مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

الحماية الجنائية للتصديق والتوقيع الالكتروني– دراسة مقارنة – (معدل ومصحح حسب توجيهات الخبيرين)

The Protection criminal of ratification and electronic signature in a commercials affairs

د. جبيري ياسين
جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة
djebiri.yacine@yahoo.fr

تاريخ النشر: 2018/06/10

الملخص:

يعتبر التوقيع شرطا أساسيا في توثيق المستندات سواء كانت تقليدية أو إلكترونيا محلية أو دولية ونسبتها إلى مصدرها، فالتصديق أو التوقيع الالكتروني ذو فوائد جمة، سواء على جانب الخدمات العامة ،و له بالغ الأثر على التجارة الالكترونية. عمليا التصديق الالكتروني هو طريقة اتصال مشفرة رقميا تعمل على توثيق المعاملات عبر الانترنت. تفاعل عوامل المتعامل ومتعامل معه وموفر خدمات التصديق ومستعمل الانترنت ينشأ أفعالا مجرمة. وهو موضوع هذه الدراسة: ماهية التوقيع الالكتروني من منظور عربي وغربي، وكذلك أفعال التعدي على التوقيع الالكتروني من منظور النظامين اللاتيني والانجلوسكسوني والعقوبات المرصودة للمخالفين في كل نظام ودراسة المسألة من منظور وطني جزائري.

الكلمات المفتاحية: الحماية الجنائية، التصديق الإلكتروني، التوقيع الإلكتروني، الأعمال التجارية.

Abstract:

Signature is a prerequisite in the documents, whether traditional or local or international electronically and attributed

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

to the source document, Ratification or electronic signature is a great benefit, both on the side of public services, and has a dramatic impact on electronic commerce. Practically electronic certification is a way of communication digitally coded working on documenting transactions via the Internet. The trader, a trader with factors interact and provider certification and used online services arises offenses established. It is the subject of this study: what the electronic signature of the Arab and Western perspective, as well as acts of infringement on the electronic signature from the perspective of the Latin and Anglo-Saxon systems and sanctions for violators observed in each system and to examine the issue from an Algerian national perspective.

Keywords: Criminal protection, electronic certification, electronic signature, business.

مقدمة:

يعد التوقيع الالكتروني من حيث تعريفه متشابها تقريبا في كل القوانين المنظمة له مع اختلاف الألفاظ لكن بنفس المؤدى، فيعرف على أنه: "توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذي شكل إلكتروني وملحق أو مرتبط برسالة الكترونية ممهورة بنية توثيق أو اعتماد تلك الرسالة". ويأخذ التوقيع أشكال متعددة كالتوقيع بالقلم الالكتروني، والتوقيع باستخدام الخواص الذاتية، وأخيرا التوقيع الرقمي.

لكن قد يحدث أن تستخدم تلك البيانات الشخصية دون علم مالكها في أفعال متعددة توصف بأفعال الاعتداء على التوقيع الإلكتروني، وفعل كهذا يأخذ توصيف التزوير في التوقيع التقليدي؛ لذلك ففعل الاعتداء على التوقيع الالكتروني يختلف كلية عما هو متعارف عليه في أعمال التجارة العادية، حيث يقوم المجرم بالحصول على

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

منظومة التوقيع الالكتروني الخاصة بشخص آخر؛ والفعل بهذا التوصيف من الأمور الحديثة النشأة التي وجب على المشرع التصدي لها في عالم يتطور بسرعة.

فماهي التكييفات القانونية المختلفة لفعل الاعتداء على التوقيع الإلكتروني في التشريع الجزائري القانون المقارن؟ وما هي أهم الإجراءات الحمائية المرصودة لردع تلك الاعتداءات؟ للإجابة على هذا التساؤل سأعمد لتناول الموضوع في الخطة التالية:

المبحث التمهيدي: ماهية التوقيع الإلكتروني في المنظور القوانين العربية والتشريعات الغربية.

المبحث الأول: جرائم الاعتداء والعقوبات والإجراءات المقررة من أجل حماية التوقيع الإلكتروني من منظور التشريعات الغربية.

المبحث الثاني: جرائم الاعتداء والعقوبات والإجراءات الحامية للتوقيع الإلكتروني من منظور المشرع الجزائري والتشريعات العربية.

المبحث الثالث: مدى نجاعة هذه الإجراءات الحمائية للتصدي لجرائم الاعتداء على التوقيع الإلكتروني.

المبحث التمهيدي: ماهية التوقيع الإلكتروني في المنظور القوانين العربية والتشريعات الغربية: لم يعد التوقيع التقليدي ملائما للمعاملات التجارية، خاصة مع التقدم العلمي التكنولوجي والتقني في وسائل الاتصال والمعلومات، لذلك ظهر التوقيع الالكتروني كأحد الوسائل الأساسية في تنظيم الخدمات المصرفية الإلكترونية فالكثير منها يستند في اثباتها وقبولها إلى التوقيع الالكتروني، إذ لابد لصحة وتمام العقود الالكترونية من توقيع جميع أطراف العقد.

المطلب الأول: تعريف وحجية التوقيع الالكتروني في الممارسات التجارية

يتسع مفهوم التوقيع بمفهومه التقليدي ليشمل كل علامة من شأنها أن ترتبط ارتباطا وثيقا بالشخص الذي تصدر عنه، فقد يكون كلمة معينة تحدد اسم هذا الشخص

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

أو لقبه أو كلمة أخرى يختارها بنفسه، أو قد يكون حرفا أو مجموعة أحرف، كما قد يكون رمزا معينا أو رقما معينا، وقد يكون عبارة عن بصمة أصبع أو ختما خاصا بصاحب الحق يستخدمه في معاملاته. فالتوقيع يعبر عن صاحبه بشكل ما.

ففي التجارة التقليدية يتيح الحضور المادي للمتعاقدين من التحقق من هويتهما مما يحقق الثقة المتبادلة بين الاطراف، حيث يتم التفاوض والتعاقد بحضور المتعاقدين والشهود ويتم التوقيع على مستند كتابي بشكل واضح للجميع. إلا ان كل ذلك قد لا يتوافر في التجارة الالكترونية التي تقوم دون الحاجة للحضور مع وسائل اتصال جديدة، والذين يقعون في مخاطر التعاقد عن بعد كعدم توافر الثقة، والذي قد يتطلب تعزيزها التوقيع بوسائل تقنية حديثة لتحديد هوية المتعاقدين وتعبر عن مسؤولياتهم عن معاملاتهم التعاقدية، فاشتراط التوقيع يوفر الائتمان التجاري ويحقق التقارب بين القانون والتكنولوجيا، مما يسهل التجارة الالكترونية.

الفرع الأول: تعريف وصور التوقيع الالكتروني

ونتناول فيه المفاهيم الفقهية والتشريعية لمصطلح التوقيع الإلكتروني؛ ثم مختلف الصور والأشكال التي يأخذها هذا التوقيع.

البند الأول: تعريف التوقيع الالكتروني (في الفقه والتشريع)

أولا– التعريف الفقهي للتوقيع الالكتروني:

عرفه جانب من الفقه بأنه: إشارة أو رمز أو صوت إلكتروني، ويرتبط منطقيا برسالة بيانات الكترونية لتعيين الشخص المنشئ للتوقيع وتأكيد هويته وبيان موافقته على المعلومات التي تتضمنها رسالة البيانات.[1]

[1]– د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الاسكندرية – مصر، 2006، ص: 186.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

وعرفه آخر بأنه: "حروف أو أرقام أو رموز أو إشارات لها طابع منفرد تسمح بتحديد الشخص صاحب التوقيع وتميزه عن غيره، ويتم اعتماده من الجهة المختصة".[1]

ثانيا– التعريف التشريعي للتوقيع الإلكتروني:

عرف المشرع الفرنسي التوقيع الالكتروني من خلال المادة 4/1316 من القانون المدني[2]، على أساس التوقيع الذي يتم باستخدام وسيلة الكترونية آمنة لتحديد هوية الموقع وضمان صلته بالتصرف الذي وقع عليه، " صوت أو رمز أو معالجة إلكترونية مرفقة أو متحدة بعقد أو بغيره من السجلات يتم تنفيذها أو إقرارها من شخص تتوافر لديه نية التوقيع على السجل".[3]

وعرف المشرع في ولاية نيويورك التوقيع الالكتروني بموجب قانون صادر في 6 أوت 2002 على أنه: "صوت أو رمز أو معالجة إلكترونية ملحقة بسجل الكتروني أو متحدة منطقيا به ويجريها أو يقرها شخص تتوافر لديه نية التوقيع في هذا السجل".[4]

ويتماثل هذا التعريف مع القانون الاتحادي الأمريكي، كما انه يكاد يتطابق مع التعريف الذي اورده المشرع الإنكليزي، إذ نص الفصل الأول من لائحة التوقيع الإلكتروني الصادر في 8 مارس 2002 على أنه يعني بيانات في شكل الكتروني ملحقة أو

[1] – عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة للنشر، مصر، 2009، ص: 211.

[2] – المادة معدلة ومتممة بالقانون التوقيع الإلكتروني الفرنسي رقم 2000/23 الصادر في 2000/03/13.

[3] -La loi n° 2000-2230 du 13 mars 2000, J.O. 14 mars 2000.P.3986.J.C.P.2000, III, 20259.

[4] - Report to the governor and legislature on New York Stat's Electronic Signatures and records act, p: 11

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

متحدة منطقيا بغيرها من البيانات الالكترونية والتي تصلح كوسيلة للتوثيق"[1] كما أنه يكاد يتطابق مع التعريف الذي قدمه المشرع الالماني في المادة الثانية من التوقيع الالكتروني.[2]

ويلاحظ أن اتجاه التشريعات المقارنة تتجه إلى التوسع في الوسائل التي تصلح لإجراء التوقيع الالكتروني، وسببه هو توفير مرونة أكبر للمتعاملين في اختيار الوسيلة التي يرونها تكفل الأمن والثقة في هذا التوقيع.[3]

المشرع الجزائري لم يعرفه بل عرضه كشكل من أشكال إثبات الالتزام المعدل بالقانون 07– 05 المؤرخ في 13 ماي 2007 بالنص على الاثبات بالكتابة العادي كالإثبات في الشكل الالكتروني على أنه: "يعتبر الإثبات بالكتابة في الشكل الالكتروني كالاثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون هذه معدة ومحفوظة في شروط تضمن سلامتها". ضمن فصل الإثبات بالكتابة، واكتفى في المادة 323 مكرر و323 مكرر 1 من القانون المدني[4] المعدل بالقانون 07– 05 المؤرخ في 13 ماي 2007 بالنص على الاثبات بالكتابة العادي كالإثبات في الشكل الالكتروني على أنه: "يعتبر الإثبات بالكتابة في الشكل الالكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون

[1] – Laws of 2002, Chapter: 314/2.

