آليات الحماية القانونية للتوقيع الالكتروني من جرائم التزوير الالكتروني في التشريع الجزائري

Mechanisms of Legal Protection of Electronic Signature From Digital Forgery Crimes in The Algerian Legislation

طالبة الدكتوراه/ وفاء صد راتي[1,2]
جامعة تبسة، (الجزائر)[1]
[2]**المؤلف المراسل:** wafase@hotmail.fr

تاريخ الاستلام: 2019/04/17 تاريخ القبول للنشر: 2020/01/29 تاريخ النشر: 2020/04/28

❖❖❖❖❖❖❖

مراجعة المقال: اللغة العربية: د./ محمد الصديق معوش (جامعة الوادي) اللغة الإنجليزية: د./ رحمة بوسحابة (جامعة معسكر)

ملخّص:

يمرّ العالم في الوقت الراهن بمرحلة انتقالية بين التعامل الورقي والتعامل الإلكتروني، وقد ظهر هذا التحول جليا في مجالات التبادل التجاري والعلاقات الاقتصادية، وفي ظل هذه التطورات الشديدة السرعة كان من الطبيعي أن يصاحبها وسائل جديدة تتناسب مع طبيعة المعلومات التي تجري عبر وسائط إلكترونية، ومن هنا ظهر التوقيع الالكتروني كبديل للتوقيع الكتابي.

وقد صاحب هذا التطوّر كثيرة الاعتداءات على هذا النوع من التوقيع، وذلك بتزويره، ما أدى إلى تضافر الجهود سواء على المستوى الدولي أو من خلال التشريعات الوطنية لإضفاء نوع من الأمان والثقة ووضع القواعد التي تكفل الاعتراف للتوقيع الالكتروني بالحجية الكاملة في الإثبات.

الكلمات المفتاحية: التوقيع الالكتروني؛ التزوير الالكتروني؛ التصديق الالكتروني؛ نظام التشفير؛ الحماية القانونية؛ الحماية الالكترونية.

Abstract:

Our world is currently undergoing a transition from paper data storage into ectronic format. Such transformation is evident in the field of trade and economic relations.Similarly these rapid developments are obviously accompanied by new means, commensurate with the nature of the information carried out through electronic media. Accrodingly, The electronic signature appears as an alternative to the manual one.

However, this signature has been a subject to many attacks, forfegering it, the situation that leads to unify efforts, either at the international level or through national legislation to provide a kind of security and confidence, as well as establishing rules that could ensure recognizing the full authoritative statement of the proof of this electronic signature.

Keys words: *electronic signature; electronic forgery; electronic certification; encryption system; legal protection Electronic protection.*

مقدّمة:

أدّى التطور الهائل الذي شهدته البشرية في الآونة الأخيرة إلى ظهور ثورة تكنولوجية أصبح العالم بموجبها قرية صغيرة، لاسيما بعد ظهور شبكة الإنترنت، ففي عصر الازدهار الالكتروني وفي زمن قيام الحكومات الالكترونية، تبدل نمط الحياة وتغيرت معه أشكال الأشياء وأنماطها، حيث تقف اليوم على أعتاب حضارات جديدة وثقافات جديدة زالت معها كل الحدود والحواجز، أحدثت ما يسمى بثورة المعلومات، وأنتجت مجتمعا جديدا هو مجتمع المعلوماتية، ورسمت معالم لمصطلحات جديدة في بيئة جديدة كالتحكيم الالكتروني، الحكومة الالكترونية، الإدارة الالكترونية.

وقد ألقى هذا التطور ظلاله على النشاط التجاري، ما أدى إلى ظهور طرق ووسائل حديثة في التعاملات، أهمها إبرام العقود على دعامات غير ورقية، ومنها جاءت فكرة التوقيع الالكتروني، الذي جاء لمواكبة هذه التطورات لاسيما أمام عجز التوقيع بمفهومه التقليدي على التكيف مع هذه النوعية الجديدة من العقود.

إلا أن هذا التطور لاسيما في مجال التجارة الالكترونية وما يحققه من مزايا، إلا أن له من السلبيات ولعل أهمها عدم توافر الأمان فيها، الأمر الذي مهد لمخترقي النظم المعلوماتية -في غياب الحماية الكافية- بالتطفل على البيانات الشخصية للأفراد وخاصة تزوير التوقيعات الالكترونية، واستخدام هذه البيانات أو المعلومات بطرق غير مشروعة. وهذا ما يثير مشكلة الأمن والخصوصية على شبكة الانترنت، وانعدام الثقة بهذه الشبكة، وكذا مشكلة تأمينه من أي اعتداء.

ونظرا للمشكلات القانونية التي يطرحها التوقيع الالكتروني والذي أصبح أمرا واقعا تتزايد أهميته يوما بعد يوم، ما يستلزم وضع آليات وضمانات يوفرها التوقيع الالكتروني للمتعاملين في البيئة الالكترونية. من هنا نطرح الإشكال الآتي: **ما هي الآليات والنصوص القانونية التي وضعها المشرع الجزائري لحماية وتأمين التوقيع الالكتروني من جريمة التزوير؟**

بغية الإجابة على هذه الإشكالية تم الاعتماد على المنهج التحليلي من خلال تحليل أغلب الجزئيات التي جاء بها الموضوع، كما تم الاعتماد على المنهج المقارن عند بيان ما تضمنته بعض الاتفاقيات والتشريعات المقارنة بما جاء في التشريع الجزائري.

وكان الهدف من هذه الدراسة هو محاولة تأصيل موضوع آليات حماية التوقيع الالكتروني من التزوير، في ظل غياب نصوص قانونية واضحة وصريحة بغية الوصول إلى دراسة نظرية واضحة ومتكاملة لهذا الموضوع، ومحاولة إيجاد حلول للمشكلات التي يثيرها هذا الموضوع الحساس والمتعلق بموضوع بمسالة مهمة تتعلق بالتزوير الالكتروني لا سيما في ظل النقص والقصور بشان هذه الجريمة في التشريع الجزائري.

وسنحاول الإجابة على هذه الإشكالية وفق الآتي:

المبحث الأول
مفهوم التوقيع الالكتروني محل الحماية

لقد نتج عن انتشار المعاملات الالكترونية في شتى المعاملات، ظهور وسائل حديثة في التعامل لا تتوافق مع فكرة التوقيع التقليدي، ذلك أن الأخير أصبح يمثل عقبة يصعب معها التكييف في المعاملات الالكترونية ما دفع إلى التوجه لبديل آخر يتمثل في التوقيع الالكتروني.

وسنحاول من خلال هذا المبحث التطرق إلى مفهوم التوقيع الالكتروني في المطلب الأول في حين نخصص المطلب الثاني لبيان صور التوقيع الالكتروني وحجيته في الإثبات.

المطلب الأول: تعريف التوقيع الالكتروني

من المستقر عليه في الفقه والقانون أن الكتابة لا تعد حجة بما دون فيها ما لم تقترن بالتوقيع، فالتوقيع مناط نسبة المحرر إلى موقعه، فهو بذلك ليس عنصرا من عناصر الدليل الكتابي فحسب وإنما هو بالدرجة الأولى تعبير عن إرادة الموقع في الالتزام بمضمون الورقة وإقراره لها ووسيلة لتمييز هوية الموقع (الزهرة، 2000، صفحة 813).

وقد اجتهدت أغلب التشريعات المقارنة والمنظمات الدولية والإقليمية في وضع تشريعات تنظيمية للتوقيع الالكتروني والمسائل المتعلقة به من خلال تنظيمه والاعتراف له بالحجية الكاملة في الإثبات.

وسنتطرق من خلال هذا المطلب إلى تعريف التوقيع الالكتروني وفقا للتشريعات والتوجهات الدولية، ثم إلى تعريفه وفقا للتشريعات الوطنية.

الفرع الأول: تعريف التوقيع الالكتروني وفقا للتشريعات الدولية

نظرا للمشكلات القانونية التي يطرحها التوقيع الالكتروني، والذي أصبح أمرا واقعا تتزايد أهميته يوما بعد يوم، خاصة في ظل انتشار وازدهار التجارة الالكترونية تضافرت الجهود الدولية لتنظيم هذا النوع من التوقيع بإصدار تشريعات وتوجيهات دولية، تضفي له نوعا من الأمان والثقة وتضع القواعد التي تكفل الاعتراف له بالحجية الكاملة في الإثبات.

وتصدت أكثر من منظمة لتعريف التوقيع الالكتروني سواء من خلال قوانين التجارة الالكترونية أو من خلال قوانين وضعت خصيصا للتوقيع الالكتروني، وسنحاول في المقام الاقتصار على منظمتين دوليتين هما: لجنة الأمم المتحدة لقانون التجارة الدولية المعروفة باليونسترال، والاتحاد الأوروبي كمثال لمنظمة إقليمية.

أولا: قانون اليونسترال النموذجي بشأن التجارة الالكترونية 1996

لقد اعترف قانون اليونسترال النموذجي بشأن التجارة الالكترونية (http://www.unictral.org، 2019)، بالتوقيع الالكتروني وسوى بينه وبين التوقيع التقليدي، وكانت الخطوة الأولى الفعلية لميلاد التوقيع الالكتروني تشريعيا، وقد عرف التوقيع الالكتروني في مادته السابعة بنصه على أنه: "عندما يشترط القانون وجود توقيع من شخص، يستوفي ذلك الشرط بالنسبة إلى رسالة البيانات إذا:

1- استخدمت طريقة لتعيين هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات،

2- كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشأت أو أبلغت من أجله رسالة البيانات، في ضوء كل الظروف كما في ذلك أي اتفاق متصل بالأمر".

ثانيا: قانون التوجيه الأوروبي رقم 1993/93 المتعلق بالتوقيع الالكتروني

لم تكن المجموعة الأوروبية بمنأى عن الاهتمام الدولي بتطوير القواعد القانونية لتتلاءم مع عصر المعلوماتية، بل العكس تماما، فقد أولت اهتماما خاصا للتنسيق بين التشريعات الداخلية الخاصة بالدول الأعضاء داخل السوق الأوروبية التي تعتمد بالدرجة الأولى على الثقة التي يوليها الأفراد للأمان المتوافر في عمليات التبادل الالكتروني، والتي ازدادت تطبيقاتها المرتبطة بالتوقيع الالكتروني بوما بعد يوم خاصة في ظل انتشار التجارة الالكترونية وازدهارها (راضية، 2012، صفحة 10).

وانطلاقا من هذا أصدر الاتحاد الأوروبي التوجيه رقم 1993/93 الصادر عن البرلمان الأوروبي في 13 ديسمبر 1993 المتعلق بالتوقيعات الالكترونية (http://www.Fs.dk/uk/acts/eu/pdf/eisgn-fi.pdf)، حيث جاء في نص المادة 02 أن: "التوقيع الالكتروني هو عبارة عن بيان أو معلومة معالجة الكترونيا، ترتبط منطقيا بمعلومات أو بيانات الكترونية أخرى –كرسالة أو محرر- والتي تصلح كوسيلة لتمييز الشخص وتحديد هويته".

