مرتبطا بالبيانات الخاصة به بحيث يمكن الكشف عن التغيرات اللاحقة بهذه البيانات.
- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع.

1 / المادة 394 مكرر/1 تنص على أنه« يعاقب بالحبس من ستة أشهر إلى ثلاثة سنوات و بغرامة من 500,000 إلى 200,000 دج كل من دخل بطريق الغش معطيات في نظام المعالجة الآلية أو إزالة أو بطريق الغش المعطيات التي يتضمنها».

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10

5- جريمة الشروع في ارتكاب جرائم المعلوماتية المادة354 مكرر7 من ق ع ج و تكون العقوبة المقررة عن الشروع بطبيعة الحال هي نفس العقوبة المقررة لجريمة التامة[1].

وما يمكن الإشارة إليه من خلال هذه الخطوة الهامة في مسار المشرع الجزائري تبنيه الحماية الجنائية للبرامج المعلوماتية من خلال القانون 04-15اقتداءا بالمشرع الفرنسي. ، إلا أنه لم يتعرض إلى جل الجرائم التي نص عليها المشرع الفرنسي، وإن كانت على قدر بالغ من الأهمية كجريمة تزوير المستندات المعلوماتية و بالتالي تبقى المنظومة التشريعية الجنائية في الجزائر ناقصة من حيث اغفال تجريم الاعتداءات الواردة على منتجات الإعلام الآلي و خصوصا خلوها من نص تحرم تزوير المعلوماتي و ذلك رغم تجريمه للاعتداءات الواردة على الأنظمة المعلوماتية[2].

ثانيا: حماية التوقيع الإلكتروني في ظل القانون المتعلق بالتوقيع والتصديق الإلكترونين(15-04)

إن التوقيع الإلكتروني يمنع بدرجة عالية من الأمان الفني والقانوني، وبصورة تمنع التلاعب به والاعتداء عليه بأي شكل كان، لذلك حرص المشرع الجزائري على تضمين القانون 15-04 مجموعة من العقوبات الإدارية والمالية[3] والجزائية لكل يمس ببيانات التوقيع الإلكتروني بما يشكل جريمة في أحكام القانون السالف الذكر وسوف نكتفي بعرض الأحكام الجزائية لأنها محور اهتمامنا وموضوع دراستنا. وهي كالآتي:

نص المشرع الجزائري على مجموعة من العقوبات الجزائية في الفصل الثاني المعنون بـ أحكام جزائية في المواد 66 إلى 75 من القانون 15-04 سالف الذكر وهي:

1- يعاقب بالحبس من ثلاثة أشهر إلى 3 سنوات وبغرامة من عشرين ألف (20,000) إلى مائتين ألف دينار (200,000) أو بإحدى هاتين العقوبتين على جريمة الادعاء بإقرارات كاذبة للحصول على شهادة التصديق الإلكتروني الموصوفة[4].

2- يعاقب بالحبس من شهرين (2) إلى سنة (1) واحدة و بغرامة من مائتين ألف دينار(200,000) إلى مليون دينار (1,000,000)، أو بإحدى هاتين العقوبتين فقط على إحلال مؤدي خدمات التصديق

1 / الأرزاق بن عبد الله و أحمد عمراني، نظام المعلوماتية في القانون الجزائري واقع و آفاق المؤتمر السادس لجمعية المكتبات و المعلومات السعودية، المنفذ بمدينة الرياض بيئة المعلومات الأمنية للمفاهيم و التشريعات و التطبيقات المنعقد بمدينة الرياض خلال الفترة 21- 22 أفريل 210 ص 83.

2 / لسد الفراغ القانوني الذي عرفه المجال المعلوماتي بصدور قانون رقم 04-15، أصدر المشرع الجزائري قانون مكافحة الجرائم المعلوماتية تحت عنوان « القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها و هو القانون رقم 09-04 مؤرخ في 2009/08/05

3 / للاطلاع على العقوبات الإدارية و المالية المفروضة على مقدمي خدمات التصديق على التوقيع الإلكتروني. أنظر المواد 64-65 من القانون 15-04 السالف الذكر.

4 / أنظر المادة 66 من القانون 15-04.

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10

الإلكتروني بالتزام أعلام السلطة الاقتصادية بالتوقف عن النشاط في الآجال المحددة في مادتين 58-59 من هذا القانون[1].

3- يعاقب بالحبس من ثلاثة(3) أشهر إلى (7) سنوات وبغرامة من مليون دينار (1,000,000) إلى خمسة ملايين (5,000,000) أو بإحدى هاتين العقوبتين فقط، كل ما يقوم بحيازة أو إفساد أو استعمال أثناء توقيع الإلكتروني موصون خاصة بالغير[2].