[2] – Report to the governor and legislature on New York Stat's Electronic Signatures and records act, op-cit,p: 7 ,note: 4.

[3] – Statutory Instrument 2002 No. 318, The Electronic Signatures Regulations 2002, op-cit. Draft of a Law on the Framework Conditions, (2), P: 4.

[4] – القانون الصادر بموجب الأمر 75–58 لـــ 26 سبتمبر 1975 المتضمن القانون المدني الجزائري المعدل والمتمم.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

هذه معدة ومحفوظة في شروط تضمن سلامتها". أما في القانون 15–04 الصادر في 1 فيفري 2015 المتعلق بالقواعد العامة المنظمة للتوقيع والتصديق الإلكتروني، فقد أورد تعريفا له في الفصل الثاني المادة 2 فقرة 1 و3 كالآتي: "التوقيع الإلكتروني هو بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق". أما بيانات إنشاء التوقيع الإلكتروني فهي في فقرة موالية: "بيانات فريدة مثل الرموز، أو مفاتيح التشفير الخاصة، التي يستعملها الموقع لإنشاء التوقيع الإلكتروني". وحسنا فعل المشرع من حيث تخصيص فصل خاص لتعريف المصطلحات الغامضة ومفاهيم مرتكزات القانون الجديد في المنظومة التشريعية القانونية الجزائرية.

أما المشرع الأردني في قانون المعاملات الإلكترونية رقم (58) لسنة 2001، في المادة 2 فعرفه أنه: "البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرهما وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة في رسالة معلومات أو مضافة عليها أو مرتبطة بها، ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره من أجل توقيعه وبغرض الموافقة على مضمونه.[1]

أما المشرع المصري فقد عرفه في المادة 1/أ من قانون التوقيع الإلكتروني بأنه: "ما يوضع على محرر الكتروني ويتخذ شكل حرف أو أرقام أو رموز أو شارات أو غيرها ويكون له طابع متفرد ويسمح بتحديد شخص الموقع ويميزه عن غيره."[2]

عرف قانون المعاملات في إمارة دبي على أنه: "توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام تعالجه ذي شكل الكتروني ومرتبط منطقي برسالة الكترونية بنية توثيق أو اعتماد تلك الرسالة".[1]

[1]– القاضي يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات، دار وائل للنشر، الأردن، 2007، ص: 68.

[2]– أبو هيبة نجوى، التوقيع الالكتروني، دار النهضة، د.ت، ص: 41.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

إذن فالغالب في التشريع والمتفق عليه تقريبا هو مكون التوقيع الالكتروني من حروف، أرقام، أو أصوات، كما أن الفقه يتفق مع هذه التعريفات. ومن الواضح من التعريفات السابقة جميعا أنه تم الحرص على أن يكون التوقيع الالكتروني يعبر ويمثل شخص الموقع ويعبر عن رغبته في الالتزام بما وقع عليه أو أمضاه، وأن يكون التوقيع موثقا ومحددا لشخص الموقع.

البند الثاني: صور التوقيع الالكتروني

يتخذ التوقيع الإلكتروني أشكالا عدة بحسب الوسيلة أو التقنية التي تستخدم في إنشائه، لاسيما وأن القوانين التي نظمته لم تنص على شكل معين له، وإن كانت قد حددت الضوابط العامة له. وتتمثل أهم صور التوقيع الإلكتروني في التوقيع الرقمي، التوقيع البيومتري، والتوقيع باستخدام القلم الإلكتروني، وأخيرا التوقيع الرقمي.

أولا– التوقيع الرقمي أو الكودي:

–**المقصود بالتوقيع الرقمي (الكودي):** قد يخلط بين التوقيع الرقمي ويعتبر نفسه التوقيع الالكتروني إلا أنه لا يعدو أن يكون شكلا من أشكال التوقيع الالكتروني، ويقصد به استخدام مجموعة من الأرقام أو الحروف أو كليهما، يختارها صاحب التوقيع لتحديد هويته وشخصيته، ويتم تركيبها أو ترتيبها في شكل كودي لا يعلمها إلا صاحب التوقيع فقط ومن يبلغه بها.[2] والتوقيع الرقمي يقوم على ترميز المفاتيح ما بين

[1]– المحامي ياسين غانم، قواعد الاثبات وحرية المحررات القانونية الإلكترونية، مجلة المحامون(سوريا)، عدد5– 6، لسنة 2004.

[2]– غالبا ما ترتبط بالبطاقة الذكية، البلاستيكية الممغنطة، وغيرها من البطاقات الحديثة المشابهة والمزودة بذاكرة الكترونية كبطاقة الفيزا والمستر كارد وأمريكان اكسبرس. أنظر: إبراهيم الدسوقي، الجوانب القانونية للتعاملات الالكترونية، مجلس النشر العلمي، جامعة الكويت، 2003، ص: 158 .

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

مفتاح عام[1]، وآخر خاص[2]، وهذه المفاتيح تعتمد في الأساس على تحويل المحرر المكتوب من نمط الكتابة الرياضية إلى معادلة رياضية، وتحويل التوقيع إلى أرقام، فإضافة التوقيع إلى محرر عن طريق الأرقام يستطيع الشخص قراءة المحرر والتصرف فيه، ولا يستطيع الغير التصرف فيه إلا عن طريق هذه الأرقام.[3]

من شأن هذه الطريقة للتوقيع الإلكتروني لأن تحقق الثقة والأمان للمحرر وتضمن تحديد هوية الأطراف بدقة، والعيب الوحيد في هذه الطريقة يتمثل فقط في حالة سرقة هذه الأرقام. فشيفرة الأرقام تضمن سرية المعاملات إضافة إلى وجود هيئة متخصصة في توثيق التوقيعات الإلكترونية وتصديقها.

2– مزود خدمات التصديق: أطلق قانون الأنيسترال للتوقيعات الإلكترونية اسم مقدم خدمات التصديق على الهيئة المختصة بتوثيق التوقيات الالكترونية، وعرفه بأنه الشخص الذي يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية؛ كما عرف الشهادة التي يصدرها مزود خدمات التصديق بأنها: رسالة بيانات أو سجل يؤكد الارتباط بين الموقع وبيانات إنشاء التوقيع.[4]

---

[1]– المفتاح العام عبارة عن أداة الإلكترونية متاحة للكافة، تنشأ بواسطة عملية حسابية خاصة وتستخدم في التحقق من شخصية الموقع الالكتروني، وللتأكد من سلامة وصحة محتوى المحرر الالكتروني الأصلي. أنظر: ممدوح محمد علي مبروك، مدى حجية التوقيع الالكتروني في الاثبات، دار النهضة العربية، القاهرة، 2005، ص: 17.

[2]– المفتاح الخاص عبارة أداة إلكترونية خاصة بصاحبها، تنشأ بواسطة عملية حسابية خاصة وتستخدم في وضع التوقيع الالكتروني على المحررات الإلكترونية، ويتم الاحتفاظ بها في بطاقة ذكية مؤمنة .

[3]– محمد عبيد الكعبي ، الجرائم الناشئة عن الإستخدام غير المشروع للأنترنت، رسالة دكتوراه في الحقوق جامعة القاهرة، 2009، ص: 241.

[4]– قانون الأنسترال بشأن التوقيعات الالكترونية، المادة 2 الفقرة ب– هـــ .

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

ثانيا– التوقيع البيومتري:

يقوم التوقيع البيومتري على خصائص بيولوجية ترتبط بجسم الانسان كبصمة أصبعه أو صوته أو شبكيته، وتختص به دون غيره؛ ذلك أن هذه الصفات تختلف من شخص إلى آخر مما يجعل هذا التوقيع متمعا بدرجة عالية من درجات الموثوقية التي تدفع المتعاملين الكترونيا إلى اعتماده أساسا في تعاملاتهم.

حيث تأخذ عينة من إحدى خصائص البيولوجية الخاصة بالموقع دون غيره، ثم تخزن عن طريق التشفير الكترونيا ليتم مطابقتها بتلك المستخدمة في المعاملات الإلكترونية. ويعتمد هذا النوع من التوقيع على جهة مختصة ومعتمدة بشكل رسمي تقوم بتوثيق التوقيع وتصديقه وتربط بينه وبين الموقع زيادة في الموثوقية وتحقيق الأمان في التعامل الإلكتروني وحماية المتعاملين من التقنية الاحتيالية المتبعة لفك رموز التشفير. يعتمد التوقيع الرقمي والتوقيع البيومتري على التشفير ومعالجة البيانات المتبادلة الكترونيا بوجود سلطة تعمل على توثيق التوقيع الإلكتروني وتصديقه.

ثالثا– التوقيع باستخدام القلم الالكتروني:

وهو الأسلوب الأكثر شيوعا، حيث يتم فيه نقل التوقيع المحرر باليد على المحرر المراد نقله إليه بواسطة الماسح الضوئي.[1] حيث تم تطوير هذا النوع من التوقيع باستخدام قلم الكتروني حسابي يمكنه الكتابة على شاشة الحاسوب عن طريق استخدام برنامج خاص بذلك، يقوم بالتقاط التوقيع والتحقق من صحته، وقبوله إذا كان صحيحا، أو رفضه إذا كان غير ذلك.

فرغم امتياز هذه الطريقة بالمرونة والسهولة في الاستعمال، إلا أنها قد تؤدي في بعض الأحيان إلى زعزعة الثقة، لأنه باستطاعة الشخص المستقبل الاحتفاظ بهذا التوقيع ووضعه على محررات أخرى، كما أنه لا يمكن التأكد من أن الشخص صاحب التوقيع

[1]– نهلا عبد القادر مومني، الجرائم المعلوماتية، دار الثقافة، عمان، 2008، ص: 137.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

هو من قام بالتوقيع على المستند لأنه باستطاعة أي شخص أن يضع هذا التوقيع، إذا حصل عليه.[1] إن التطور التقني المستمر يفرض أشكالا جديدة متطورة من التوقيع الإلكتروني على أن تحقق الهدف الأساسي منه المتمثل في تحديد هوية الموقع والتعبير عن إرادته في الالتزام بما وقع عليه.

الفرع الثاني: القوة القانونية للتوقيع الإلكتروني

أضحى التوقيع الإلكتروني من اولى الأولويات وبخاصة في المعاملات التجارية والمدنية عموما لتوسع استعمال التقنيات التكنولوجية، فلم يعد التوقيع التقليدي كافيا ولا مواكبا لمقتضيات العصر أين اختفت المستندات الورقية التقليدية تماما، وجاء نظام التوقيع الالكتروني ليواكب التطور الحادث. ولكي يتمتع التوقيع الالكتروني بالقوة القانونية الملزمة للأطراف لابد أن تتوفر فيه شروط معينة، وهو موضوع الفرع الأول، أما الفرع الثاني فيتضمن حجية التوقيع الإلكتروني في الإثبات في عدد من التشريعات العربية والغربية.