ثالثا: قانون الأونسترال النموذجي الخاص بالتوقيعات الالكترونية لسنة 2001

جاء بهذا القانون لجنة الأمم المتحدة للقانون التجاري الدولي في دورتها الرابعة والثلاثين وهذا بتنظيم التوقيع الالكتروني الموثوق به، وقد عرفت المادة الثانية منه على تعريف التوقيع الالكتروني بأنه: "بيانات في شكل الكتروني مدرجة برسالة أو مضافة إليها أو مرتبطة بها منطقيا، بحيث يمكن أن تستخدم لبيان هوية الموقع بالنسبة إلى هذه الرسالة، ولبيان موافقته على المعلومات الواردة في الرسالة". (http://www.unictral.org).

والملاحظ على النص أعلاه أن قانون اليونسترال بشأن التوقيعات الالكترونية لم يقيد مفهوم التوقيع الالكتروني، فهذا النص يمكن أن يستوعب أي تكنولوجيا تظهر في المستقبل تفي بإنشاء توقيع الكتروني (المادة 03).

الفرع الثاني: تعريف التوقيع الالكتروني وفقا للتشريعات الوطنية

لم تكن التشريعات الوطنية التي نظمت البنية القانونية للتعاملات الالكترونية بمعزل عن التطور التكنولوجي والمعلوماتي، إذ شرعت العديد من الدول إلى تعريف التوقيع الالكتروني محاولة إزالة كل ما يواجه هذا المفهوم الجديد من مشكلات قانونية لاسيما في مجال الإثبات.

وسنحاول في هذا الصدد التطرق إلى بعض التشريعات التي تناولت مسألة التوقيع الالكتروني، ووضعت تعريفا له سواء ضمن قانون مستقل خاص به، أو من خلال تعديل نصوصها القانونية.

أولا: تعريف التوقيع الالكتروني في التشريع الفرنسي

نتيجة للتطور الحاصل في المعاملات الالكترونية من جهة والتزاماتها بالتوجيهات الأوروبية الخاصة بالتوقيع الالكتروني من جهة أخرى، وجد المشرع الفرنسي نفسه أمام ضرورة إدخال تعديلات على مواد القانون المدني الخاصة بالإثبات، وكان ذلك بموجب القانون رقم 2000-230 الصادر في 13 مارس 2000 المتعلق بتطوير قانون الإثبات للتكنولوجيات المعلومات والتوقيع الالكتروني (n°, 2000). حيث تم إضافة فقرة 4 للمادة 1316 من القانون المدني لتعتبر بذلك مقدمة لتعريف التوقيع الالكتروني، والتي تنص على أن: "التوقيع ضروري لإتمام عقد قانوني يكشف عن هوية الشخص الذي وضع التوقيع، كما يعلن عن رضا الأطراف بالالتزام الناجم عن هذا العقد، وإذا ما وضع التوقيع بواسطة موظف عام، فإن هذا التوقيع يضفي على العقد الطابع الرسمي (Article).

وقد ترك المشرع الفرنسي لمجلس الدولة وهذا بحسب المادة 1316-4 السابق ذكرها إصدار القرارات التي تبين الشروط القانونية والضوابط الفنية والتقنية اللازمة لتمتع التوقيع الالكتروني بالحجية في الإثبات، وأصدر مجلس الدولة الفرنسي القرار رقم 2001-272 (n° 2.-2. D., 2001)، وجاء هذا المرسوم ليحدد آليات تطبيق أحكام المادة 1316 فقرة 4 من القانون المدني، وقد ميز بين التوقيع العادي والتوقيع الالكتروني الآمن.

ثانيا: تعريف التوقيع الالكتروني في التشريع الجزائري

استخدم المشرع الجزائري مصطلح التوقيع الالكتروني لأول مرة بموجب نص المادة 2/372 من القانون المدني المعدل سنة 2005 والتي تنص على أنه: "... ويعتد بالتوقيع الالكتروني وفق الشروط المذكورة في المادة 323 مكرر1" (المدني).

ولم يضع المشرع الجزائري تعريفا للتوقيع الالكتروني، بل اعترف بحجية هذا الأخير رابطا بذلك هذه الأخيرة بتوفر نفس الشروط المتطلبة في الكتابة العادية، ليتدخل بعد ذلك بموجب المرسوم التنفيذي 07-162 (المرسوم التنفيذي رقم162-07) ليميز بين التوقيع الالكتروني العادي والتوقيع الالكتروني المؤمن وذلك بموجب المادة 3 مكرر. وهذا بقولها إن: "... التوقيع الالكتروني المؤمن هو توقيع الكتروني يفي بالمتطلبات الآتية: يكون خاصا بالموقع، يتم بوسائل يمكن أن يحتفظ بها الموقع تحت مراقبته الحضرية يضمن مع الفعل المرتبط به صلة بحيث يكون كل تعديل لاحق للفعل قابلا للكشف عنه".

وبصدور القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436هـ الموافق لـ 01 فبراير سنة 2015م الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين (القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436هـ الموافق لـ 01 فبراير سنة 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين 6، 2015)، تم وضع تعريف للتوقيع الالكتروني وذلك من خلال نص المادة 1/2 وذلك بقولها: "التوقيع الالكتروني بيانات في شكل الكتروني، مرفقة ومرتبطة منطقيا ببيانات الكترونية أخرى، تستعمل كوسيلة توثيق (القانون 04/15)".

ولم يحدّد المشرع الجزائري صورا للتوقيع الالكتروني، بل اكتفى بأن يكون التوقيع في شكل الكتروني فقط أيا كان هذا الشكل، وقد أحسن فعلا كونه فتح المجال أمام الاعتراف بجميع صور التواقيع الالكترونية التي تتمتع بالثقة الكافية وتحقيق وظائف التوقيع هذا من جهة، ومن جهة ثانية هناك نظام مزدوج للتوقيع الالكتروني، العادي والموصوف، هذا الأخير الذي يتمتع بكافة المزايا التي تتمتع بها التوقيع التقليدي (المادة 8 من القانون 04/15 المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني)، أما التوقيع الالكتروني فيشبه تعريف التوجيه الأوروبي بشأن التوقيعات الالكتروني (بوكر، صفحة 67).

الفرع الثالث: خصائص التوقيع الالكتروني

يتمتع التوقيع الالكتروني بخصائص منفردة تميزه، تتمثل في:

1- إن التوقيع الالكتروني يتكون من عناصر متفردة وسمات خاصة بالموقع تتخذ شكل أرقام أو حروف أو إشارات أو غيرها (مسعودي يوسف، أرجيلوس رحاب، 2017، صفحة 84). وعليه فلا يشترط في التوقيع الالكتروني صورة معينة، المهم أن يكون ذا طابع منفرد يسمح بتمييز صاحب التوقيع وتحديد هويته وإظهار رغبته في إقرار العمل القانوني والرضا بمضمونه (العبودي، 2010، صفحة 149)،

2- يحدد التوقيع الالكتروني شخصية الموقع وتميزه ويعبر عن رضاه بمضمون المحرر. (العبيدي، 2008، صفحة 147)،

3- التوقيع الالكتروني يتصل برسالة الكترونية وهو عبارة عن معلومات يتم إنشاؤها أو إرسالها أو تسليمها أو تخزينها بوسيلة الكترونية،

4- يحقق التوقيع الالكتروني الأمان والخصوصية بالنسبة للمتعاملين والسرية في نسبته للموقع من خلال إمكانية تحديد هوية الموقع، ومن ثم حماية المؤسسات من عمليات تزوير التوقيعات (بوكر، 2016، صفحة 69).

واستنادا إلى هذه الخصائص توجد عدة فروق جوهرية بين التوقيع الالكتروني والتوقيع التقليدي نوردها فيما يلي:

1- إن الدعامة الأساسية للتوقيع التقليدي هي الورقة أمام الدعامة التي يرتكز عليها التوقيع الالكتروني هي دعامة الكترونية كالقرص المرن أو المضغوط (بوكر، 2016، صفحة 69)،

2- إن التوقيع التقليدي عبارة عن رسم يقوم به الشخص بمعنى أنه فن وليس علما ومن هنا يمكن تزويره، أما التوقيع الالكتروني فهو علم وليس فنا ويصعب تزويره، بحيث يتم التوقيع الالكتروني بواسطة برامج كمبيوتر خاصة لهذه الغاية. (مسعودي يوسف، أرجيلوس رحاب، 2017، صفحة 84)،

3- إن تقليد أو تزوير التوقيع التقليدي من قبل الغير، لا يفرض على صاحبه عند اكتشاف التقليد أو التزوير تغيير شكل توقيعه، بعكس صاحب التوقيع الالكتروني، إذ يجب عليه تغيير توقيعه إن اكتشف توصل الغير إلى المنظومة التي تنشئه (ريضي ع.، القواعد الخاصة للتوقيع الالكتروني، 2018، صفحة 86)،

4- التوقيع التقليدي يقوم بوظيفتين، فهو يحدد هوية الشخص الموقع ويعد دليلا على الحضور المادي أثناء التوقيع، أما التوقيع الالكتروني فوظائفه تنحصر في أنه يحدد هوية الشخص الموقع ويحقق الأمان والثقة في صحة التوقيع ونسبه لصاحبه ويمنح كذلك صفة المحرر الأصلي للمستند مما يجعل هذا الأخير دليلا للإثبات (مبروك، 2009).

المطلب الثاني: صور التوقيع الالكتروني وحجيته في الإثبات

ظهرت العديد من الصور التي يتخذها التوقيع الالكتروني، وهي تختلف تبعا لاختلاف الطريقة التي يتم بها، كما تتباين فيما بينها من حيث درجة الثقة والأمان ومستوى ما تقدمه من ضمان بحسب الوسيلة التقنية المستخدمة والإجراءات المتبعة في إصداره وتأمينه.

وسنحاول في هذا الصدد بيان أهم هذه الصور في الفرع الأول، لنعرج في الفرع الثاني إلى حجية التوقيع الالكتروني في الإثبات.

الفرع الأول: صور التوقيع الالكتروني

إن الحديث عن التوقيع لا يعني الحديث عن توقيع يأخذ صورة واحدة، فكما تختلف أشكال التوقيع التقليدي بين توقيع بالإمضاء، وتوقيع بالختم، وتوقيع ببصمة الأصبع، فإن للتوقيع الالكتروني أشكالا مختلفة بين توقيع رقمي، وبيومتري، وتوقيع عن طريق استخدام بطاقات الدفع الالكتروني وتوقيع بالقلم الالكتروني، وسنحاول بيان بعضها على النحو الآتي:

أولا: التوقيع الرقمي

يعد التوقيع الالكتروني من أوسع أنواع التوقيع الالكتروني وأكثرها استخداما في إبرام التصرفات القانونية عبر الوسائط الالكترونية نظرا لطابع الأمان والثقة التي يوفرهما، وحاز على اعتراف وثقة العديد من الدول بشكل عام والشركات والبنوك بشكل خاص.