4- يعاقب بالحبس من شهرين (2) إلى (3) سنوات وبغرامة من عشرين ألف دينار (20,000) إلى مائتين دينار (200,000) أو بإحدى هاتين العقوبتين فقط، كل ما يخلو عمدا بالالتزام تحديد هوية طالب شهادة تصديق الإلكتروني موصوفة[3].

5- يعاقب بالحبس من (3) أشهر إلى سنتين (2) وبغرامة من مائتين ألف دينار (200,000) إلى مليون دينار (1,000,000) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 42 من هذا القانون[4].

6- يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من مائتين ألف دينار (200,000) إلى مليون دينار (1,000,000) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 43 من هذا القانون[5].

7- يعاقب بالحبس من سنة (1) واحدة إلى ثلاث(3) سنوات وبغرامة من مائتين ألف دينار (200,000) إلى مليونين دينار (2000,000) أو بإحدى هاتين العقوبتين فقط كل من يؤدي خدمات التصديق الإلكتروني للجمهور دون ترخيص أو كل مؤدي خدمات التصديق الإلكتروني سيستأنف أو يواصل نشاطه بالرغم من سحب ترخيص تصادر التجهيزات التي تستعمل في ارتكاب الجريمة طبقا للتشريع المعمول به[6].

8- يعاقب بالحبس من ثلاثة(3) أشهر إلى سنتين (2) و بغرامة من عشرين ألف دج(20,000) إلى مائتين ألف دينار (200,000) أو بإحدى هاتين العقوبتين فقط، كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية اطلع عليها أثناء قيامه بالتدقيق[7].

---

1 / أنظر المادة 67 من القانون 15-04.

2 /أنظر المادة 68 من القانون 15 -04.

3 /أنظر المادة 69 من القانون 15- 04.

4 /أنظر المادة 70 من القانون 15 – 04.

5 / أنظر المادة 71 من القانون 15-04.

6 / أنظر المادة 72 من القانون 15-04.

7/ أنظر المادة 73 من القانون 15-04.

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10

9- يعاقب بغرامة من ألفي دينار(2000) إلى مائة دينار(200,000) كل شخص يستعمل بشهادته للتصديق لإلكتروني الموصوفة لغير الأغراض التي منحت لها[1].

10- يعاقب الشخص المعنوي الذي ارتكب إحدى الجرائم المنصوص عليها في هذا الفصل بغرامة تعادل الخمس(5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي[2].

من الواضح أن القانون15-04 يهدف إلى إرساء جو من الثقة و ضمان تأمين المبادلات على الإنترنت، و وضع المشرع ثلاثة مبادئ أساسية هي: التوثيق، السلامة، وعدم الإنكار بجعل التوقيع الإلكتروني موثقا وغير قابل للتزوير ولا يمكن إعادة استعماله[3].

خاتمة:

مما سبق وبعد تحليل موضوع الحماية الفنية والجزائية للتوقيع الإلكتروني يمكن الوصول الى النتائج والمقترحات الآتية:

– اهمية تدعيم الحماية الفنية للتوقيع الالكتروني باستعمال الطرق الحديثة للتشفير الإلكتروني وتحويل بياناته إلى رموز أو إشارات لحمايته وسريته وكذا إيكال التأكد من صحة التوقيع الإلكتروني والمصادقة عليه إلى جهة ثالثة غير الأطراف المتعاملة مهمتها إضفاء الثقة والأمان على المعاملات الإلكترونية.

– ضرورة توفير حماية جنائية لتدعيم الثقة في المعاملات الإلكترونية وخاصة حماية التوقيع الإلكتروني وذلك من خلال تجريم الاعتداء بكل أشكاله كالتزوير أو الدخول بطريق الغش إلى قاعدة البيانات التي تتعلق به أو جريمة صنع أو حيازة برنامج الإعداد التوقيع الإلكتروني.

– ضرورة تدعيم التصدي لكافة أشكال التحايل الإلكتروني والذي قد يظهر من جانب عدة أطراف كالتاجر أو العميل أو الغير وذلك لمواجهة كافة صور التحايل حماية للمصالح التي يقع عليه.

---

1 / أنظر المادة 74 من القانون 15-04.

2 / أنظر المادة 75 من القانون 15-04.

3 / ج. ب « حكومة سلال تعيد بعث مشاريع التصديق و التوقيع الإلكترونيين

http://yagool.dzLAr/article 2071.html

تاريخ الاطلاع في 2016/05/14.