البند الأول: شروط التوقيع الإلكتروني للتمتع بالقوة القانونية الملزمة

لا يختلف التوقيع الإلكتروني عن التوقيع التقليدي من حيث الشروط الواجب توافرها لإضفاء القيمة القانونية على المستند الموقع وتعزيز الثقة فيه؛ وتتلخص هذه الشروط في تحديد هوية الموقع، وتمييزه عن غيره، ونسبة المستند إلى الموقع، والتعبير عن إرادة الموقع في الالتزام بما وقع عليه.

أولا– في الاتفاقيات الدولية

حددت المادة 3/6 من قانون الأونسيترال النموذجي بالنسبة للتوقيعات الإلكترونية الشروط الواجب توافرها لتحقق قانونية التوقيع الإلكتروني وهي كما يلي:

[1] – محمد عبيد الكعبي ،الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، المرجع السابق، ص: 239.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

1- أن تكون الوسيلة المستخدمة لإنشاء التوقيع مرتبطة بالموقع دون أي شخص آخر.

2- أن تكون الوسيلة المستخدمة لإنشاء التوقيع الإلكتروني خاضعة وقت التوقيع لسيطرة الموقع دون أي شخص آخر.

3- أن تكون المستخدمة لإنشائه خاضعة وقت التوقيع لسيطرة الموقع دون أي شخص آخر.

4- أن يكون أي تغيير في التوقيع يجري بعد حدوث التوقيع قابلا للاكتشاف.

واشترط التوجيه الأوربي الخاص بالتوقيع الإلكتروني:

1- في التوقيع المقدم وجود رابطة قوية بين التوقيع والموقع،

2- والقدرة على التعرف على شخصية الموقع،

3- وإنشاء التوقيع باستخدام وسائل تقع تحت سيطرة الموقع،

4- ومقدرة متلقي الرسالة على التحقق من التوقيع، وعلى اكتشاف أي تعديلات على الوثيقة الموقعة.

هذا وأكدت المادة 23 من اتفاقية التي تنظم أحكام التوقيع الإلكتروني في الدول العربية وذلك بعد موافقة جميع الأعضاء في مجلس الوحدة الاقتصادية العربية بموجب القرار رقم /1377/ بتاريخ 2008/6/5 بالدورة رقم /87/، تمتع التوقيع الإلكتروني والكتابة الإلكترونية والوثائق والمحررات الإلكترونية بالحجية في الإثبات إذا توفرت فيها الشروط التالية:

1- ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره.

2- سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.

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

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

ثانيا– في القوانين الوطنية

لم يشترط القانون الأمريكي أي شرط في التوقيع الإلكتروني ليكون له حجية قانونية إنما اعتبر استخدام أي وسيلة من وسائل تكوين التوقيع كافية للوفاء بالمتطلبات القانونية للتوقيع.[1]

أكد مجلس الدولة الفرنسي في المادة 2 /1 من المرسوم رقم /272/ لسنة 2001 أن التوقيع الإلكتروني الآمن هو التوقيع الإلكتروني الذي يحقق الشروط التالية: [2]

1- أن يكون خاصا بالموقع.

2- يتم انشاؤه بوسائل تقع تحت سيطرة الموقع وحده.

3- يرتبط بالمحرر ارتباطا وثيقا بحيث أن كل تعديل في المحرر بعد ذلك يمكن اكتشافه.

أما في التشريع المصري والقانون الخاص بالتوقيع الإلكتروني، فحددت شروطه المادة 18 على النحو التالي:

1- ارتباط التوقيع الالكتروني بالموقع وحده.

2- سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.

3- إمكان اكتشاف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

---

[1]– عدنان برانبو، أبحاث في القانون وتقنية المعلومات، شعاع للنشر والعلوم، سوريا، 2007، ص: 64.

[2]– برني النذير، إثبات العقد الإلكتروني، المرجع السابق،
https://web.facebook.com/permalink.php?id=284480191669868&story_fbid=146368528862275
تاريخ الاطلاع: 2015/12/08. الساعة: 08: 12.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

أما المشرع الجزائري فقد حذى حذو المشرع الفرنسي في اشتراط قيود على التوقيع الإلكتروني ليكون له القوة القانونية والحجية، ونستقرئ ذلك من المادة 323 مكرر1 والقاضية باعتبارـــ: " الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها أن تكون معدة ومحفوظة في ظروف تضمن سلامتها."والتي يقابلها في التشريع الفرنسي المادة 1316–1 من القانون المدني الفرنسي المتعلق بإثبات الكتابة حيث وضع المشرع الجزائري شرطان لا غير مع اعتماد الرأي الفقهي القائل بالتماثل بين الإثبات بالشكل الإلكتروني كالإثبات بالكتابة، والمعادلة بهذا الشكل هو مدار جدل فقهي واسع بين من يرى عما إذا كانت الكتابة في صورتها الحديثة في الشكل الإلكتروني تعادل في حجيتها حجية الكتابة الرسمية. أما عن الشروط لقبول الكتابة في الشكل الإلكتروني للإثبات وهما:

1- إمكانية التأكد من الشخص الذي أصدرها.

2- أن تكون معدة ومحفوظة في ظروف تضمن سلامتها.

أ– إمكانية التأكد من الشخص الذي أصدرها:

وتعد هذه الإشكاليات من بين أهم الإشكاليات التي تواجه العقود الالكترونية. في هذا المجال حاول المختصون إيجاد بعض الحلول التقنية لهذه الإشكالية باستعمال وسائل تعريف الشخصية عبر كلمة السر أو الأرقام السرية، وكذا وسائل التشفير أو ما يعرف بوسيلة المفتاح العام والمفتاح الخاص، ووسائل التعريف البيولوجية للمستخدم، كبصمات الأصابع المنقولة رقميا أو تناظريا وسمات الصوت أو حدقات العين أو غيرها.

وهي وسائل أريد منها ضمان تأكيد الاتصال من جهة وإثبات هوية الشخص الذي أصدر الوثيقة الإلكترونية من جهة أخرى، لكن تأكد بعد تجربتها أن لكل منها ثغرات أمنية ولذلك تعد غير كافية.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

وهذا ما استدعى اللجوء إلى فكرة الشخص الوسيط بالعلاقة العقدية أو ما يسمى سلطات الموثوقية (سلطة التصديق) Autorités de certification أو Prestataire de service de certification électronique؛ وقد أخذت معظم التشريعات التي اعترفت بحجية الكتابة في الشكل الإلكتروني في الإثبات بهذه الوسيلة للتأكد من هوية الشخص الذي صدر منه الإيجاب او القبول، ومنها القانون الفرنسي الذي أنشأ ما يسمى بهيئة خدمات التصديق prestataire de service de certification، وكذلك القانون التونسي الذي أنشأ ما يسمى بجهات المصادقة وسماها الوكالة الوطنية للمصادقة الإلكتروني.[1] وبالرجوع إلى القانون الجزائري، نجده لم يحدد إلى يومنا هذا كيفيات تطبيق هذا الشرط المقرر بالمادة 323 مكرر من القانون المدني المتعلق بكيفيات التأكد من هوية الشخص الذي صدرت منه الكتابة في الشكل الإلكتروني أو الوثيقة الإلكترونية، وفي انتظار صدور المرسوم التنفيذي الذي يحدد كيفيات تطبيق هذه المادة، فإن تطبيقها يبقى معلقا، كونه يصعب على القاضي التثبت من هوية من صدرت عنه الكتابة، لذا يبقى إنشاء مثل هذه الهيئات أفضل حل لهذا المشكل في الوقت الحاضر .

أ– أن تكون معدة ومحفوظة في ظروف تضمن سلامتها:

ويمكن حفظ الوثيقة الإلكترونية على حامل إلكتروني، ويسمى الوسيط أيضا، وهو وسيلة قابلة لتخزين وحفظ واسترجاع المعلومات بطريقة إلكترونية كأن تحفظ في ذاكرة الحاسب الآلي نفسه في أسطواناته الصلبة Disques Durs أو على الموقع في شبكة الأنترنيت أو على شبكة داخلية تخص صاحب الشأن، وقد تتمثل في قرص مدمج–CD ROM أو قرص مرن Disquette informatique، أو قرص فيديو رقمي. DVD وفي كل الأحوال يجب أن يكون الحامل الإلكتروني من الوسائط المتاحة حاليا أو التي يكشف

[1] – سامح عبد الواحد التهامي، التعاقد عبر الانترنت، دراسة مقارنة، دار الكتاب القانونية، مصر، 2008، ص: 457.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

عنها العلم مستقبلا، فنص المادة 323 مكرر يحتمل توسيع مجال الدعائم الإلكترونية ووسائط جديدة تعد بمثابة الحامل الإلكتروني، كما سبقت الإشارة إلى ذلك عند تعريف الكتابة في الشكل الإلكتروني.

ويتعين حسب الفقه أن يتوافر في الحامل الإلكتروني الذي تحفظ عليه الوثيقة الإلكترونية خصائص معينة تتعلق بهذه الرسالة أو الوثيقة وهي: [1]

إمكانية الاطلاع على الوثيقة الإلكترونية طيلة مدة صلاحيتها.

– حفظ الوثيقة الإلكترونية في شكلها النهائي طوال مدة صلاحيتها.

– يتعين كذلك حفظ المعلومات المتعلقة بالجهة التي صدرت عنها الوثيقة الإلكترونية سواء كان شخصا طبيعيا أو اعتباريا، وكذلك الجهة المرسلة إليها.

– حفظ المعلومات المتعلقة بتاريخ ومكان إرسال الوثيقة واستقبالها.

– التزام المرسل بحفظ الوثيقة الإلكترونية في ذات الشكل الذي أرسلها به، حتى تكون حجة عليه متى تعلق حق للغير بهذه الوثيقة.

ونشير في الأخير إلى أن تخزين أدلة الإثبات في الآلات وعبر المواقع المؤقتة التي يمكن أن لا تتمتع بصفة الدوام والاستقرار جعل الفقيه Caprioli يقترح إنشاء جهات ثالثة تضمن سلامة الوثائق الالكترونية من التبديد والتحريف أو يسمى بـــ Tiers " Archiveur أو" Service d'archivage ، .

فتخزين المعلومات في الكومبيوتر الخاص بأحد المتعاقدين يمكن أن يعرضها للتبديل أو التحريف كون هذا الجهاز يخضع لإرادة وإشراف وتوجيهات مستعمليه، وإذا كان هذا الكمبيوتر يؤدي مهمته تنفيذا للتعليمات ولإيعاز الشخص الذي يخزنها فإنه يقال بأن

[1]– يونس عرب، حجية الإثبات بالمستخرجات الالكترونية www.arablaw.orgتاريخ الاطلاع: 2015/12/3. الساعة: 23: 13.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

هذه المعلومات التي سوف تقدم كدليل إثبات يمكن أن تكون من صنع هذا المستعمل، فهي إذن صادرة عنه وبالتالي لا يجوز له أن يحتج بها كدليل إثبات، تطبيقا لمبدأ عدم جواز اصطناع الشخص دليلا لنفسه، ومن هنا تظهر القيمة القانونية لوجود الوسيط لحفظ هذه الوثائق.