ويعرف التوقيع الرقمي على أنه: بيان أو معلومة يتصل بمنظومة بيانات أخرى أو صياغة منظومة في صورة شيفرة (كود)، والذي يسمح للمرسل إليه إثبات مصدرها والتأكد من سلامة مضمونها، وتأمينها ضد أي تعديل أو تخريف".

ويتم الحصول على التوقيع الالكتروني الرقمي عن طريق التشفير، وذلك بتحويل المحرر المكتوب والتوقيع الوارد عليه من نمط الكتابة العادية إلى معادلة رياضية، وذلك باستخدام مفاتيح سرية وطرق حسابية لوغاريتمية، ومؤدى ذلك تحويل المستند الالكتروني من صورته المقروءة والمفهومة إلى صورة رسالة رقمية غير مقروءة وغير مفهومة، ولا يكون بمقدور أي شخص إعادة هذه المعادلة اللوغارتمية إلى صورتها المقروءة إلا الشخص الذي لديه المعادلة الخاصة بذلك، والتي تتمثل في المفتاح، فالشخص المالك لمفتاح التشفير هو الذي يمكنه فكه (سليمان، 2000، صفحة 276،266).

ولا يمكن فهم التوقيع الالكتروني الرقمي فهما جيدا دون التطرق إلى نظام التشفير، إذ أن التوقيع بالمفاتيح العمومية والخصوصية يرتكز بصفة أساسية على وسائل التشفير كآلية تقنية لحماية التوقيع الالكتروني، والتي سنحاول تفصيلها وبيانها أكثر في المبحث الثاني من هذه الدراسة.

ثانيا: التوقيع بالقلم الالكتروني

من بين أشكال التوقيع الالكتروني التي يمكن استخدامها في توثيق التصرفات القانونية التي يتم إبرامها على الوسائط الالكترونية، التوقيع باستخدام قلم خاص، يعرف بالقلم الالكتروني، وهو عبارة عن قلم الكتروني حساس يمكنه الكتابة على شاشة الحاسوب عن طريق برنامج معلوماتي يتيح التقاط التوقيع والتحقق من صحته حيث يتلقى البرنامج المثبت على قاعدة بيانات الحاسوب، بيانات المستخدم عن طريق بطاقة تحقيق هوية الكترونية خاصة تحتوي على بيانات كاملة عن هذا الشخص (راضية، 2012، صفحة 44).

ثم يظهر بعد ذلك بعض التعليمات على شاشة الحاسوب ليتبعها المستخدم حتى تظهر رسالة على الشاشة تطلب من المستخدم كتابة توقيعه باستخدام القلم الالكتروني داخل مربع يعرض على الشاشة، وعندما يقوم المستخدم بتحريك القلم على الشاشة وكتابة توقيعه، يلتقط البرنامج حركة اليد ويظهر التوقيع مكتوبا على الشاشة بسماته الخاصة من حيث حجم وشكل الحروف والمنحنيات والدوائر، وغيرها، ثم يظهر للمستخدم ثلاثة مفاتيح للموافقة على شكل التوقيع، والثاني لإعادة المحاولة، والثالث لإلغاء التوقيع، وعندما يضغط المستخدم على أيقونة قبول التوقيع يقوم الحاسوب بتجميع البيانات الخاصة بالمستخدم الموقع ويدمجها مع شكل التوقيع الموافق عليه ثم يقوم بتشفير جميع هذه البيانات والاحتفاظ بها على نحو يتيح استرجاعها واستخدامها عند الضرورة (المرسوم التنفيذي رقم 162-07) (ريضي ع.، لقواعد الخاصة للتوقيع الالكتروني، 2018).

وبالرغم من إيجابية هذا الشكل من التوقيع المتمثلة في المرونة وسهولة الاستعمال بتحويل التوقيع اليدوي إلى الكتروني من خلال أنظمة المعلومات، إلا أن هذا الشكل لا يتمتع بدرجة عالية من الأمان، إذ أن المرسل إليه يستطيع أن يحتفظ بنسخة من التوقيع ويعيد لصقها على أي مستند الكتروني مدعيا أن واضعها هو صاحب التوقيع الفعلي.

ثالثا: التوقيع البيومتري

يقوم هذا النظام بالاعتماد على الصفات والخواص الفيزيائية والطبيعة والسلوكية للإنسان والتي من المفروض والطبيعي أن تختلف من شخص لآخر، ومن هذه الخواص بصمة الأصبع ومسح العين أو ما يعرف ببصمات القزحية وخواص اليد وبصمات أو نبرة الصوت، ويتم تخزين هذه الخواص في الحساب وذلك بطريقة التشفير، ويعاد حل هذا التشفير للتأكد من صحة التوقيع (بلال، 2017، صفحة 126).

ولما كانت الخواص المميزة لكل شخص تختلف عن تلك التي تميز غيره، فإن التوقيع الخاص بالخواص الذاتية -التوقيع البيومتري- يعد طريقة موثوقا بها لقدرته على تحديد الشخص مما يسمح باستخدامه في التوقيع التصرفات القانونية المبرمة عبر الانترنت (الحميد، 2001، صفحة 61).

ولقد طبق المشرع الجزائري هذا النمط من التوقيع، وهذا بغية الاستفادة من هذه التقنية لما تنطوي عليه من سمات محددة لهوية الموقع بدقة، وذلك من خلال إصدار قرار مؤرخ في 19 جويلية

2010 والمتضمن إصدار جواز السفر وبطاقة التعريف البيومتريين، وهذا استجابة للمنظمة العالمية للطيران التي دعت دول العالم إلى إصدار جواز سفر بيومتري (يوسف، 2013، صفحة 250).

ويؤخذ على هذا النوع من التوقيع أنه بالرغم من الدقة والأمان والثقة المتوافرة فيه، إلا إنه ليس بعيدا عن التزوير، فيمكن أن تخضع الذبذبات الحاملة للصوت أو صورة بصمة الأصبع للنسخ وإعادة الاستعمال بالإضافة إلى إمكانية إدخال تعديلات عليها، كذلك الشأن لبصمة العين، فيمكن تزويرها بتقليدها عن طريق بعض أنواع العدسات اللاصقة والتي تحمل نفس اللون والشكل والخصائص المخزنة على الحساب الآلي، لاسيما في ظل التطور التقني المذهل في عالم الالكترونيات (الحميد، 2001، صفحة 61).

الفرع الثاني: حجية التوقيع الالكتروني في مجال الإثبات

ترتبط حجية التوقيع الالكتروني باستيفائه للشروط اللازمة للاعتداد به كتوقيع كامل، ولهذا بادرت الدول إلى تضمين نصوصها والشريعة المنظمة للتوقيع الالكترونية قوة ثبوتية لهذا الأخير تعادل تلك الممنوحة للتوقيع الالكتروني بوضعها أحكاما خاصة بحجيته قاطعة كل جدل حول ذلك.

وانطلاقا من هذا سنحاول بيان شروط حجية التوقيع الالكتروني في التشريع الجزائري وكذا عرض بعض نصوص التشريعات المختلفة التي نظمت التوقيع الالكتروني وأقرت بحجيته.

أولا: شروط حجية التوقيع الالكتروني في التشريع الجزائري

لقد ساوى المشرع الجزائري -من خلال القانون المدني الجزائري- في الحجية بين التوقيع الالكتروني والتوقيع التقليدي، حيث نصت المادة 2/327 من القانون المدني على أنه: "يعتد بالتوقيع الالكتروني وفقا للشروط المذكورة في المادة 323 مكرر 1".وتتمثل هذه الشروط في إمكانية التأكد من هوية الشخص الذي أصدر التوقيع وأن يكون هذا التوقيع معدا في ظروف تضمن سلامته.

وبالرجوع إلى القانون 04/15 المتعلق بالتوقيع والتصديق الالكتروني، نجد أن المشرع الجزائري قد ميز بين التوقيع البسيط والتوقيع الالكتروني الموصوف، حيث أقر صراحة حجية توقيع هذا الأخير مساويا بينه وبين التوقيع التقليدي طبقا لنص المادة 08 من هذا القانون والتي تنص على أنه: "يعتبر التوقيع الالكتروني الموصوف وحده مماثلا للتوقيع المكتوب، سواء كان لشخص طبيعي أو معنوي". وحددت المادة 07 من نفس القانون الشروط الواجب توافرها حتى يكون التوقيع الالكتروني موصوفا والتي تتمثل في:

1- أن ينشأ التوقيع على أساس شهادة تصديق الكتروني موصوفة حيث ميز المشرع الجزائري بين شهادة التصديق الالكتروني البسيطة وشهادة التصديق الالكتروني الموصوفة وهذا من خلال المادة 2 في فقرتها 7 والمادة 15، وعرف الأولى بأنها عبارة عن وثيقة في شكل الكتروني تثبت الصلة بين بيانات التحقق من التوقيع الالكتروني والموقع، أما شهادة التصديق الالكتروني الموصوفة فقد نظمها من حيث البيانات التي يجب أن يحتويها كأن يمنح من قبل طرف ثالثا موثوق أو من قبل مؤدي خدمات تصديق الكتروني (بوكر، 2016، صفحة 72).

2- أن يرتبط بالموقع دون سواء و يمكن من تحديد هويته حتى يكون التوقيع الالكتروني توقيعا موصوفا فيتطلب أن يميز الشخص موقع المستند الالكتروني عن غيره،

3- أن يكون التوقيع مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الالكتروني،

4- أن يكون منشأ بواسطة وسائل دعمت التحكم الحصري للموقع وهذا ما أطلق علها المشرع ببيانات إنشاء التوقيع الالكتروني،

5- أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بها.

ثانيا: حجية التوقيع الالكتروني في التشريعات المقارنة

لقد أكد المشرع الفرنسي حجية التوقيع الالكتروني في الإثبات، شريطة أن يستوفي الشرط المحددة في المادة 4/1316 من القانون المدني، وكذا أحكام المرسوم 2001-272 -السابق ذكرهما- والتي تقتضي بأنه حتى يؤدي التوقيع الالكتروني وظيفته في إثبات ما ورد في مضمون العقد،لا بد من يحدد هوية الموقع ويميزه عن غيره، فضلا عن ارتباطه بالعقد على نحو لا يمكن فصله، وأن يعبر عن إرادته في قبوله الالتزام بمضمون العقد.

وفضلا عن الشروط السابقة، استلزم المرسوم 2001-272 المحدد لآليات تطبيق أحكام 4/1316 من القانون المدني بموجب المادة 02 أن ينشأ التوقيع بواسطة وسائل يمكن الاحتفاظ بها تحت سيطرة الموقع وحده دون غيره، مع وضع الفقرة الأخيرة من المادة 4/1316 من القانون المدني.