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10

– صياغة نصوص جنائية لمواجهة الإجرام المستحدث بما فيها تلك النصوص التي تحمي التوقيع الإلكتروني وذلك حتى تسمح بدخول الصور الإجرامية المستحدثة مستقبلا في النص بما لا يمثل اعتداء على مبدأ الشرعية الجنائية خاصة وأن توقعات أهل الاختصاص تصب كلها في زيادة حجم الإجرام الإلكتروني مستقبلا.

وهنا تكمن الاهمية البالغة التي وقف عليها المشرع الجزائري في محاولته تبني قانون خاص بالتوقيع الإلكتروني و هو القانون 15-04 متفاديا مختلف الانتقادات التي وجهت له خاصة بعد أن أصبح التعامل بالرسائل الإلكترونية واقعا مفروضا على المشرع و المجتمع الجزائري معا، حيث حاول المشرع الجزائري من خلال قانون التوقيع و التصديق الإلكترونين الحفاظ على الحق في الخصوصية و ضمان سرية المعلومات حيث جرم العديد من الأفعال و قرر لها عقوبات رادعة و يعتبر هذا القانون خطوة مستحقة الإصدار قانون خاص بالتجارة الإلكترونية في الجزائر على غرار دول أشقاء سبقونا في هذا الحقل و لمواكبة التطور الحاصل في التشريعات السبيرانية في المجتمع الدولي.

قائمة المراجع

باللغة العربية:

1) يونس عرب، التعاقد والدفع الإلكتروني، تحديات النظامين الضريبي و الجمركي، جزء من أوراق عمل برنامج الندوات المتخصصة حول التجارة الإلكترونية، الخرطوم، معهد التدريب و الإصلاح القانوني، 2002.

2) يمينة حوحو، عقد البيع الإلكتروني في القانون الجزائري، دار بلقيس للنشر، الطبعة الأولى 2016.

3) عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، لكتاب الثاني الحماية الجنائية للتجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية مصر 2002.

4) هدى حامد قشقوش: الحماية الجنائية للتوقيع الإلكتروني، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية من الشريعة و القانون، المتعمد برعاية كلية الشريعة بجامعة الإمارات بالتعاون مع غرفة التجارة و الصناعة بدبي للفترة ما بين 10-13 ماي 2003.

5) عبد الفتاح بيومي حجازي، النظام القانوني للتوقيع الإلكتروني في النظم المقارنة، ط 1، دار الفكر العربي الإسكندرية 2005.

6) محمد أمين الرومي، النظام القانوني للتوقيع الإلكتروني، دار الكتب القانونية مصر 2008.

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10

7) الأرزاق بن عبد الله، و أحمد عمراني، نظام المعلوماتية في القانون الجزائري، واقع و آفاق، المؤتمر السادس لجمعية المكتبات و المعلومات السعودية المنعقد بمدينة الرياض بيئة المعلومات الأمنية للمفاهيم و التشريعات و التطبيقات المنعقد بمدينة الرياض خلال الفترة 21 و 22 أفريل 2010.

8) لزهر بن سعيد، النظام القانوني لعقود التجارة الإلكترونية، دار هومة الجزائر 2012.

9) ابراهيم الدسوقي أبو الليل، التوقيع الإلكتروني و مدى أهميته في الإثبات (دراسة مقارنة) مجلة الحقوق جامعة الكويت، العدد 03 سنة 2005.

10) عبد الفتاح البيومي حجازي، التجارة الإلكترونية و حمايتها القانونية، دار الفكر الجامعي، الإسكندرية، بدون سنة نشر.

11) سمير حامد عبد العزيز جمال، التعاقد عبر تقنيات الاتصال الحديث (دراسة مقارنة) دار النهضة العربية مصر 2001.

12) هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الأنترنت، دار النهضة العربية القاهرة2000.

13) خالد ممدوح ابراهيم، حجية البريد الإلكتروني في الإثبات، دار الفكر الجامعي، الإسكندرية 2010.

14) محمد حسين منصور، الإثبات الإلكتروني، دار الفكر الجامعي، الإسكندرية 2006.

15) خالد ممدوح ابراهيم، أمن المعلومات الإلكترونية، دار الجامعية الإسكندرية 2008.

16) مصطفى أبي مندور موسى، الجوانب القانونية الخدمات التوثيق الإلكتروني، دار النهضة العربية، القاهرة، دون تاريخ النشر.

17) خالد ممدوح ابراهيم، إبرام العقد الإلكتروني، الدار الجامعية، مصر، 2007.

باللغة الفرنسية:

1) Edward H, Ereeman J .d « Digital signature and Electronic contracts» Information systems security, 2004.

2) Lamy, AtainBensousancaproblématique Française : colloque du 13Mai 1998 : commerce eletronique .

تاريخ الإرسال: 2018/05/08 تاريخ القبول: 2018/08/07 تاريخ النشر:2018/12/10