فالمشرع إذ يشترط في التوقيع الإلكتروني شروطا محددة ليتمتع بالقوة القانونية الملزمة التي تمنح السجل الموقع الأثر القانوني في مواجهة الأطراف والغير، فهو يجعل للتوقيع الإلكتروني المستوفي لتلك الشروط الحجية القانونية في الإثبات؛ وهو ما سنعرض له في الفرع الموالي.

أما في القانون 04–15 فجاء أكثر تفصيلا ووضوحا، حيث أوردت المادة 7 تلك الشروط تحت وصف المتطلبات وعددها كالآتي:

1- أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة.
2- أن يرتبط بالموقع دون سواه.
3- أن يمكن من تحديد هوية الموقع.
4- أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.
5- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع.

أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات.

البند الثاني: حجية التوقيع الإلكتروني في الإثبات

الدور الجوهري للتوقيع الإلكتروني يكمن في تحقيق موثوقية المعاملات الإلكترونية وضمان الثقة وزيادة الامان بين المتعاملين إلكترونيا، فهو يقوم بالدور نفسه الذي يؤديه التوقيع التقليدي؛ الأمر الذي دفع المشرع إلى إيلائه بالغ الأهمية وفي إعطائه الحجية القانونية كوسيلة إثبات. وسنرى ذلك في الاتفاقيات الدولية كما في القوانين الوطنية:

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

أولا– في الاتفاقيات الدولية:

كما اكد القانون النموذجي للأونيسترال بشأن التجارة الإلكترونية أن للتوقيع الإلكتروني الحجية نفسها المقررة للتوقيع التقليدي بشرط توافر شرطين أساسيين: – تحديد هوية الشخص الموقع بشكل يعبر فيه عن إرادته بالالتزام بمضمون الوثيقة الإلكترونية. وأن تكون طرقة التوقيع تحقق الموثوقية والأمان.[1]

كما اكد القانون النموذجي للأونسترال بشأن التوقيعات الإلكترونية في المادة 1/6: " عندما يشترط القانون وجود توقيع من شخص يستوفي ذلك الشرط بالنسبة إلى رسالة البيانات التي إن استخدم توقيع الكتروني موثوق به بالقدر المناسب للغرض الذي أنشأت أو أبلغت من أجله رسالة البيانات."

فعندما اشترط قانون الأونسترال النموذجي بشأن التجارة الإلكترونية شرطين لتمتع التوقيع الإلكتروني بالحجية القانونية، جاء قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية أكثر تفصيلا حيث اشترط في التوقيع الالكتروني الملزم بأن يكون موثوقا به من خلال شروط تفصيلية سبق ذكرها.

ثانيا– في القوانين الوطنية:

ساوى المشرع الجزائري والمشرع المصري بين التوقيعين الإلكتروني والتقليدي من حيث الحجية القانونية حيث جاء في المادة /14/ من قانون التوقيع الإلكتروني رقم 15 لسنة 2008: "للتوقيع الإلكتروني في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للتوقيعات في قانون الإثبات في المواد المدنية والتجارية، إذا روعي في

[1]– برني النذير، إثبات العقد الإلكتروني: https: //www.facebook.com/permalink.php تاريخ الاطلاع: 2015/12/03. الساعة: 23: 17.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

إنشائه وإتمامه الشروط المنصوص عليها في هذا القانون والضوابط الفنية والتقنية لهذا القانون."

أما المشرع الجزائري نصت المادة 323 مكرر 1 من القانون المدني على أنه: "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها أن تكون معدة ومحفوظة في ظروف تضمن سلامتها." لقد أسس المشرع من خلال هذا النص مبدأ التعادل الوظيفي L'équivalent fonctionne بين الكتابة في الشكل الإلكتروني والكتابة على الدعامة الورقية. غير أنه لم يأخذ به على إطلاقه بل قيده بشرطين، كما سبق الإشارة إليه، هما:

– إمكانية التأكد من هوية الشخص الذي صدرت عنه هذه الكتابة.

– أن تكون معدة ومحفوظة في ظروف تضمن سلامتها.

فمبدأ التعادل الوظيفي بين الكتابة في الشكل الإلكتروني والكتابة على الورق تم النص عليه في المادة 323 مكرر1 من القانون المدني حيث اعترفت بالكتابة الإلكترونية في إثبات التصرفات والعقود من جهة، وجعلتها معادلة في حجيتها للوثيقة المخطوطة على دعامة ورقية، أي لهما نفس الأثر والفعالية من حيث حجية وصحة الإثبات، لكن السؤال الذي يطرح في هذا الصدد حول نوع الكتابة التي يمكن أن تعادل في حجيتها الكتابة في الشكل الإلكتروني؟، وبمعنى آخر هل يمكن إثبات التصرفات والعقود التي يتطلب القانون في إثباتها الكتابة الرسمية بالكتابة في الشكل الإلكتروني؟[1]

إن موقع المادة 323 مكرر من القانون المدني المقابلة لنص المادة 1316–1 من القانون المدني الفرنسي المتعلقة بتعريف الكتابة الواردة ضمن الباب المخصص بإثبات الالتزام وتحديدا في الفصل الأول الخاص بالإثبات بالكتابة قد أثار جدلا فقهيا، خاصة في فرنسا عما إذا كانت الكتابة في صورتها الحديثة في الشكل الإلكتروني، تعادل في حجيتها

[1]– المادة السابعة – الفقرة 1 من قانون الأونسترال النموذجي بشأن التجارة الإلكترونية لعام 1996.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

حجية الكتابة الرسمية، وبالتالي يمكن من خلالها إثبات عكس التصرفات والعقود المثبتة بكتابة رسمية.

بحيث تتشابه التشريعات العربية الناظمة للمعاملات الإلكترونية فالتشريع الأردني يمنح التوقيع الإلكتروني الحجية في الإثبات إذا استوفى الشروط المنصوص عليها في قانون المعاملات الإلكترونية الأردني المؤقت رقم 85 لسنة 2001.

حيث جاء في المادة 1/10 من هذا القانون: " إذا استوجب تشريع نافذ توقيعا على مستند أو نص على ترتيب أثر على خلوه من التوقيع فإن التوقيع الإلكتروني على السجل الإلكتروني يفي بمتطلبات ذلك التشريع".

المبحث الأول: جرائم الاعتداء والعقوبات والإجراءات المقررة من أجل حماية التوقيع الإلكتروني من منظور التشريعات الغربية

وفرت بعض التشريعات الأجنبية حماية جنائية للتوقيع الالكتروني ومن أبرزها التشريع الفرنسي في إطار قانون العقوبات ، وفي التشريع الأمريكي في إطار جرائم الكمبيوتر الفدرالي.

المطلب الأول: جرائم الاعتداء على التوقيع الإلكتروني في التشريع اللاتيني

قامت فرنسا بتاريخ 13 /2000/3 باستصدار قانون خاص بالتوقيع الإلكتروني رقم 230 لسنة 2000، في صورة تعديل للنصوص المنظمة للإثبات في القانون المدني الفرنسي بما يجعلها متوافقة مع تقنيات المعلوماتية، وكثرة استخدام التوقيع الالكتروني في المعاملات الالكترونية وقد أدرج هذا التعديل في نص المادة 1316 من القانون المدني الفرنسي في ست فقرات.[1]

لم يوفر المشرع الفرنسي حماية خاصة للتوقيع الإلكتروني بل تركها للنصوص العامة، ، وبالرجوع لها نجد أنه تطبق عليه جرائم الإعتداء على النظام المعلوماتي وبياناته

[1]– عبد الحميد ثروت، التوقيع الالكتروني، دار الإسكندرية، مصر، 2007، ص: 173.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

الواردة في المواد 1/323 إلى 7/323 وجريمة التزوير المعلوماتي في المادة 441 من قانون العقوبات الفرنسي والتي هي كالآتي:

الفرع الأول– الاعتداء على النظام المعلوماتي للتوقيع الإلكتروني:

منذ ربع قرن تعد فرنسا، من أوائل الدول الغربية التي سارعت بإصدار تشريعات تهتم بحماية المعلوماتية والتصدي لبعض صور الجرائم التي تقع بسبب التقدم في استعمال الحاسب الآلي، وكذلك شبكة المعلومات الدولية أو بعض الشبكات المحلية، كما هو الحال في شبكة مانتيل الفرنسية. حيث أصدر ترسانة من القوانين تواكب التطور وتتصدى للجرائم الحديثة بأنواعها.

فقد استصدر قانون العقوبات الجديد لعام 1994 واستحدث المشرع نصوصا تتعلق بحماية المعلومات المعالجة، كما جرم التزوير المعلوماتي، الأمر الذي يسبغ حماية جنائية متكاملة على نظام التجارة الإلكتروني.[1]

يوفر المشرع الفرنسي حماية جنائية للنظام المعلوماتي ومحتوياته في المواد 1/323 –7/323 من قانون العقوبات، وباعتبار التوقيع الالكتروني نظام معلوماتي، فيعاقب بالدخول أو البقاء غير المشروع على قاعدة بيانات التوقيع الالكتروني، والاعتداء على سلامته بتزوير التوقيع، ويعاقب أيضا على التلاعب ببيانات التوقيع الالكتروني .

وصدر أخيرا في عام 2000، صدر القانون رقم 2000/230 في 2000/3/13 في شأن الاثبات المتعلق بتكنولوجيا المعلومات واعتماد التوقيع الإلكتروني وقد جاء بما يلي:

-ورد أن التوقيع الإلكتروني إنما يعبر عن شخصية صاحبه، ومن ثم يفيد في إسناد الواقعة التي وقع عليها ذلك الشخص إليه صحتها، وذلك إلى أن يثبت العكس. حيث مدت الحماية لتشمل التوقيع الإلكتروني من خلال المساواة بين التوقيع التقليدي

[1]– عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الاسكندرية، 2005، ص: 470 .

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

والإلكتروني؛ وحسب نص المادة 3/1316 ساوى بين المحرر الكتابي والالكتروني. واعتبارها دليل اثبات مثل الكتابة الورقية تماما بنص المادة 1/1316.

أ- الاعتداء على النظام المعلوماتي للتوقيع الإلكتروني: من خلال

1- الدخول أو البقاء غير المشروع:

يتمثل الركن المادي في الدخول أو البقاء غير المشروع في قاعدة بيانات تتعلق بالتوقيع الإلكتروني، وتصنف هذه الجريمة من جرائم الخطر حيث يتم تجريم السلوك دون توقف ذلك على نتيجة معينة ، فهذه الجريمة ليست من جرائم الضرر التي يشترط فيها إلحاق ضرر بالمجني عليه.[1]

وتعدد هذه الصورة من الجرائم العمدية وبالتالي فإنه لا يتصور وقوعها بطريق الخطأ، وصورة الركن المعنوي فيها هو القصد الجنائي العام .