كما اعترف المشرع المصري بوجود التوقيع الالكتروني ومنحته الحجية القانونية في الإثبات وهذا من خلال القانون 15 لسنة 2004 (15-04 القانون، 2004). حيث نصت المادة 14 منه على أنه: "للتوقيع الالكتروني في نطاق المعاملات التجارية والمدنية ذات الحجية المقررة للتوقيعات في أحكام قانون الإثبات في المواد المدنية والتجارية، إذا روعي في إنشائه وإتمامه الشروط المنصوص عليه في هذا القانون والضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون".

وتتمثل هذه الشروط والتي حددتها المادة 18 من هذا القانون في:

1- ارتباط التوقيع الالكتروني بالموقع وحده دون غيره،

2- سيطرة الموقع دون غيره على الوسيط الالكتروني،

3- إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الالكتروني أو التوقيع الالكتروني.

ويتضح من خلال النصوص السابقة أن التشريعات قد ساوت في الحجية ما بين التوقيع الالكتروني والتوقيع التقليدي، غير أن هذه الحجية ليست مطلقة بل مقيدة بضرورة توافر شروط وضوابط فنية وتقنية معينة.

المبحث الثاني
مظاهر حماية التوقيع الالكتروني من التزوير

يعتبر التوقيع الالكتروني العنصر الرئيسي الذي تقوم عليه إجراءات التجارة الالكترونية كونه مرتبطا بتوثيق التصرفات القانونية الالكترونية وتحديد هوية المرسل والمستقبل، والتأكد من صحة البيانات، وإزاء هذه الأهمية بات من الضروري وجود حماية جنائية له ضد كل تصرف يهدده، بالاعتداء أو الضرر. ولعل من أكثر الجرائم تهديدا للتوقيع الالكتروني جريمة تزوير التوقيع الالكتروني، وقد عالجت ذلك تشريعات وقوانين الدول، ليس هذا فقط بل وحفاظا على الثقة والأمان في المعاملات الالكترونية وحمايتها من مخاطر القرصنة ثم استخدام آليات تقنية حماية للمعلومات المرسلة عبر الانترنت حفاظا على الأمن القانوني والمعلوماتي.

وسنحاول بيان هذه الآليات والضمانات في المطلبين المواليين:

المطلب الأول: الحماية الجنائية للتوقيع الالكتروني من جريمة التزوير

مع تزايد المعاملات الالكترونية على المستوى المحلي والعالمي، والذي جاء نتيجة التطور المذهل في استعمال التكنولوجيا، كان من الضروري توفير الحماية القانونية والتشريعية لهذه المعلومات. فالقاعدة العامة تنص على أن التوقيع الالكتروني الذي لا يتمتع بالحجية في الإثبات ليس محلا للتزوير، بينما التوقيع الالكتروني المتمتع بالحجية يقع محلا للتزوير، وعليه فالحجية في الإثبات شرط لحصول التوقيع على الحماية الجنائية.

وتعد جريمة تزوير التوقيع أحد أهم الجرائم التي يمكن أن تقع على التوقيع الالكتروني والتي تؤدي إلى إهدار الثقة في المعاملات الالكترونية، ما دفع التشريعات والقوانين في دول العالم إلى حماية التوقيع الالكتروني من هذا الشكل من أشكال الغش المعلوماتي، وهذا ما سنوضحه فيما يلي:

الفرع الأول: مفهوم جريمة تزوير التوقيع الالكتروني

نتيجة لظهور فكرة التوقيع الالكتروني والحاجة للحماية الجنائية لهذا التوقيع نص المشرع في بعض التشريعات على صور مستحدثة لحماية الاعتداء عليه، لكنها انقسمت اتجاه التزوير الذي يقع في مجال المعلوماتية، حيث يرى فريق من الفقه عدم إمكانية تطبيق النصوص التقليدية على جرائم التزوير الالكتروني، في حين يرى البعض الآخر إمكانية تطبيقها وفقا للمفهوم السائد والمستقر للتزوير الالكتروني، ولابد من وضع تشريع نصوص خاصة بجرائم التزوير التي تقع في البيئة الالكترونية.

وسنحاول في هذا الصدد بيان مفهوم جريمة تزوير التوقيع الالكتروني وبيان أركانها فيما يلي:

أولا: تعريف جريمة تزوير التوقيع الالكتروني

التزوير في مفهوم قانون العقوبات –هو تغيير الحقيقة بقصد الغش ويكون بإحدى الطرق المقررة قانونا في محرر يحميه القانون (قشقوش، 2003)، ويعد من أخطر الجرائم التي تخل بالثقة الواجب توافرها في المحررات.

ولم يضع المشرع الجزائري تعريفا محددا لجريمة التزوير في المحررات ولم يقم بتحديد أركانها وإنما اكتفى بتحديد الطرق التي يقع بها، تاركا هذه المهمة للفقه والقضاء. ويعتبر تغيير الحقيقة جوهر التزوير، فلا يتصور وقوع التغيير إلا بإبدال الحقيقة بما يغايرها فإذا انعدم تغيير الحقيقة لا تقوم جريمة التزوير.

والتزوير قد يكون ماديا أو معنويا، حيث يقع التزوير المادي بوسيلة مادية يترتب عنها أثار في مادة المحرر أو في شكله، أما التزوير المعنوي فهو الذي يقع بتغيير الحقيقة دون أن يترك أثرا يدركه الحس، قد يقع التزوير المادي وقت أو بعد إنشاء المحرر، بينما التزوير المعنوي لا يقع إلا وقت إنشاء المحرر (الجنبيهي.، 2006، صفحة 98).

كما عرف التزوير الالكتروني بأنه ذلك التزوير الذي ينصب على مخرجات الحاسب الآلي، أي البيانات والمعلومات الخارجة منه بشرط أن تطبع على داعمة مكتوبة أو مسجلة، أي يكون لها كيان مادي يمكن إدراكه، ولم يتم تغيير الحقيقة دون طباعة، وذلك أمر وارد، فلا يمكن أن يطلق عليه تزوير (حجازي، 2002، صفحة 164).

وذهبت الغالبية العظمى من الفقه القانوني إلى عدم انطباق نصوص التزوير التقليدية على التعديل أو التغيير الواقع على المعطيات والبيانات المخزنة بشكل غير مرئي كونها بيانات الالكترونية مستندين في ذلك إلى حجة عدم إمكانية القراءة البصرية لمحتويات المحرر وانتقاء الكتابة.

ولم يتناول كل من قانون العقوبات الجزائري وكذا القانون 04/15 جريمة التزوير الالكتروني (المادة23)، مما يطرح إشكالا حول مدى إمكانية تطبيق أركان جريمة التزوير التقليدي على جريمة تزوير التوقيع الالكتروني، أم أنها تعتبر صورة من صور جرائم المعالجة الآلية لنظم المعطيات المنصوص عليها في قانون العقوبات ؟.

ثانيا: أركان جريمة تزوير التوقيع الالكتروني

سنحاول دراسة الركن المادي لجريمة التزوير ثم الركن المعنوي مع بيان مدى انطباق هذه الأركان على جريمة تزوير التوقيع الالكتروني:

أ- الركن المادي في جريمة تزوير التوقيع الالكتروني

الركن المادي في جريمة تزوير التوقيع الالكتروني لا يختلف عن الركن المادي في جريمة التزوير التقليدية من حيث عناصره، فالركن المادي يقتضي عنصرين: العنصر الأول أن يتم تغيير الحقيقة بإحدى الطرق المنصوص عليها قانونا (محبوب، 2013، صفحة 31)، أما العنصر الثاني هو ضرورة توافر الضرر الذي لا يكتمل الركن المادي إلا به، فيشترط تحقق الضرر للغير، وهذا الضرر قد يكون ماديا كخسارة مادية المجني عليه وأيضا قد يكون أدبيا يفقدان الثقة في المعاملات في المجتمع عموما. (قشقوش، 2003، صفحة 583) ولقد حددت المواد 214 إلى 216 من قانون العقوبات طرق التزوير المادي والمعنوي.

.و قد اعتمد المشرع على الكتابة في الشكل الالكتروني ضمن وسائل الإثبات المدني وكذا التوقيع الالكتروني، ومن ثم يتصور أن يقع التلاعب أو التزوير على التوقيع الالكتروني بحيث يمكن للقراصنة اختراق نظم المعلوماتية، وفك شفرته واستخدامه دون موافقة صاحبه، أو نقل إمضاء الشخص على

الأوراق المسحوبة على الحاسب الآلي وتزويرها دون علم ورضا صاحبه خاصة في التعاملات الشبكية (مشري، 2017، صفحة 130).

لكن هناك من يرى أن التوقيع الالكتروني عبارة عن مخرجات ليست ورقية بل الالكترونية تحتوي مجموعة من الرموز أو الأرقام تتضمن علامة مميزة لصاحبها في مجملها، وهي بذلك تعد بيانات تتضمن معلومات تنشأ أو تندمج أو تخزن بوسيلة الالكترونية أو رقمية باعتبارها ومضات كهرومغناطيسية ذات طابع معنوي، وعليه فكل تزوير ينصب على هذه البيانات هو من قبيل التزوير المعنوي وليس تزويرا ماديا (القادر، 2000، صفحة 20).

ومهما يكن من أمر فإن مناط التزوير سواء تعلق الأمر بتوقيع تقليدي أو توقيع الالكتروني فإن الأمر يتم بطريقة مختلفة، إذ أن التوقيع الالكتروني لا يمكن تقليده، وإنما يمكن استخدامه دون علم مالكه كونه يتم بواسطة منظومة الكترونية، تتخذ شكل حروف أو أرقام أو رموز أو غيرها، فيما يتم تزوير التوقيع التقليدي بتقليد توقيع شخص آخر، وذلك لأن توقيع المقلد لا يمكن أن يكون بذات خواص التوقيع الأصلي وبالتالي لا يكون متماثلا معه، ومن ثم فجريمة تزوير التوقيع التقليدي تختلف عن جريمة التوقيع الالكتروني، سواء في طريقة التزوير أو في أسلوب اكتشافه، فالكشف عن التوقيع المزور تكون عن طريق المضاهاة، في حين لا يمكن استخدام هذه الطريقة في اكتشاف تزوير توقيع على محرر الكتروني (مشري، 2017، صفحة 132).

ب- الركن المعنوي لجريمة تزوير التوقيع الالكتروني

تعدّ جريمة التزوير بصفة عامة من الجرائم العمدية التي تتطلب قصدا جنائيا عاما وقصدا جنائيا خاصا، فلا يكفي القصد العام الذي يقوم على علم المتهم بأركان الجريمة، واتجاه إرادته إلى الفعل المكون لها وتحقيق نتيجته، بل تتطلب هذه الجريمة توافر قصد جنائي خاص، يتمثل في نية استعمال المزور فيما زور من أجله، (الكومي، 2016، صفحة 155) وعلى هذا فإن القصد الجنائي في جريمة التزوير يعرف على نحو غالب لدى الفقه والقضاء بأنه: "تعمد تغيير الحقيقة في محرر تغييرا من شأنه أن يسبب ضرر وبنية استعمال المحرر فيما غيرت من أجله الحقيقة" (حسني، 1994، صفحة 271).