2- إفساد أو تدمير سير النظام العام: نص عليها المشرع الفرنسي في المادة 323/ 2، ويتمثل الركن المادي لهذه الجريمة في التعطيل والتوقيف، أو بإفساده بأي وسيلة، ويبدو ذلك أمرا منطقيا بالنظر لتعدد الوسائل ولغلبة الصبغة التقنية عليها بحيث يعسر حصرها أو تبويبها.[2]

الفرع الثاني– الاعتداء على بيانات التوقيع الالكتروني :

نص المشرع الفرنسي على جريمة التلاعب ببيانات النظام المعلوماتي بموجب المادة 2/323 من قانون العقوبات الفرنسي. أما الركن المعنوي لهذه الجريمة فيتمثل في القصد

[1] – عبد الفتاح بيومي الحجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني: الحماية الجنائية للتجارة الالكترونية ، دار الفكر الجامعي، مصر 2002 ، ص: 296.

[2] – Gassin, ®. la protection pénale d'une nouvelle universalité de fait en droit français: le système de traitement automatisé des données, Dalloz 1989, 4ème cahier.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

الجنائي العام، بعنصريه العلم والإرادة، ولا يشترط توافر القصد الخاص، بل يكفي القصد الجنائي العام لتحقيق الركن المعنوي .

– تزوير التوقيع الإلكتروني:

وجاء النص على هذه الجريمة في المادة 441 التي نصت على أنه "يعد تزويرا كل تغيير تدليسي للحقيقة ، يكون من شأنه أن يحدث ضررا، ويقع بأي وسيلة كانت، سواء وقع في محرر أو سند أيا كان موضوعه والذي أعد مسبقا كأداة لإنشاء حق أو ترتيب أثر قانوني معين. ولقيام هذه الجريمة لا بد من توافر ركنين مادي ومعنوي، على النحو الآتي:

الركن المادي: يتمثل الركن المادي لهذه الجريمة في فعل تغيير الحقيقة في توقيع الكتروني بأي وسيلة ، ومن أشهر وسائل تزوير التوقيع الالكتروني استخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك، يتم تصميمها على غرار البرامج والأنظمة المشروعة أو محاولة البعض كسر الشيفرة والوصول إلى المحرر الالكتروني أو البيانات واستخدامها.

يتمثل الركن المادي لهذه الجريمة من خلال فعل التلاعب الإلكتروني بأي شكل كان كإزالة ومحو بيانات التوقيع أو تغيير بياناته.[1] أما الركن المعنوي لهذه الجريمة فيتمثل في القصد الجنائي العام، بعنصريه العلم والإرادة، ولا يشترط توافر القصد الخاص، بل يكفي القصد الجنائي العام لتحقيق الركن المعنوي .

– تزوير التوقيع الإلكتروني:

وجاء النص على هذه الجريمة في المادة 441 التي نصت على أنه "يعد تزويرا كل تغيير تدليسي للحقيقة، يكون من شأنه أن يحدث ضررا، ويقع بأي وسيلة كانت، سواء وقع في محرر أو سند أيا كان موضوعه والذي أعد مسبقا كأداة لإنشاء حق أو ترتيب

1– عبد القادر قهوجي، المرجع السابق، ص: 50.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

أثر قانوني معين. ولقيام هذه الجريمة لا بد من توافر ركنين مادي ومعنوي، على النحو الآتي:

الركن المادي: يتمثل الركن المادي لهذه الجريمة في فعل تغيير الحقيقة في توقيع الكتروني بأي وسيلة ، ومن أشهر وسائل تزوير التوقيع الالكتروني استخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك، يتم تصميمها على غرار البرامج والأنظمة المشروعة أو محاولة البعض كسر الشيفرة والوصول إلى المحرر الالكتروني أو البيانات واستخدامها.[1]

الركن المعنوي: تعد هذه الجريمة من الجرائم العمدية ، صورة الركن المعنوي فيها القصد الجنائي العام بعنصريه العلم والإرادة، حيث يجب أن يعلم الجاني بوقائع الجريمة وكونها من المحضورات، ومع ذلك تتجه إرادته إلى الفعل المجرم.

المطلب الثاني: جرائم الاعتداء على التوقيع الالكتروني في التشريع الانجلوسكسوني (الأمريكي)

وبالإضافة إلى قانون اساءة استعمال الكمبيوتر أصدر المشرع الأمريكي في03 جوان سنة 2000 قانونا اتحاديا "للتوقيع الالكتروني والتجارة الوطنية"، وقد سبق هذا القانون جهودا تشريعية ومنها القواعد الاتحادية للتوقيع والسجلات الالكترونية الصادرة في 20 مارس سنة 1997 والتي وضعت لتطبيقها في شركات الأجهزة والقانون الاتحادي للغذاء والدواء ومستحضرات التجميل وقانون الخدمة الصحية العامة.[2]

[1]– عبد الفتاح بيومي الحجازي ، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني: الحماية الجنائية للتجارة الالكترونية ، المرجع السابق ، ص: 290، 305 –304.

[2]– أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني (دراسة مقارنة)، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر: أكاديمية شرطة دبي، مركز البحوث والدراسات، رقم العدد: 1، من 26 إلى 28 نيسان، 2003 بدبي – الإمارات العربية المتحدة

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

وقد وضعت مجموعة العمل تقريرا في جويلية سنة 1992 اقتصرت فيه على إلقاء الضوء على القواعد المتصلة بالتوقيع الإلكتروني؛ غير أنها في 31 أوت 1994 أصدرت تقريرا وضعت فيه القواعد المتعلقة بالسجلات الإلكترونية، كما وضعت قواعد للتوقيع والسجلات الإلكترونية صدرت في 20 مارس سنة 1997. يعد أول تشريع "قانون المعاملات الإلكترونية الموحد" الذي أصدرته ولاية كاليفورنيا في 16 سبتمبر سنة 1999 والذي دخل حيز النفاذ في 01 يناير سنة 2000، وقانون المعاملات الالكترونية الموحد الذي أصدرته نورث كارولاينا والذي دخل حيز النفاذ في 01 أكتوبر 2000. وقد أصدرت ولاية نيويورك تشريعا في 28 سبتمبر سنة 1999 للسجلات والتوقيع الالكتروني وكان هدف هذا التشريع هو تنظيم وتشجيع التعامل بالسجلات الالكترونية وقبول التوقيع الالكتروني في التعاملات التجارية، كذلك أصدرت ولاية كونتكيت قانونا للمعاملات الالكترونية.

في فبراير سنة 2002 ودخل حيز النفاذ في الأول من أكتوبر في ذات السنة، كما أصدرت ولاية بنسيلفينيا قانونا مماثلا في 16 ديسمبر سنة 1999.[1]

وبالرغم من تلك النصوص المتعلقة بالتوقيع الالكتروني، إلا أن تلك القوانين الاتحادية والولائية لم تأت بحماية جنائية خاصة، بل تركتها للنصوص العامة لجرائم الحاسوب. وبالرجوع للقانون الفدرالي الأمريكي المتعلق بالاعتداء على الحاسوب لسنة 1996، نجد أن الفصل 1030 تصمن نصوصا خاصة تجرم الاعتداء على الحاسوب. حيث يجرم المشرع الدخول على البيانات الموجودة بأجهزة الكومبيوتر بدون تصريح أو بـــتجاوز التصريح الممنوح له أيا كانت الوسيلة المستخدمة والحصول على معلومات سرية متعلقة بالدفاع الوطني أو العلاقات الخارجية أو الطاقة النووية، أو الحصول على معلومات موجودة في سجل اقتصادي لمؤسسة مالية، أو يخص مصدر بطاقات مالية أو

[1]– أشرف توفيق شمس الدين، المرجع نفسه، ص: 7.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

تقرير يتعلق بالمستهلكين. كما عاقب المشرع على الدخول في حاسوب يستخدم في التجارة أو الاتصال بين الولايات ويقوم عمدا بنقل برامج أو معلومات أو كود أو نظام الكومبيوتر. ويعاقب المشرع كذلك كل من يمنع أو يحرم أو يتسبب في منع أو حرمان الغير من استعمال كمبيوتر أو خدماته أو نظام أو شبكة معلومات أو بيانات أو برامج. كما يعاقب المشرع على نقل أي مكونات لبرامج أو معلومات أو كود أو أمر دون موافق المسؤولين على الكمبيوتر المستقبل للبرامج أو المعلومات أو الكود أو الأمر إذا أدى هذا النقل إلى خسارة لشخص أو أكثر.[1]

وتجدر الاشارة إلى أنه يمكن توفير حماية جنائية عامة للتوقيع الالكتروني، يكن يلاحظ أن المشرع اهتم بالتفصيل أكثر لأن القانون الأمريكي من القوانين التي تهتم بالأمن القومي والجانب الاقتصادي، يتطلب أن تكون المعلومات المحصل عليها متعلقة بالأمن القومي، أو بإحدى المؤسسات الاقتصادية، ولا يجرم الدخول إلى النظام المعلوماتي، بل لابد أن يترتب على الدخول اتلاف معلومات أو البرامج التي تهتم بالأمن القومي والجانب الاقتصادي.[2]

المبحث الثاني: جرائم الاعتداء والعقوبات والإجراءات الحامية للتوقيع الإلكتروني من منظور المشرع الجزائري والتشريعات العربية.

خصصت بعض التشريعات العربية التوقيع الالكتروني بحماية جنائية، أبرزها التشريع المصري والتشريع التونسي، على خلاف التشريع الجزائري الذي سمله في إطار القواعد العامة في قانون العقوبات والقانون المدني المعدل والمتمم بالقانون رقم 10–05،

[1]– عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني: الحماية الجنائية للتجارة الالكترونية، المرجع السابق، ص: 356.

[2]– صالح شنين، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، رسالة دكتوراه، جامعة بوبكر بلقايد، تلمسان، الجزائر، 2013، (مذكرة منشورة)، ص: 123.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

والذي عدل عن رأيه ذاك بموجب القانون 15–04. وعليه سنبحث جرائم الاعتداء على التوقيع الالكتروني في التشريع الجزائري والمصري والتشريع التونسي، على النحو الآتي:

المطلب الأول: جرائم الاعتداء على التوقيع الالكتروني في التشريع الجزائري:

لم يخص المشرع الجزائري التوقيع الالكتروني بحماية جنائية خاصة على غرار التشريع الفرنسي بل يمكن حمايته جنائيا في إطار قانون العقوبات من خلال جرائم الاعتداء على أنظمة الحاسوب[1] وجريمة التزوير؛ وذلك قبل صدور القانون 15–04 الصادر بتاريخ 2015/2/1، لكن بعد صدور هذا القانون فقد تغيرت المسألة تماما.

الفرع الأول: في القانون 05–10 الصادر في 2005/06/20 المعدل والمتمم للقانون المدني

البند الأول: جرائم الاعتداء على النظام المعلوماتي للتوقيع الالكتروني

يتحقق الاعتداء على التوقيع الالكتروني بالاعتداء على النظام المعلوماتي للتوقيع الالكتروني من خلال الدخول أو البقاء غير المشروع. عالج المشرع الجزائري جريمة الدخول أو البقاء غير المشروع في المادة 394 مكرر ق ع ج، يتمثل الركن المادي في الدخول أو البقاء غير المشروع في قاعدة بيانات التوقيع الالكتروني.[2]

وتصنف هذه الجريمة من جرائم الخطر ، حيث يتم تجريم السلوك دون توقف ذلك على نتيجة معينة، فهذه الجريمة ليست من جرائم الضرر المتطلب فيها حصول ضرر للمجني عليه. وتعدد هذه الصورة من الجرائم العمدية ، وبالتالي فإنه لا يتصور وقوعها بطريق الخطأ، ويتخذ فيها صورة القصد الجنائي العام بعنصري العلم والإرادة .

[1]– راجع المواد 394 مكرر394– مكرر7 من قانون العقوبات الجزائري المقابلة للمواد 323/7 – 323/1 من قانون العقوبات الفرنسي .

[2]– عبد القادر القهوجي، المرجع السابق، ص: 128.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة ن 50.000 دج إلى 100.000 دج. وإذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة تضاعف العقوبة ، وتكون العقوبة الحبس من ستة أشهر (6) إلى سنتين (2)، والغرامة من 150.000 دج إلى 50.000 دج.

ويلاحظ أن المشرع الجزائري لم ينص على جريمة الاعتداء القصدي عبى سلامة النظام المعلوماتي ، بل اكتفى بالنص على الاعتداء على النظام كظرف مشدد ، على خلاف المشرع الفرنسي الذي ينص عليها في المادة 2/323 من قانون العقوبات الفرنسي.

البند الثاني: جريمة الاعتداء على بيانات التوقيع الالكتروني

نص المشرع الجزائري على جريمة التلاعب ببيانات النظام المعلوماتي بموجب المادة 394 مكرر1، ولهذه الجريمة ركنان مادي ومعنوي. يتمثل الركن المادي لهذه الجرائم في إدخال بطريق الغش المعطيات الآلية أو إزالة ومحو أو تغيير بياناته بطريق الغش. أما الركن المعنوي لجريمة التلاعب ببيانات التوقيع الالكتروني ، فيتمثل في القصد الجنائي العام، بعنصريه العلم والارادة.[1] ولا يشترط توافر القصد الجنائي الخاص، إذ يكفب أن تتجه إرادة الجاني إلى الاعتداء على بيانات التوقيع الالكتروني بالادخال أو التعديل أو المحو، وأن يعلم بأن نشاطه ذلك يترتب عليه التلاعب في بيانات التوقيع الالكتروني.

البند الثالث: جريمة تزوير التوقيع الالكتروني

لم ينص المشرع الجزائري على جريمة التزوير المعلوماتي بصراحة كما فعل المشرع الفرنسي في المادة 441 من قانون العقوبات الفرنسي. ويتمثل الركن المادي في تغيير الحقيقة في بيانات التوقيع الالكتروني بطرق مادية أو معنوية ومن شأن ذلك التغيير أن

[1]– محمد رايس، الحماية الجنائية للسند الالكتروني في القانون الجزائري، المرجع السابق، ص: 100.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

يؤدي إلى حصول ضرر.[1] ولا يشترط توافر القصد الجنائي الخاص ،إذ يكفي أن تتجه إرادة الجاني إلى الاعتداء على بيانات التوقيع الالكتروني بالإدخال أو التعديل أو المحو، وأن يعلم بأن نشاطه ذلك يترتب عليه التلاعب في بيانات التوقيع الالكتروني.

الفرع الثاني: في قانون التصديق والتوقيع الإلكتروني رقم 15–04 الصادر في 2015/2/1

ويتعلق الأمر بالجرائم التي قد تبدر من مؤدي خدمات التصديق الإلكتروني بمناسبة آداء مهامه، أو تلك التي قد تصدر عن المعتدي خارج إطار مؤدي خدمات التصديق.

البند الأول: جرائم الاعتداء على التوقيع الالكتروني من طرف مؤدي خدمات التصديق الإلكتروني

أ.الإخلال بإلتزام إعلام السلطة الإقتصادية بالتوقف عن نشاطه في الآجال المحددة في المادتين58و59: ففي حال عدم إلتزام مؤدي خدمات التصديق الإلكتروني بإعلام السلطة الإقتصادية للتصديق الإلكتروني برغبته وفي الآجال المحددة قانونا أو بأي فعل قد يؤدي إلى ذلك؛ والذي يترتب عليه في الاحوال العادية سحب الترخيص؛ وأيضا في عدم إعلام السلطة الإقتصادية فورا عن أي وقف نشاطه لأسباب خارجة عن نطاقه؛ والتي تقوم في الأحوال العادية بإلغاء شهادة التصديق بعد تقدير الأسباب المقدمة. ففي الحالتين المذكورتين توقع الجزاءات الحبس من شهرين إلى سنة، وبغرامة من 200.000 دج إلى 1.000.000 دج، أو بإحدى هاتين العقوبتين فقط.

ب.حيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاص بالغير: يعاقب بالحبس من ثلاثة أشهر إلى ثلاثة سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج؛ أو بإحدى هاتين العقوبتين فقط.

[1]– عبد القادر القهوجي، المرجع السابق ، ص: 155.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

ج.الإخلال عمدا بالتزام تحديد هوية طالب شهادة تصديق الكتروني موصوفة: بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 20.000دج إلى 200.000 دج أو بإحدى هاتين العقوبتين فقط.

د. حالة الإخلال بواجب الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة يعاقب بالحبس من 3 أشهر إلى 2سنة وبغرامة 200.000 دج إلى 1.000.000 دج أو بإحدى هاتين العقوبتين فقط.

ه–عدم إعتبار الموافقة الصريحة في جمع البيانات الشخصية للمعني؛ أو فعل التعدي إلى معلومات أخرى غير ضرورية؛ أو في حال استعمالها لأغراض أخرى، في هذه الأحوال يعاقب مرتكب هذه الأفعال بالحبس من 6 أشهر إلى 3 سنوات، أو بغرامة من 200.000 إلى 1.000.000 دج أو بإحدى هاتين العقوبتين فقط.

و.مزاولة أداء نشاط خدمة التصديق الإلكتروني دون ترخيص أو مواصلته بالرغم من سحب الترخيص فيعاقب بالحبس من سنة إلى 3 سنوات وبغرامة 2.00.000 إلى 2.000.000 دج أو بإحدى هاتين العقوبتين فقط.

ز.كشف معلومات سرية من طرف المكلف بالتدقيق بمناسبة آداء وظيفته فيعاقب بالحبس من 3 اشهر إلى سنتين وبغرامة من 20.000 دج إلى 200.000 دج أو بإحدى هاتين العقوبتين فقط.

ح. الشخص المعنوي المرتكب لأحد الأفعال المنصوص عليها سابقا بغرامة تعادل 5 مرات الحد الأقصى المنصوص عليها بالنسبة للشخص الطبيعي.

البند الثاني: جرائم الاعتداء على التوقيع الالكتروني من طرف الغير

كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة يعاقب بالحبس من ثلاث أشهر إلى ثلاث سنوات وبغرامة من 20.000 دج إلى 200.000

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

دج أو بإحدى هاتين العقوبتين فقط. وفي حال الشخص الإعتباري فالعقوبة هي 5 مرات الحد الأقصى للغرامة.

البند الثالث: جرائم الاعتداء على التوقيع الالكتروني من طرف صاحب التوقيع نفسه

إستعمال شهادة التصديق الإلكتروني الموصوفة لغير الأغراض الممنوحة من أجلها فيعاقب بغرامة من 2.000 إلى 200.000دج.

المطلب الثاني: جرائم الاعتداء على التوقيع الالكتروني في التشريع المصري:

نص المشرع المصري على جرائم التوقيع الالكتروني في المادتين 21 و23، من قانون رقم 15 لسنة 2004 المتعلق بتنظيم التوقيع الالكتروني.

الفرع الأول– الجرائم المنصوص عليها في المادة 21 من قانون التوقيع الالكتروني:

نصت المادة 21 من قانون التوقيع الالكتروني المصري على: "أن بيانات التوقيع الالكتروني والوسائط الالكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الالكتروني سرية، ولا يجوز لمن قدمت إليه أو بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجله ".

ويتضح من المادة 21 من قانون التوقيع الالكتروني، أن المشرع المصري يجرم إفشاء بيانات التوقيع الالكتروني، وجريمة استخدام هذه البيانات في غير الغرض المخصص لها، على التفصيل الآتي:

أ– جريمة افشاء بيانات التوقيع الالكتروني:

يتضح من خلال المادة 21 من قانون التوقيع الالكتروني المصري ، أنه يتطلب لقيام هذه الجريمة ، توافر ركنين مادي يتمثل في إفشاء للغير بيانات التوقيع الإلكتروني والوسائط الالكتونية والمعلومات من قبل الجهة المرخص لها بإصدار شهادات التصديق

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

الإلكتروني للغير أو استخدامها في غير الغرض الذي قدمت من أجله. كما يتطلب فيها إلى جانب الركن المادي ركن معنوي يتخذ صورة القصد الجنائي العام دون القصد الجنائي الخاص، على التفصيل الآتي:

الركن المادي: يتمثل الركن المادي في هذه الجريمة في إفشاء بيانات التوقيع الالكتروني، أي نشرها وإطلاع الغير عليها، السرية بعد أن كان العلم بها قاصرا على الذين ائتمنوا عليها بحكم وظيفتهم ويتحقق الركن المادي للجريمة بمجرد انتهاك بيانات سرية البيانات وخصوصيتها حتى ولو لم يترتب على الفعل إي نتيجة ، فالجريمة سلوكية يكتفي فيها المشرع بتحقق السلوك المادي.

الركن المعنوي: هذه الجريمة العمدية يلزم لقيامها توافر القصد الجنائي باتجاه إرادة الجاني إلى إساءة استخدام بيانات التوقيع اللكتروني، باستعمالها لغير الغرض المخصص لها، مع علمه بذلك وقبو ل النتائج المترتبة على هذا السلوك الاجرامي الذي لا يتصور وقوعه بطريق الخطأ. ومتى تحقق الركن المادي والركن المعنوي وجب إنزال العقوبة على الجاني دون النظر في الباعث الذي دفعه إلى إساءة استخدام بيانات التوقيع الالكتروني.

الفرع الثاني– الجرائم المنصوص عليها في المادة 23 من قانون التوقيع الالكتروني:

تنص المادة 23 من قانون 04–15 لسنة 2004 على أنه " مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في قانون آخر يعاقب بالحبس وبغرامة لا تقل عن 10 آلاف جنيه ولا يتجاوز مئة ألف جنيه، أو بإحدر هاتين العقوبتين كل من:

أ– أصدر شهادة تصديق دون الحصول على ترخيص .