وانطلاقا مما سبق نصل إلى نتيجة مفادها أنه لا يمكن القياس على جريمة التزوير التقليدي، لأن هذا يتنافى مع مبدأ الشرعية، والنصوص التقليدية، كون جريمة تزوير التوقيع الالكتروني جريمة مستحدثة لا تنسجم مع النصوص التقليدية، ما يدعو إلى ضرورة تدخل المشرع الجزائري للنص على هذه الجريمة أخذا بما ذهب إليه المشرع المصري من خلال القانون 15-2004 الخاص بتنظيم التوقيع الالكتروني وأن ما قام به المشرع الجزائري من خلال تعديله لقانون العقوبات لسنة 2004 وإدخاله لجرائم المعالجة الآلية لمعطيات الحاسوب بموجب المادة 394 مكرر إلى 394 مكرر 7 غير كاف بالنسبة لجريمة تزوير التوقيع الالكتروني.

الفرع الثاني: أساليب تزوير التوقيع الالكتروني

نظرا لضعف إجراءات الأمان والثقة في التوقيع الالكتروني، يكون من السهل تزويرها، بعد أن يتم مهاجمته أو نسخه من قبل قراصنة الحاسب الآلي، ومن أهم الصور الأكثر عرضة للتزوير التوقيع بالرقم السري وكذا التوقيع الرقمي.

أولا: تزوير التوقيع الالكتروني الذي يتم بالرقم السري

أهم تطبيقات هذه الصورة بطاقات الصرف البنكي –بمختلف أنواعها- وأهم صور الاستخدام المشروع لهذه البطاقات هو تزويرها سواء تزويرا كليا أو جزئيا ولعل أهمها بطاقات الدفع، التي يمكن أن تكون محلا للاعتداء عليها عن طريق تزويرها، والمبدأ الأساسي لتزوير هذه البطاقة هو سرقة بياناتها من خلال جهاز الحاسب الآلي باستخدام أدوات معينة، حيث يتم نقش هذه البيانات على بطاقة أخرى تكون معدة لهذا الغرض أو تكون بطاقة منتهية أو مسروقة ويتم استخدامها بعد ذلك في عمليات الدفع أو السحب (راضية، 2012، صفحة 145).

وقد لا تكون البطاقة في حدّ ذاتها صحيحة لكن تم الحصول عليها بواسطة وثائق مزورة أو وضع توقيع مزور، فالطريقة الأولى يطلق عليها اصطناع المستند، وهذا بخلق محرر بأكمله ونسبته إلى غير محرره، أما الطريقة الثانية وتعد من طرق التزوير المادي الأكثر شيوعا وذلك بتزييف أو تقليد الكتابة بتدوين عبارات أو وضع توقيعات مقلدة (عبيد، 2017، صفحة 210،211).

وقد يحدث وأن تستعمل هذه البطاقة البنكية المزورة وهي جريمة قائمة بذاتها، وقد فصل فيها المشرع الجزائري، إذ فصل تزوير المحررات عن استعمالها، كما نص على استعمال الأوراق العرقية أو التجارية او المصرفية المزورة (المادة 221 من قانون العقوبات الجزائري).

ويترتب عن فعل التزوير والاستعمال والفصل بينهما أن مرتكب التزوير يعاقب ولو لم يستعمل الورقة المزورة، وأن من يستعمل الورقة المزورة يعاقب حتى ولو لم يرتكب التزوير أو يشترك فيه.

ثانيا: تزوير التوقيع الرقمي

إنّ التوقيع الرقمي يتم بواسطة منظومة الكترونية تتخذ شكل حروف أو أرقام أو رموز أو إشارات... حيث لا يمكن تقليدها إنما استعمالها دون علم مالكها، عن طريق الحصول على منظومة التوقيع بطريقة التجسس الالكتروني أو الدخول غير المشرع، والتوقيع هنا سليما إلا أنه استخدم من غير صاحبه، وعليه يتم الكشف عن التوقيع الرقمي المزور بإثبات أنه لم يصدر من صاحب المنظومة، وإنما من شخص آخر قام بسرقتها (الجنبيهي.، 2006، صفحة 54).

وتكون جريمة تزوير التوقيع بالدخول إلى قاعدة البيانات وتعديلها، سواء بإلغاء بيانات موجودة بالفعل أو بإضافة بيانات لم تكن موجودة من قبل، وتعد جريمة مركبة تتكون من جريمتين: جريمة سرقة منظومة التوقيع الالكتروني (التجسس-الدخول غير المشروع عن طريق القرصنة الالكترونية)، والتي يصعب اكتشافها إلا بعد استخدام غير المشروع لمنظومة التوقيع الالكتروني (راضية، 2012، صفحة 151).

الفرع الثاني: العقوبات المقررة لجريمة تزوير التوقيع الالكتروني

يحظى التوقيع الالكتروني بحماية قانونية، إضافة إلى تلك التي يضيفها القانون الخاص به، الحماية التي يستمدها من القوانين التقليدية القائمة، سواء بإصدار قانون خاص باسم التوقيع الالكتروني، أو بإدخال تعديلات على النصوص التشريعية القائمة على نحو يؤدي إلى استيعابها الصور المستحدثة من الجرائم الالكترونية.

وتماشيا مع التطور التكنولوجي في مجال الاتصالات وانتشار استخدام النظم المعلوماتية، أدخل المشرع الجزائري جملة من التعديلات على ترسانته القانونية منذ 2004، وهذا من خلال تعديل قانون العقوبات بموجب الأمر 04-15 تحت عنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات والاستعمال للإعلام الآلي من خلاله حرم كل أنواع الاعتداءات التي تستهدف الدخول غير المشروع لأنظمة المعلوماتية، تغيير أو إتلاف المعطيات، محددا بذلك الأفعال والسلوكات التي تدخل ضمن مجال هذا النوع الجديد من الجرائم على سبيل الحصر، ومن بينها إدخال معطيات في منظومة المعالجة الآلية أو إزالة أو حذف أو تعديل معطيات منظومة المعالجة الآلية عن طريق الغش طبقا للمادة 394 مكرر ف 1 من قانون العقوبات الجزائري، وتقوم هذه الجريمة بمجرد ارتكاب أحد هذه الأفعال، بغض النظر عن المجال المستهدف، سواء كانت البرامج أو المعطيات أو قاعدة البيانات للتوقيع الالكتروني (المادة 394 مكرر 1 من قانون العقوبات الجزائري).

إضافة إلى هذا أصدر المشرع الجزائري القانون 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وأطلق عليها الجرائم المعلوماتية (المادة 02 فقرة 01 القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها).

ويستشف من هذا القانون أن الجريمة محل الدراسة غير محددة بوضوح في الجريمة محل الدراسة أو بالأحرى لم يجرمها المشرع وفقا لهذا القانون، والجدير بالذكر أنه وبالرجوع إلى نصوص التزوير في قانون العقوبات لا نجد فيه أي تعديل يتعلق بإمكانية تطبيق هذه النصوص على التزوير الالكتروني بالرغم من أن المشرع قد اعترف بهذه المحررات وساواها في القيمة الثبوتية بالمحررات الورقية –كما سبقت الإشارة- وعليه كان على المشرع أن يعدل كذلك في نصوص التزوير ليستوعب العقاب على التزوير الالكتروني (خليفة، 2016، صفحة 83).

وتحال العقوبات المتعلقة بالتزوير الالكتروني –تزوير التوقيع الالكتروني- إلى نصوص قانون العقوبات. فعاقب المشرع الجزائري على التزوير في المحررات العرفية المصرفية أو التجارية بمقتضى المادة 219 بالحبس من سنة إلى خمس سنوات والغرامة من 500 دينار جزائري إلى 20,000 دج كعقوبة أصلية، إضافة إلى العقوبات التكميلية وهذا حسب الفقرة 02 من المادة 219 والمتمثلة في الحرمان من حق أو أكثر من الحقوق الواردة في المادة 14 من نفس القانون، وبالمنع من الإقامة من سنة إلى 05 سنوات على الأكثر (المادة 14 من قانون العقوبات الجزائري).

كما خصّ المشرع الجزائري التزوير الواقع على شهادة التزوير الواقع على شهادة التصديق الالكتروني بعقوبات خاصة، فقد جاء في المادة 66 من قانون التوقيع والتصديق الالكترونيين بالحبس من ثلاثة أشهر إلى ثلاثة سنوات، وبغرامة من 20,000دج إلى 200,000دج أو بإحدى هاتين العقوبتين فقط كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق الكتروني موصوفة، ولم يتكلم النص على المحاولة في التزوير أو الاشتراك فيها، وعليه فيطبق القاضي للأحكام العامة.

وعاقب المشرع الجزائري على الشروع، وعليه فإنه يعاقب من بدأ في تنفيذ جريمة التزوير في المحررات المصرفية أو التجارية ولم يحقق نتيجتها ومن بدأ فيها وأتمها بنفس العقوبة (انظر المادتان 219،220 من قانون العقوبات الجزائري).

هذا بالنسبة للعقوبات المقررة للشخص الطبيعي، أما بالنسبة للشخص المعنوي فقد نص المشرع الجزائري على مسؤولية الشخص المعنوي فيما يتعلق بجرائم التزوير في المادة 253 مكرر من قانون العقوبات (انظر المادة 253 من قانون العقوبات الجزائري).

وتطبق على الشخص المعنوي العقوبات المنصوص عليها في المادة مكرر، وعند الاقتضاء تلك المنصوص عليها في المادة 18 مكرر 2 من هذا القانون ويتعرض أيضا لواحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 18 مكرر.

كما نصت المادة 75 من قانون التوقيع والتصديق الالكترونيين على مسؤولية الأشخاص المعنوية عن الجرائم المنصوص عليها في هذا القانون بقولها: "يعاقب الشخص المعنوي الذي ارتكب إحدى الجرائم المنصوص عليها في هذا الفصل بغرامة تعادل خمس مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي".

المطلب الثاني: الحماية الالكترونية للتوقيع الالكترونية من التزوير

تعد مسألة الأمن المعلوماتي (الحميد م.، 2007، صفحة 34) من أهم الضمانات والتحديات التي تواجهها وسائل الدفع الالكتروني، لأن غياب الأمن المعلوماتي يعتبر من معوقات اعتماد التجارة الالكترونية على الرغم من المزايا التي توفرها. ويقصد بالأمن المعلوماتي حماية جميع المعلومات التي يتم التعامل معها والمعالجة من منظمة وغرفة تشغيل أجهزة،ووسائط التخزين من السرقة والتزوير والتلف والضياع والاختراق (دباس، 2017، صفحة 34).

فلا يكفي الاعتراف بحجية التوقيع الالكتروني في الإثبات، دون العمل على إيجاد الآليات الكفيلة التي تبعث الثقة والاطمئنان لدى المتعاملين به، وتحقيق الحماية الضرورية للتوقيع الالكتروني من أي تحايل أو اختراق، ما جعل المشرع يقر عملية التشفير كإجراء الكتروني تقني لحماية البيانات الالكترونية، إضافة إلى تنظيم مهام جهة التوثيق الالكتروني وتحديد مسؤولياتها قصد تحقيق الأمان القانوني للمتعاملين في المجال الالكتروني.