ب– أتلف أو عيب توقيعا أو وسيطا أو محررا إلكترونيا، أو زور شيئا من ذلك بطريق الاصطناع أو التعديل أو بأي طريق آخر.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

ج- استعمل توقيعا أو وسيطا أو محررا الكترونيا معينا أو مزورا مع علمه بذلك

د- توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني أو اخترق أو اعترضه أو عطله عن أداء وظيفته، وفي حالة العود تزداد بمقدار مثل العقوبة المقرر لهذه الجرائم .

1- جريمة إصدار شهادة التصديق الالكتروني بدون ترخيص:

وقد نص المشرع المصري على هذه الجريمة في المادة 23/أ من قانون التوقيع الالكتروني، ويتطلب لقيامها توافر ركن مادي ومعنوي.

الركن المادي: يتمثل السلوك الاجرامي في هذه الجريمة، في انتحال الجاني صفة مزود خدمات التصديق المرخص له بخلاف الحقيقة، ويصدر شهادات التصديق الالكتروني دون ترخيص بذلك من الهيئة العامة لتنمية صناعة تكنولوجيا المعلومات".[1] وبالتالي تقع هذه الجريمة إذا أصدر الجاني شهادة تصديق الكتروني دون الحصول على ترخيص مخالفة للمادة 19 من قانون التوقيع الالكتروني. والسبب في تجريم هذا الفعل هو الآثار الخطيرة المترتبة على شهادة التصديق الالكترونية في حق الغير، حيث يكون مضمونها التسليم بصحة بيانات التوقيع الالكتروني، أو بيانات المعاملة المطلوب صدور شهادة التصديق عنها. ويمكن القول أن هذه الجريمة من جرائم الخطر، أو جرائم السلوك المجرد حيث يتكامل قيام الركن المادي فيها بمجرد إتيان الجاني لسلوك إصدار شهادة التصديق الالكتروني بدون ترخيص، دون تطلب حصول ضرر بجهة ما أو شخص ما.

الركن المعنوي: وهذه الجريمة من الجرائم العمدية، لابد فيها من توافر القصد الجنائي العام ، وذلك بأن يعلم الجاني بأنه يقوم باصدار الشهادة دون ترخيص، وأن

1- عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الانترنت، دار الفكر الجامعي، الاسكندرية، مصر، 2006 ، ص: 157.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

تتجه ارادته إلى هذا السلوك[1]، ومن ثمة فلا يتصور وقوع هذه الجريمة بطريق الخطأ بل يجب أن تنصرف الإرادة إلى هذا الفعل، انطلاقا من المادة 23/1.

1- إتلاف أو تعييب أو تزوير التوقيع الالكتروني:

جرم المشرع الفرنسي هذه الأفعال في المادة 23/ب من قانون التوقيع الالكتروني، كالآتي:

أ-جريمة اتلاف أو تعييب التوقيع الإلكتروني:

الركن المادي: ويتحقق الركن المادي في هذه الجريمة باتلاف أو تعييب التوقيع الالكتروني، ويتحقق فعل الاتلاف بإفقاد البرنامج المعلوماتي الخاص للتوقيع الالكتروني قدرته على العمل، أما تعييب التوقيع الإلكتروني يكون بفقده القدرة على العمل أو الصلاحية بصورة جزئية، كأن يصدر التوقيع مشوها أو غير صالح.[2] ومن ثمة فلا يتصور وقوع هذه الطريمة بطريق الخطأ بل يطب أن تنصرف الأرادة من هذا الفعل، انطلاقا من المادة 23/1. ويتطلب لقيام هذه الريمة ضرورة توافر الضرر، فالضرر هو النتيجة الإجرامية المترتبة على الاعتداء وترتبط بالفعل برابطة سببية قانونية حال توافر أركان الجريمة، ويستوي أن يكون الضرر ضررا ماديا أو معنويا.

الركن المعنوي: هذه الجريمة من الجرائم العمدية، يتطلب فيها توافر ركن معنوي يتمثل في القصد الجنائي العام بعنصريه العلم والارادة، فيجب أن يعلم الجاني بأن فعل الاتلاف أو تعييب التوقيع الالكتروني محظور ويعاقب عليه قانون، وأن تتجه إرادته للفعل المجرم، أما إذا كان الاتلاف أو التعييب ناتج عن حادث غير مقصود كما لو وقع من العامل شيء على الجهاز أدى إلى إتلاف جزء منه فلا تقوم هذه الجريمة. ولا تتطلب

1- عبد الفتاح حجازي، التوقيع الالكتروني، دار الفكر الجامعي، الاسكندرية، مصر، 2006، ص: 540.

2- عبد الفتاح حجازي، حماية المستهلك عبر شبكة الانترنت ، المرجع السابق، ص: 159

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

هذه الجريمة قصدا خاصا، وإنما يكتفي بشأنها القصد العام العام بعنصريه العلم والارادة، فتقوم الجريمة بتوافر الركن المادي والقصد الجنائي العام .

ب–جريمة تزوير التوقيع الالكتروني:

الركن المادي: يتمثل الركن المادي لهذه الجريمة في تزوير التوقيع الالكتروني بتغيير الحقيقة في التوقيع الالكتروني بطريق الاصطناع أو التعديل أو التحويل، أو بأي طريق على نحو يضر بالغير.

الركن المعنوي: يمثل الركن المعنوي في هذه الجريمة في القصد الجنائي العام، بأن يكون الجاني عالما بأنه ترتكب جريمة وأن تتجه إرادته إلى تزوير التوقيع الالكتروني، فمجرد إهماله في تحري الحقيقة مهما كانت درجته لا تتحقق به جريمة التزوير. ويتطلب كذلك تزافر القصد الجنائي الخاص لدى الجاني إلى جانب القصد الجنائي العام وهو نية استعمال التوقيع الالكتروني فيما زور من أجله، على خلاف جريمة الاتلاف التي اكتفى فيها المشرع المصري بالقصد الجنائي العام.[1]

الركن المعنوي: تعتبر هذه الجريمة من الجرائم العمدية ، تتحقق بتوافر القصد الجنائي العام فلابد أن يعلم الجاني بأن حصوله على التوقيع الالكتروني يعتبر حق، وأنه يخترق التوقيع الالكتروني أو يعترضه، أو يعطله، وأن تتجه إرادته إلى ذلك الفعل، ولا يتطلب المشرع في هذه الطريمة قصدا جنائيا خاصا، بل اكتفى بالقصد الجنائي العام.[2]

لذلك ينتفي القصد الجنائي إذا قام الشخص الذي يتعامل مع النظام بالحصول على التوقيع الالكتروني أو اختراقه أو اعتراضه أو تعطيله نتيجة الخطأ، فهذه الجريمة من الجرائم العمدية لا يتصور وقوعها بطريق الخطأ.

1– عبد الفتاح بيومي حجازي، حماية المستهلك عبر الانترنت، المرجع السابق، ص: 161.
2– عبد القدر قهوجي، المرجع السابق، ص: 140– 141 .

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

المطاب الثالث: جرائم الاعتداء على التوقيع الالكتروني في التشريع التونسي:

نظرا للانتشار الواسع للتوقيع الالكتروني في إطار المعاملات التجارية ، كان لابد من إقرار حماية جزائية ضد الاعتداءات التي يتعرض لها التوقيع الالكتروني، لذا نظم المشرع المشرع التونسي حماية جنائية خاصة بالتوقيع الالكتروني بموجب القانون المؤرخ في 9 أوت 2000 المتعلق بالمبادلات والتجارة الالكترونية.

الفرع الأول – جريمة مباشرة خدمات التصديق بدون ترخيص

اقتضى الفصل 46 من نفس القانون "يعاقب كا من يمارس نشاط مزود خدمات التصديق الالكتروني بدون ترخيص مسبق طبقا للفصل 11 من هذا القانون بالسجن لمدة تتراوح بين شهرين و3 سنوات وبخطية تتراوح بين 1000 و10000 دينار أو بإحدى هاتين العقوبتين" ويتضح بأن المشرع التونسي يتطلب لقيام هذه الجريمة توافر ركن مادي يتمثل في ممارسة نشاط مزود خدمات المصادقة الالكترونية بدون ترخيص، وركن معنوي يتخذ صورة القصد الجنائي العام ، على النحو الآتي:

الركن المادي: يتحقق الركن المادي في هذه الجريمة بالتعامل في بيانات التجارة الالكترونية دون ترخيص، فالجريمة تعتبر جريمة سلوكية.[1] وتشرف الوكالة الوطنية للمصادقة الالكترونية على منح الترخيص اللازم لممارسة نشاط وخدمات المصادقة الالكترونية، وتحقق الوكالة من خلال هذه الصلاحية رقابتها على الأشخاص الذين يمكن أن توكل لهم الوظائف المتعلقة بشهادات المصادقة والامضاء الالكتروني، والتثبت من مدى توفر الشروط اللازمة للاضطلاع بهذه المهام على الوجه المطلوب ، لذلك كان لابد من زجر كل ممارسة لهذه الوظائف خارج مراقبة الوكالة الوطنية للمصادقة االالكترونية، ودون الحصول على الترخيص المذكور.

1– عبد الفتاح بيومي حجازي، التوقيع الالكتروني ، المرجع السابق، ص: 133.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

الركن المعنوي: وهذه الجريمة هي جريمة عمدية يكفي لتوافرها توفر القصد الجنائي العام بعنصريه العلم والإرادة، أي أن يكون المزود على علم أنه غير مرخص له في مباشرة النشاط، ومع ذلك تتجه لإرادته إلى القيام بذلك. ومتى قامت الجريمة فإنه يعاقب الجاني بالسجن لمدة شهرين إلى ثلاث سنوات وبخطية تتراوح بين 1000 و10.00 دينار أو بإحدى هاتين العقوبتين.

الفرع الثاني– جريمة التصريح عمدا بمعطيات خاطئة

وينص عليها المشرع التونسي في المادة 47 بأنه: " يعاقب كل من صرح بمعطيات خاطئة لمورد خدمات التوثيق الالكتروني لكافة الأطراف التي طلب منها أن تثق بإمضائه للسجن لفترة تتراوح بين 6 أشهر وعامين، وبغرامة تتراوح بين 1000 و10.000 دينار أو بإحدى هاتين العقوبتين وبالتالي الهدف من تجريم هذا الفعل هو حماية عملية التجارة الالكترونية وأطرافها من استقبال معلومات خاطئة تؤثر على حقوق أطراف التعاقد أو على الثقة المفترضة في هذه التجارة لذلك فهذه الجريمة من شأن العقاب عليها زيادة الثقة لدى المتعلمين في هذه التجارة والحفاظ على حقوقهم، ويتطلب لقيام هذه الجريمة ركنين، ركن مادي وركن معنوي.