الفرع الأول: نظام التشفير

يعد نظام التشفير أفضل تقنية لحماية البيانات والمعلومات المرسلة عبر الشبكات المفتوحة من أي تعديل أو تغير غير مرغوب فيه، ولذلك تأتي تقنيات التشفير في مقدمة الوسائل في مجال توفير الأمن وسرية المعلومات والمعاملات والصفقات المتبادلة (الحجار، 2002، صفحة 198).

أولا: المقصود بالتشفير

يعرف التشفير بأنه: "كل العمليات التي تؤدي بفضل بروتوكولات سرية إلى تحويل معلومات أو إشارات مفهومة (مقروءة)، أو القيام بالعكس وذلك باستخدام برامج مصممة لهذه الغاية"، ويعرف أيضا بأنه: "آلية يتم بمقتضاها ترجمة معلومة مفهومة إلى معلومة غير مفهومة عبر تطبيق بروتوكولات سرية قابلة للانعكاس أو يمكن إرجاعها إلى حالتها الأصلي" (الجواري، 2010، صفحة 202).

أما بالنسبة للتعريف التشريعي للتشفير، فلم يتطرق المشرع الجزائري من القانون 18-05 المتعلق بالتجارة الالكترونية (القانون رقم 05/18 المؤرخ في 10 ماي 2018، 2018)، إلى تعريف التشفير، واكتفى بتعريف مفتاح التشفير الخاص ومفتاح التشفير العمومي في القانون 15-04 للقواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني. (نصت على ذلك المادة 02 في فقرتها الثامنة بقولها: "مفتاح التشفير الخاص، هو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط وتستخدم لإنشاء التوقيع الالكتروني، ويرتبط هذا المفتاح بمفتاح تشفيير عمومي".

ويعرف التشفير بأنه: "كل الأعمال التي تهدف إلى تحويل معلومات أو إشارات واضحة باستخدام وسائل مادية أو معالجة آلية إلى معلومات أو إشارات غامضة للغير أو إلى إجراء العملية العكسية عبر وسائل مادية أو معلوماتية مخصصة لهذا الغرض" (الجمال، 2006، صفحة 219).

ثانيا: ضوابط وطرق التشفير

لقد أقر المشرع الجزائري بضرورة تشفير البيانات والمعلومات حفاظا على سرية البيانات والمعلومات، وواضع ضوابط لذلك، كما حدد طرق التشفير وسنوضحها في الآتي:

أ- ضوابط التشفير

نص المشرع الجزائري على ضرورة التشفير، كما نص على العمل من أجل الحفاظ على سرية البيانات والمعلومات المشفرة وتتمثل هذه الضوابط في:

1- مشروعية تشفير البيانات والمعلومات والتي يتم تبادلها عن طريق الوسائط الالكترونية، إذ أقر المشرع الجزائري من خلال القانون 15-04 نصوصا تتناول نظام التشفير، وعرف التشفير الخاص والعام، وأجاز استخدامه في المراسلات الالكترونية والتعاملات التجارية الالكترونية، كما أكد على حماية البيانات المشفرة والعناصر المستخدمة في عملية التشفير وفكها من كل اعتداء سواء تم ذلك باستخدام عناصر التشفير الخاصة بالتوقيع من غير طرفي العلاقة، أو بسبب استخدام التشفير في ارتكاب جرائم احتيالية (عقوني، 2019، صفحة 304).

2- الحق في الحفاظ على سرية البيانات والمعلومات المشفرة: اعتبر المشرع الجزائري من خلال القانون 15-04 (42 و1/11المواد)، الاعتداء على البيانات المرسلة بين طرفي العقد عبر الوسائط الالكترونية هو اعتداء على خصوصية وسرية البيانات والمعلومات المرسلة بين طرفي العلاقة، وبالتالي وجب ضمان سرية البيانات المستخدمة لإنشاء التوقيع الالكتروني بكل الوسائل التقنية المتوفرة (عقوني، 2019، صفحة 304).

كما أقرّ المشرع الجزائري نصوصا تعاقب كل من يقوم بانتهاك سرية البيانات المشفرة وإفشائها سواء من طرف الغير، أو من طرف مؤدي خدمات التصديق الالكتروني، أو من طرف الشخص المكلف بالتدقيق،

3- اعتبار النص المشفر محررا الكترونيا حيث اعتبر المشرع الجزائري النص المشفر من المحررات الالكترونية بالرغم من أنها غير مفهومة للعامة، وبالتالي فإنه يتم تحويل الإشارات والرموز إلى نصوص مقروءة ومفهومة تكون حجة على من يخالف ما التزم به طرفا الاتفاق (عقوني، 2019، صفحة 305).

ب- طرق التشفير

يمكن تصنيف طرق التشفير إلى فئتين رئيسيتين بالنظر إلى نوعية المفتاح المستخدم في التشفير:

1- التشفير المتماثل: يتم في هذا المستوى تشفير جميع المعلومات والبيانات بين نقطة الإرسال ونقطة الاستقبال، ويتم عن طريق الشبكات الافتراضية الخاصة، وهي شبكات جزئية من شبكة الانترنت، تقوم فيه إحدى المنشآت أو المشروعات بتخصيصه لخدمتها عن طريق إحاطته بالاحتياطات التأمينية المطلوبة لإرسال واستقبال المعلومات من خلاله بشكل آمن (أحمد، 2003، صفحة 25). يطلق على هذه الطريقة تقنية المفتاح الخصوصي، كونها تعمل بواسطة مفتاح واحد خصوصي يمتلكه كل من مرسل الرسالة ومتلقيها، وهذا ما يعاب على هذه التقنية، إذ أن استعمال هذا المفتاح من قبل شخصين مختلفين (المرسل والمرسل إليه) قد يضعف من حجية المستندات الرقمية والتوقيع الالكتروني وقوتها الثبوتية (عقوني، 2019، صفحة 306).

2- التشفير غير المتماثل: يطلق على هذه التقنية التشفير بالمفتاح العمومي وخلافا للتشفير بالمفتاح الخصوصي لا يستعمل المفتاح ذاته من أجل تشفير الرسائل، بحيث يستعمل مفتاحين سريين مختلفين من أجل فك تشفيرها، الأول خصوصي يمتلكه مستخدم معين لمستعمل الوسائط الالكترونية ويبقيه سريا وخاصا به، أما الثاني عمومي يوزعه إلى المتعاملين الآخرين الذي يود تلقي رسائل مشفرة منهم (المطالقة، الأردن، صفحة 159).

الفرع الثاني: التصديق الالكتروني

إزاء تنامي مخاطر القرصنة الالكترونية وإساءة استخدام الغير، استوجب الأمر توفير الوسائل التي تكفل تحديد هوية المتعاقدين والتعبير عن إرادتهم على نحو صحيح ثم الاستعانة بطرف ثالث محايد موثوق به، يتمثل في جهة مختصة تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الالكترونية، بإصدار شهادة تسمى بشهادة التصديق الالكتروني.

وبناء على ما سبق سنحاول التطرق إلى تعريف التصديق الالكتروني، ودور الجهة المختصة بإصدار شهادات التصديق في إضفاء الحماية على التوقيع الالكتروني.

أولا: تعريف التصديق الالكتروني

التصديق الالكتروني آلية تهدف إلى بناء الثقة في نظام الشهادات الرقمية وتشجيع المعاملات الالكترونية بإضفاء المصداقية عليها، فالتصديق بمعناه العام يعني التوثيق والاعتماد ومجاله الطبيعي هو التصرفات القانونية في شكلها التقليدي أي السندات الورقية، حيث على الموظف التأكيد والتصديق على صحة ما ورد في المحرر المقدم للتصديق وصحة نسبته إلى من وقع عليه، وبالتالي فالتصديق الالكتروني يعني تدخل طرف ثالث لتأمين التبادل الالكتروني وللمعطيات في المجال الالكتروني لتحقيق السلامة والثقة في المعاملات الالكترونية (نزيهة، 2017، صفحة 291).

ويعد التصديق أو التوثيق الالكتروني وسيلة فنية آمنة للتحقق من صحة التوقيع أو المحرر، حيث يتم نسبته إلى شخص معين أو جهة معينة أو طرف محايد يطلق عليه مقدم خدمات التصديق أو مورد خدمات التصديق أو جهة التوثيق.

ولم يعرف المشرع الجزائري التصديق الالكتروني ولكنه عرف شهادة التصديق الالكتروني وهذا من خلال المادة 02 من القانون 04/15 بأنها وثيقة في شكل الكتروني تثبت الصلة بين بيانات التحقيق من التوقيع الالكتروني والموقع.

ثانيا: دور الجهات المختصة بإصدار شهادات التصديق الالكتروني في حماية التوقيع الالكتروني

اختلف الفقه والقانون في الاصطلاح الذي يطلق على الجهة المختصة بإصدار شهادات التصديق الالكتروني، حيث يستخدم جانب من الفقه اصطلاح سلطة الإشهار، ويطلق عليها جانب من الفقه مصطلح مقدم خدمات التصديق، أما قانون الأمم المتحدة النموذجي بشأن التوقيعات الالكترونية لسنة 2001، فاستخدم مصطلح مقدم خدمات التصديق. وعرفه في المادة 02 من بأنه: "شخص يصدر شهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الالكترونية". أما التوجه الأوروبي فعرف مقدم الخدمات بأنه كل "شخص قانوني طبيعي أو معنوي يصدر شهادات توثيق التوقيع الالكتروني، ويتولى خدمات أخرى مرتبطة بالتوقيع الالكتروني (محمد، 2008، صفحة 173).

أما المشرع الجزائري فقد استمد مصطلح وتعريف مقدم خدمات التوثيق من نصوص قانون اليونسترال بشأن التوقيعات الالكترونية وأحكام التوجيه الأوروبي عند تعريفه بأنه: "شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق الكتروني موصوفة، ويقدم خدمات أخرى في مجال التصديق الالكتروني (المادة 11/2 من القانون 04/15).

ويكمن الهدف الأساسي من إنشاء جهات مختصة في إصدار شهادات التصديق الالكتروني في تسهيل مراقبة التعاملات الالكترونية، إضافة إلى ضمان الأمن القانوني وحماية التعاملات الالكترونية

وخاصة التوقيع الالكتروني من الأخطار التي قد تواجهه بسبب طبيعة هذه المعاملات التي تتم عبر وسائط الكترونية ومجلس عقد افتراضي.

ولعلّ من أهم الضمانات القانونية للحماية والمحافظة على سلامة التوقيع الالكتروني هو إصدار شهادة التصديق الالكتروني، والتحقق من هوية الشخص الموقع، إضافة إلى إثبات مضمون البيانات الالكترونية وإصدار مفاتيح التشفير، نحاول إنجازها فيما يلي:

أ- إصدار شهادة التصديق الالكتروني

ميز المشرع الجزائري بين الشهادة الالكترونية البسيطة والشهادة الالكتروني الموصوفة –كما سبقت الإشارة- فالشهادة الالكترونية البسيطة تتطلب إجراءات ترتبط بمعطيات ومعلومات تتعلق بالتحقق من توقيع شخص معين وتأكيد هوية هذا الشخص (المادة 03 مكرر من المرسوم التنفيذي 162/07 المؤرخ في 30 ماي 2007، المعدل والمتمم للمرسوم التنفيذي رقم 01-123 المؤرخ 09 ماي 2001، 2007).أما شهادة التصديق الالكترونية الموصوفة، فإنها ترتبط بإصدار الشهادة النوعية وفق شروط حددها المشرع من بينها أن تتضمن على الخصوص التوقيع الالكتروني الموصوف (المادة 7 فقرة 2 من القانون 04/15 المتضمن تحديد القواعد العامة للتوقيع مادة 11/2 من القانون 04/15 المحدد للقواعد الخاصة بالتوقيع والتصديق الالكترونيين).

وكل من الشهادتين تفي بوجوب ارتباط التوقيع الالكتروني بشهادة الكترونية والتي تصدر حصريا من جهة تصديق الكتروني معتمدة، ومن ثم فلابد من توافر شهادة التصديق الالكتروني لكل يكون التوقيع الالكتروني موصوفا (عقوني، 2019، صفحة 309).

ب- التحقق من هوية الشخص الموقع

يتمثل الدور الرئيسي لجهات التصديق الالكتروني في تمكين المرسل إليه من التأكد من هوية المرسل وصلاحية توقيعه، حيث تقوم بإصدار شهادة تصديق الكترونيين تفيد التصديق على التوقيع الالكتروني في تعاقد معين، كما تفيد أيضا في صحة التوقيع ونسبته إلى من صدر عنه (الشخص الموقع) (راضية، 2012، صفحة 153).

وقد نص المشرع الجزائري من خلال المادة 44 من القانون 15-04 على أنه يجب على مؤدي خدمات التصديق الالكتروني وقبل منح شهادة التصديق الالكتروني أن يتحقق من تكامل بيانات الإنشاء مع بيانات التحقق من التوقيع، ويمنح مؤدي خدمات التصديق الالكتروني شهادة أو أكثر لكل شخص يقدم طلبا وذلك بعد التحقق من هويته وعند الاقتضاء التحقق من صفاته الخاصة. أما في حالة الأشخاص المعنوية فإن مؤدي خدمات التصديق الالكتروني يحتفظ بسجل يدون فيه هوية وصفة الممثل القانوني للشخص المعنوي المستعمل للتوقيع المتعلق بشهادة التصديق الالكتروني الموصوفة، بحيث يمكن تحديد هوية الشخص الطبيعي عند كل استعمال لهذا التوقيع الالكتروني (عقوني، 2019، صفحة 309).

ج- إثبات مضمون التبادل الالكتروني

تقوم الجهة المختصة بإصدار شهادات التصديق الالكتروني كذلك بالتحقق من مضمون التعامل أو التبادل الالكتروني بين الأطراف المتعاقدة، وكذلك التيقن من سلامته وجديته وبعده عن الغش والاحتيال. إضافة إلى إثبات ومضمونه، حماية للمتعاملين من أي غش قد يقعون فيه أثناء تعاملاتهم. (الليل، 2003، صفحة 178).

وقد نص المشرع الجزائري على أن يلغي خدمات التصديق الالكتروني الموصوفة عندما يتبين أنه قد تم منحها بناء على معلومات خاطئة أو مزورة أو إذا أصبحت المعلومات الواردة في شهادة التصديق الالكتروني غير مطابقة للواقع، أو إذا تم انتهاك سرية بيانات إنشاء التوقيع (المادة 45 من القانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين).

د- إصدار المفاتيح الالكترونية

تقوم جهات التصديق الالكتروني بإصدار مفاتيح التشفير الالكتروني، سواء المفتاح الخاص الذي من خلال يتم تشفير المعاملة الالكترونية الذي يكون خاصا بصاحبه ولا يعلمه غيره، أهم المفتاح العام الذي يتم بواسطته فك هذه الشفرة، كما تتولى المصادقة على هوية الحائز على المفتاح العمومي وإصدار شهادات الكترونية من شأنها أن تضمن بأن المفتاح العمومي العائدة إلى الجهة الحائزة على المفتاح الخصوصي، ومن ثم استخدام المفتاح العام لفك تشفير الرسالة الأصلية والتأكد من عدم حصول أي تعديل عليها (عقوني، 2019، صفحة 310).

الخاتمة:

من خلال ما سبق توصلنا إلى أن التوقيع الالكتروني جاء ليقر للتعاملات المبرمة بين الوسائط الالكترونية القوة الثبوتية، ويرسي جوا من الثقة فيها، مع قدرته على تحقيق نفس وظائف التوقيع التقليدي. فالتوقيع الالكتروني يعد شرطا أساسيا لضمان موثوقية معاملات التجارة الالكترونية.

وضرورة توافر الثقة والأمان في المعاملات التي تتم عبر الوسائط الالكترونية مسالة مهمة وضرورية لبقائها وانتشارها نظرا لعدم الحضور المادي لأطراف التعامل، وهو ما استلزم ضرورة توفير حماية تعزز هذه الوسيلة، وتجلى ذلك من خلال تبني المشرع الجزائري جملة من الآليات وبرز ذلك انطلاقا من اعتراف المشرع من خلال القانون المدني المعدل سنة 2005 بإمكانية الإثبات بواسطة المستندات الموقعة الكترونيا،إضافة غلى ما جاء به المشرع من خلال القانون 04/15 المدعم لحماية التوقيع الالكتروني من القرصنة الالكترونية وغيرها من الاختراقات التي يتم تبادلها من خلال شبكة الانترنت أو تحريفها أو تزويرها وهذا بوضعه نظام التشفير كآلية تقنية ووجود طرف ثالث محايد مهمته توثيق العلاقات بإصدار شهادة التصديق الالكترونية.

وفي الأخير نقترح **التوصيات** التالية:

1- بالرغم من أن القانون 04/15 المتعلق بالتصديق والتوقيع الالكترونيين نص على بعض الجرائم لحماية التوقيع الالكتروني، إلا أنه لم ينص على جريمة تزوير التوقيع الالكتروني، ومن ثم ضرورة إيجاد نص صريح ينص على هذه الجريمة، إما بإضافة نص في قانون العقوبات أو من خلال القانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين،

2- ضرورة إنشاء سلطات التصديق الالكتروني لما لها من دور فعال في حماية التعاملات الالكترونية بوجه عام والتوقيع الالكتروني بوجه خاص،

3- ضرورة إصدار النظام اللازم والمتعلق بتنظيم كيفية حماية الوثيقة الموقعة الكترونيا.

مراجع المقال:

1. يتكون هذا التوجيه من 28 حيثية و15 مادة وأربعة ملاحق، حيث جاءت في مادته الأولى أن الهدف منه هو تسهيل استخدام التوقيعات الالكترونية والمساهمة بالاعتراف القانوني لها كدليل إثبات، وأضفى على التوقيع الالكتروني نفس الحجية القانونية الممنوحة للتوقيع الالكتروني،، المنتج) تاريخ الاسترداد 15 02، 2019، من http://www.Fs.dk/uk/acts/eu/pdf/eisgn-fi.pdf ،. (s.d.). Consulté le 03 22, 2019, sur http://www.unictral.org

(s.d.). (ق. 2002, Producteur) Consulté le 03 22, 2019, sur http://www.unictral.org.

2. وهذا ما أكدته المادة 03 من قانون اليونسترال النموذجي بشأن التوقيعات الالكترونية بقولها: "لا تطبق أي من أحكام هذا القانون، بإنشاء المادة الخامسة، بما يشكل استبعادا أو تقيدا أو حرمانا من مفعول قانوني لأي طريقة لإنشاء توقيع الكتروني تفي بالاشتراطات المشار.

3. المادة 8 من القانون 04/15 المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني.

4. المادة 7 فقرة 2 من القانون 04/15 المتضمن تحديد القواعد العامة للتوقيع مادة 11/2 من القانون 04/15 المحدد للقواعد الخاصة بالتوقيع والتصديق الالكترونيين. (بلا تاريخ).

5. -وهذا ما أكدته المادة 03من قانون اليونسترال النموذجي بشأن التوقيعات الالكترونية بقولها" :لا تطبق أي من أحكام هذا القانون، بإنشاء المادة الخامسة، بما يشكل استبعادا أو تقيدا أو حرمانا من مفعول قانوني لأي طريقة لإنشاء توقيع الكتروني تفي بالاشتراطات المشار.(s.d.) .

6. مسعودي يوسف، أرجيلوس رحاب. (جانفي، 2017). مدى حجية التوقيع الالكتروني في التشريع الجزائري (دراسة على ضوء أحكام القانون 15-04). مجلة الاجتهاد للدراسات القانونية والاقتصادية، صفحة 84.

7. القانون 15-04 (21 أفريل، 2004). (لمتضمن تنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيات المعلومات المصري، متاح على الموقع الالكتروني:، المحرر، و االمتضمن تنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيات المعلومات المصري، المنتج).

8. (10 02، 2015). القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436ه الموافق لـ 01 فبراير سنة 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين 6(الجريدة الرسمية ،العدد رقم 06).

9. 42 و1/11 المواد. (بلا تاريخ). من القانون 15-04 المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.

10. ,.183 .(s.d.) .2-.لحماية الجنائية للمحررات الالكترونية من التزوير.

11. Article, 4. (s.d.). du code civil crée par loi n° 2000.230 du mars2000. (d. q. Article 1316.4 du code civil crée par loi n° 2000.230 du mars 2000 portant adaptation du droit de la preuve aux technologie de l'information et relative à la signature électronique, Éd.)

12. http://www.unictral.org. (13 مارس، 2019). (اليونسترال: هي لجنة قانون التجارة الدولية التابعة للأمم المتحدة، وتضم في عضويتها غالبية دول العالم الممثلة لمختلف النظر القانونية الرئيسية، غرضها الأساسي هو تحقيق الانسجام والتوافق بين القواعد القانونية الناظمة للتجارة الالكترونية، وقد اعتمدت الأمم، المنتج) تاريخ الاسترداد 13 مارس، 2019، من http://www.unictral.org.

13. n°, 2.-2. D. (2001, 03 30). (p. p. - Décret n° 2001-272 du 30 mars 2001, Éd.)

14. n°, 2.-2. l. (2000, 03 13). (p. a. - Loi n° 2000.230 du 13 mars 2000, Éd.)

15. أسامة بن غانم العبيدي. (2008). حجية التوقيع الالكتروني في الإثبات. المجلة العربية للدراسات الأمنية والتدريب، 5، صفحة 147.

16. أسيا بن عبيد. (أوت، 2017). الحماية الجناية لبطاقات الدفع من جرائم التزوير في القانون الجنائي. مجلة دراسات (57)، صفحة 210،211.

17. الحميد محمد دباس. (2017). حماية أنظمة المعلومات. الأردن: دار الحامد للنشر والتوزيع.

18. الحميد ,م .د .(2007) .حماية أنظمة المعلومات .الاردن :دار الحامد للنشر والتوزيع.

19. الدسوقي أبو الليل. (2003). توثيق التعاملات الالكترونية ومسؤولية جهة التوثيق تجاه الغير المضرور. مؤتمر الأعمال المصرفية الالكترونية. المجلد الخامس، صفحة 178. جامعة الإمارات العربية المتحدة: كلية الشريعة والقانون.

20. الزهرة ,م .م .(2000) .مخرجات الكمبيوتر في الإثبات في المواد المدنية والتجارية .مؤتمر القانون والكمبيوتر والانترنت .(p. 813) الإمارات : كلية الشريعة والقانون.

21. القانون المدني. (بلا تاريخ). القانون المدني. (تنص المادة 323 مكرر 1 من القانون المدني على أنه: "يعتبر الإثبات بالكتابة في الشكل الالكتروني كالإثبات على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها، المحرر).

22. القانون رقم 05/18 المؤرخ في 10 ماي 2018. (16 ماي، 2018). المتعلق بالتجارة الالكترونية، ، العدد 28.

23. القانون 04/15. (بلا تاريخ). (- لقد ميز المشرع الجزائري من خلال القانون 04/15 المتعلقة بالتوقيع والتصديق الالكترونيين بين نوعين من التوقيع وهما التوقيع الالكتروني البسيط والتوقيع الالكتروني الموصوف. فالتوقيع الالكتروني البسيط عرف بموجب الفقرة 01 من المادة 2 من القانون 04/15 على أنه:، المحرر، و - لقد ميز المشرع الجزائري من خلال القانون 04/15 المتعلقة بالتوقيع والتصديق الالكترونيين بين نوعين من التوقيع وهما التوقيع الالكتروني البسيط والتوقيع الالكتروني الموصوف. فالتوقيع الالكتروني البسيط عرف بموجب الفقرة 01 من المادة 2 من القانون 04/15 على أنه:، المترجمون).

24. المادة 02من تنص المادة 02 فقرة 01 القانون 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .(s.d.) .

25. المادة 03 مكرر المرسوم التنفيذي 162/07 المعدل والمتمم للمرسوم التنفيذي رقم 01-123 المؤرخ 09 ماي 2001. (30 ماي، 2007).

26. المادة 03 مكرر من المرسوم التنفيذي 162/07 المؤرخ في 30 ماي 2007، المعدل والمتمم للمرسوم التنفيذي رقم 01-123 المؤرخ 09 ماي 2001. (30 ماي، 2007). المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية (العدد 37).

27. المادة 14 من قانون العقوبات الجزائري. (بلا تاريخ).

28. المادة 11/2 من القانون 04/15 . (بلا تاريخ). المحدد للقواعد الخاصة بالتوقيع والتصديق الالكترونيين.

29. المادة 221 من قانون العقوبات الجزائري. (بلا تاريخ).

30. المادة 394 مكرر 1 من قانون العقوبات الجزائري. (بلا تاريخ).

31. المادة 45 من القانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين. (بلا تاريخ).

32. المادة03. (بلا تاريخ). قانون اليونسترال النموذجي بشأن التوقيعات الالكترونية .

33. المرسوم التنفيذي رقم162-07. (بلا تاريخ). المرسوم التنفيذي 162-07 المؤرخ في 13 جماده الأولى 1428 الموافق لـ 30 مايو 2007 المتمم للمرسوم التنفيذي رقم 123-01 المؤرخ في 15 صفر عام 1428 الموافق لـ 9 مايو 2001 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية.

34. المطالقة محمد فواز. (2008). الوجيز في عقود التجارة الالكترونية (الإصدار 2). الأردن: دار الثقافة للنشر والتوزيع.

35. الهام بن خليفة. (2016). الحماية الجنائية للمحررات الالكترونية من التزوير(أطروحة دكتوراه). 83. باتنة، الجزائر.

36. انظر المادة 253 من قانون العقوبات الجزائري. (بلا تاريخ).

37. انظر المادتان 219،220 من قانون العقوبات الجزائري. (بلا تاريخ).

38. إيمان مأمون أحمد سليمان. (2000). ابرام العقد الالكتروني وإثباته. مصر: دار الجامعة الجديدة النشر.

39. بلال، ,س. س. .(2017) .جرائم المعلومات والشبكات في العصر الرقمي .مصر :دار الفكر الجامعي.

40. تنص المادة 02 فقرة 01 القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنه (أ- الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة ترتك. (بلا تاريخ).

41. تنص المادة 394مكرر 1 على أنه: "يعاقب بالحبس مدة ستة أشهر إلى ثلاثة سنوات وبغرامة من 500,000دج إلى 2,000,000دج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.(s.d.) ".

42. تنص المادة 394 مكرر 1 على أنه: "يعاقب بالحبس مدة ستة أشهر إلى ثلاثة سنوات وبغرامة من 500,000دج إلى 2,000,000 دج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها". (بلا تاريخ).

43. ثروت عبد الحميد. (2001). التوقيع الالكتروني. مصر: دار النيل للطباعة والنشر.

44. راضية مشري. (جوان، 2017). جريمة تزوير التوقيع الالكتروني في التشريع الجزائري. مجلة حوليات للعلوم الاجتماعية والإنسانية (20)، صفحة 130.

45. رشيدة بوكر. (ديسمبر، 2016). التوقيع الالكتروني في التشريع الجزائري،العدد الرابع، ديسمبر 2016،ص67. - رشيدة بوكر، التوقيع الالكتروني في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، الجزائر ، العدد الرابع، ديسمبر 2016،ص67، صفحة 67.

46. ريضي ,غ .(2018) .القواعد الخاصة للتوقيع الالكتروني. عمان ,الأردن : دار الثقافة للنشر والتوزيع.
47. سلطان عبد الله محمود الجواري. (2010). عقود التجارة الالكترونية. الأردن: دار الثقافة للنشر والتوزيع.
48. سمير حامد عبد العزيز الجمال. (2006). التعاقد عبر تقنيات الاتصال الحديثة. مصر: دار النهضة العربية.
49. عباس العبودي. (2010). تحديات لإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها. لبنان: الطبعة الأولى، منشورات الحلبي الحقوقية.
50. عبد الفتاح بيومي حجازي. (2002). الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت. مصر: دار الكتب القانونية.
51. عزت عبد القادر. (2000). جرائم التزوير والتزييف. مصر: دار أسامة للنشر والتوزيع.
52. عيسى غسان ريضي. (2018). القواعد الخاصة للتوقيع الالكتروني. عمان: دار الثقافة للنشر والتوزيع.
53. عيسى غسان ريضي. (2018). لقواعد الخاصة للتوقيع الالكتروني. الأردن، عمان: دار الثقافة للنشر والتوزيع.
54. غزالي نزيهة. (2017). لآليات القانونية لحماية وسائل الدفع الالكتروني في التشريع الجزائري. مجلة البحوث السياسية والإدارية، صفحة 291.
55. فقرة ب المادة23. (بلا تاريخ). القانون رقم 15-04. (خلافا للمشرع الجزائري جرم المشرع المصري فعل تزوير التوقيع الالكتروني من خلال نصوص قانون التوقيع الالكتروني، حيث نص في المادة 23 فقرة ب من القانون 15-2004، المتضمن تنظيم التوقيع الالكتروني على معاقبة كل من: "أتلف أو عيب توقيعا أو وسيطا أو محررا الكترونيا أ، المحرر).
56. فواز المطالقة محمد. (2008). الوجيز في عقود التجارة الالكترونية (الإصدار 2). الأردن: دار الثقافة للنشر والتوزيع.
57. فواز محمد المطالقة. (الأردن). الوجيز في عقود التجارة الالكترونية،. 2008: دار الثقافة للشر والتوزيع.
58. لالوش راضية. (2012). أمن التوقيع الالكتروني (مذكرة ماجستير). (جامعة مولود معمري، المحرر) كلية الحقوق والعلوم السياسية، تيزي وزو.
59. لامية محبوب. (2013). جريمة التزوير. مصر: دار الجامعة الجديدة.
60. لمادة 02 فقرة 01 القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها . (بلا تاريخ).
61. محمد الهواري أحمد. (2003). عقود التجارة الالكترونية في القانون الدولي الخاص. الجوانب القانونية والأمنية للعمليات الالكترونية (صفحة 25). الإمارات العربية المتحدة: مركز البحوث والدراسات بأكاديمية شرطة دبي.
62. محمد عقوني. (2019). الآليات التقنية والقانونية لحماية التوقيع الالكتروني. مجلة المفكر (18)، صفحة 304.
63. محمود نجيب حسني. (1994). شرح قانون العقوبات القسم الخاص. 2. مصر، حلوان: دار النهضة العربية.
64. ممدوح علي مبروك. (2009). مدى حجية التوقيع الالكتروني في الإثبات. مصر: دار النهضة العربية.
65. منير محمد الجنبيهي، ممدوح محمد الجنبيهي. (2006). تزوير التوقيع الالكتروني. دار الفكر الجامعي: مصر.

66. نصت على ذلك المادة 02 في فقرتها الثامنة بقولها: "مفتاح التشفير الخاص، هو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط وتستخدم لإنشاء التوقيع الالكتروني، ويرتبط هذا المفتاح بمفتاح تشفيير عمومي"، وتنص الفقرة التاسعة من ذات المادة على أن: "مفتاح التشفير. (بلا تاريخ).

67. هدى حامد قشقوش. (2003). الحماية الجنائية للتوقيع الالكتروني. تأليف بحوث مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون (المحرر). المجلد الثاني، صفحة 582. الإمارات العربية المتحدة: كلية الشريعة والقانون وغرفة تجارة وصناعة دبي.

68. وسيم شفيق الحجار. (2002). الإثبات الالكتروني. لبنان: منشورات الحلبي الحقوقية.

69. ياسر محمد الكومي. (2016). الحماية الجنائية والأمنية للتوقيع الالكتروني في التشريع المصري والتشريعات المقارنة، أطروحة دكتوراه، في القانون الجنائي، كلية الحقوق. 155. مصر، جامعة حلوان.

70. ياسر محمد الكومي، ا، ، في القانون الجنائي، كلية الحقوق، جامعة حلوان، مصر، 2016، ص 155. (بلا تاريخ). لحماية الجنائية والأمنية للتوقيع الالكتروني في التشريع المصري والتشريعات المقارنة أطروحة دكتوراه.

71. يوسف ,ر .(2013) .حجية وسائل الإثبات الحديثة)أطروحة دكتوراه .(تلمسان ,كلية الحقوق والعلوم السياسية ,الجزائر :جامعة أبو بكر بلقايد.