الركن المادي: تتحقق هذه الجريمة بالتصريح بمعطيات خاطئة، أي إعطاء معطيات غير صحيحة سواء كان ذلك من قبل أي شخص، وسواء أعطيت هذه البيانات إلى مورد خدمات التوثيق الالكتروني أو أحد أطراف التعاقد أو طرف آخر كبنك. هذه الجريمة مثل سابقتها من الجرائم تعد من قبيل جرائم السلوك المجرد وليست من جرائم الضرر، بمعنى أن المشرع لا يشترط لقيام الركن المادي فيها حلول ضرر معين، وإنما يكفي تحقق النشاط الاجرامي وهو إعطاء المعطيات غير الصحيحة.

الركن المعنوي جريمة التصريح بمعطيات غير صحيحة هي جريمة عمدية، حيث تطلب المشرع صراحة توافر القصد الجنائي من خلال عبارة " صرح عمدا" ولذلك

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

فصورة القصد هو القصد الجنائي العام.[1] وبالتالي يجب أن يعلم أن ذلك الفعل محظور وفقا للقانون ومع ذلك تنصرف إرادته إلى فعل الإدلاء بالمعطيات غير الصحيحة ، وكذلك إلى قبول النتيجة المترتبة على فعله بوصفها مخالفة للقانون ، لهذا لا يتصور وقوع الجريمة بطريق الخطأ لأن فعل الإعطاء ناتج عن قصد. ولا تتطلب هذه الجريمة لقيامها قصد جنائي خاص أو نية خاصة يتعين توافرها لدى الجاني. ذلك أن مجرد الادلاء بمعلومات خاطئة تقوم به هذه الجريمة.[2]

ويعاقب المشرع على هذه الجريمة بالسجن لمدة تتراوح بين 6 أشهر إلى عامين، وبغرامة تتراوح بين 1000 الى 10.000 دينار أو بإحدى هاتين العقوبتين.

الفرع الثالث– جريمة فض تشفير إمضاء إلكتروني

يقتضي الفصل 48 من قانون المبادلات والتجارة الالكترونية 15–04 يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية متلقة بامضاء غيره بالسجن لمدة تتراوح بين 6 أشهر وعامين وبغرامة تتراوح بين 1.000 و10.000 دينار أو بإحدى هاتين العقوبتين. ولقيام هذه الجريمة يتطلب توافر ركنين مادي ومعنوي ، على النحو الآتي:

الركن المادي: والركن المادي في هذه الجريمة يتمثل في اختراق التشفير المتعلق بالامضاء الالكتروني وبالتالي كل من استعمل عناصر تشفير غيره بصفة غير مشروعة يشكل اختراقا لنظام التشفير يجعله عرضة للمتابعة الجزائية. وهذه الجريمة من جرائم السلوك المجرد لا يتطلب فيها تحقق نتيجة اجرامية بل تقوم بمجرد فض شفرة التوقيع الالكتروني، دون حصول ضرر للمجني عليه.

1– عبد الفتاح بيومي حجازي ، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني: الحماة الجنائية للتجارة الالكترونية ، المرجع السابق، ص: 276 –275.

2– عبد الفتاح بيومي حجازي ، المرجع نفسه، ص: 290.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

وما يلاحظ أنه بالنظر للصبغة الفنية لهذه الجرائم فقد حرص المشرع أن تكون معاينتها من قبل أشخاص مختصين حتى تتم الاحاطة بهذه الجرائم المعقدة، لكن دون أن يمنع ذلك من إمكانية معاينة أعوان الضبطية العدلية أو القصائية لمثل هذه المخالفات .

الركن المعنوي: هذه الجريمة من الجرائم العمدية التي تتطلب لقيامها القصد الجنائي العام بعنصريه العلم والإرادة ، وبالتالي يجب أن يعلم الجاني أن ذلك الفعل محضور وفقا للقانون ومع ذلك تنصرف إرادته إلى فعل الاعتداء على البيانات المشفرة.[1]

المبحث الثالث: مدى نجاعة هذه الإجراءات الحمائية للتصدي لجرائم الإعتداء على التوقيع الإلكتروني

المطلب الأول: أهمية حماية التوقيع الإلكتروني

إن التوقيع الإلكتروني في حد ذاته نوع من الحماية، فليست حمايته هي مطلب في حد ذاتها بقدر ما هو مطلب لحماية البيانات التي يمكن توقيعه من الوصول إليها؛ فالغاية هنا هي حماية الوصول إلى تلك البيانات التي يسمح الولوج إليها عبر هذا التصديق.

فالهدف من التوقيع الإلكتروني يندرج تحت الأمن والسلامة الرقميين، وعند ثبوت صحتها فإنها بالطبع تحقق جميع الجوانب العلمية والأهداف المرجوة منها ولعدة أهداف قانونية بحتة تبعد المتطفلين عن التلصص وسرقة البيانات[2]، وتكمن الموثوقية التي يتمتع بها هذا النوع من التوقيع بإحدى طريقتين:

-عن طريق سلطات التوثيق التي تقوم بمنح شهادة رقمية لذوي الشأن تؤكد حجية إرسال الرسالة حيث يتم تخزين هذه الشهادة على الكمبيوتر ()، ويمكن أن يصل

1– عبد الفتاح بيومي حجازي ، المرجع نفسه، ص: 292.

2– أسامة الكسواني، التوقيع الإلكتروني، المجلة الإلكترونية، ص: 3. مقال منشور:
http: // newsmaktoub.com/article

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

إلى الجميع للتحقق من مطالبتها للأصل عبر التوقيع الرقمي للسلطة حيث يمكن التثبت منها بالمفتاح العام الخاص بالشهادة.

-عن طريق قيام مستلم الرسالة بتشفير جزء من الرسالة باستخدام المفتاح العام المرسل وبرنامج التشفير المستخدم في تشفير الرسالة، فإذا كانت النتيجة واحدة فهذا يدل على صحة الرسالة والتوثق من المرسل.[1]

المطلب الثاني: صناعة أمن المعلومات والإجراءات الاحترازية المتعلقة بالحماية

الفرع الأول: أمن المعلومات وصناعته

مكمن مشاكل أمن المعلومات يكون على مستوى المستهلك أو الزبون، على مستوى العنوان الإلكتروني للمؤسسة التي تتعامل عبر الإنترنت، فتأمين المعلومات سمح بضمان من الناحية التكنولوجية المسار الجيد والصحيح للمعاملة التجارية وذلك بالضمان لأنظمة الحواسيب وتأمين تحويل البيانات ما بينها وذلك بالقدرة على:

-القدرة على الاستعمال (توفير هذه الخدمات، الموارد والبرامج اللائقة).

-عدم السماح بالدخول للمعطيات والموارد الرقمية سوى للأشخاص والبرامج ذات الاختصاص لضمان (السرية، صحة البيانات والمعطيات وكذلك الخدمات).

-التأكيد وتبيان أن المعاملة قد حدثت فعلا (سيرورة المعاملة، دلائل عدم الرجوع).

-تطبيق المعاملة وجعل الخدمات المرجوة في أوضاع جيدة والاستعمال اللائق (استمرارية الخدمات، أمن الاستعمال اللائق (استمرارية الخدمات، أمن الاستعمالات وفعالية البرامج).[1]

1- نضال إسماعيل برهم، أحكام عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، 2005، عمان، ص: 174–175.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

فصناعة أمن المعلومات تتزايد تقنياتها ومجالاتها يوما بعد يوم وتزدحم الأسواق بمنتجاتها، فيوجد على سبيل المثال أكثر من خمسين شركة في العالم توفر برمجيات جدران الحماية pare-feu وهذه مجرد تقنية واحدة من تقنيات أمن المعلومات بمحاولة جذب انتباه العملاء خاصة أولئك الذين يتعاملون مع شبكات الإنترنت.[2]

الفرع الثاني: الإجراءات والتدابير الاحترازية المتعلقة بالحماية من الجرائم المعلوماتية

تقوم الكثير من المواقع العالمية بعدة إجراءات وقائية وترتيبات متعلقة بتكنولوجيا الحماية فتتخذ بعض هذه الإجراءات:

- حصر فتح المعلومات المشفرة على عدد قليل من الموظفين الموثوق بهم.

- يتم فتح المعلومات بعد فتحها وفرزها إلى الأقسام المتخصصة إلكترونيا بحيث لا يتم إعطاء رقم بطاقة الدفع إلى قسم المحاسبة لخصم المبلغ ويتم تشفيرها مرة أخرى ولا يمكن لأي شخص أن يطلع عليها.

- يقوم الموقع بعمل عدة طبقات من الصلاحيات للموظفين بحيث لا يمكن لأي موظف الوصول إلى معلومات غير مسموح له بالوصول إليها، فمثلا موظف في قسم الشحن ليست له صلاحيات غير الوصول إلى معلومات محددة مثل طبيعة السلعة ورقم الطلبية وتاريخها وعنوان المرسل إليه.

1 –SolangeGhernaouti-Hélie, Internet,, stratégie et technologie, Edition Dunod, Paris,2000,p.p: 228-229.

2– حسن طاهر داوود، الحاسب وأمن المعلومات، معهد الإدارة العامة، مكتبة الملك فهد الوطنية، الرياض، ص: 30–31.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

المطلب الثالث: مدى فاعلية الإجراءات والقوانين في مجال مكافحة هذه الجرائم

إن الفاتورة الإجمالية لجرائم المعلومات في 2011 وحده تقدر بـــ 388 مليار دولار أمريكي[1]، أما التكلفة النقدية المباشرة لهذه الجرائم والمتمثلة في الأموال المسروقة ونفقات إزالة آثار الهجمات فتقدر بحوالي 114 مليار دولار. ومعنى ذلك أن القيمة المالية لجرائم المعلومات أكبر من السوق السوداء لمخدرات المارخوانا والكوكايين والهيروين مجتمعين، والتي تقدر بحوالي 288 مليار دولار، وتقترب من قيمة السوق العالمية للمخدرات عموما والتي تصل إلى 411 مليار دولار، وأعلى من الإنفاق السنوي لمنظمة الأمم المتحدة للأمومة والطفولة اليونيسيف بحوالي 100 ضعف، كما تساوي هذه الخسائر ما تم إنفاقه خلال 90 عاما على مكافحة الملاريا وضعف ما تم إنفاقه على التعليم في 38 عاما. وقد بلغ المعدل الزمني لوقوع جرائم المعلومات حول العالم 50 ألف جريمة واعتداء في الساعة، تأثر بها 589 مليون شخص، وهو رقم أكبر من عدد سكان الولايات المتحدة وكندا وغرب أوربا مجتمعين، ويعادل 9٪ من إجمالي سكان العالم.

وتوزعت هذه الجرائم ما بين جرائم الفيروسات والبريد الإلكتروني الملوث والضار، وجرائم الاحتيال والنصب والاصطياد (الحصول على معلومات بنكية سرية)، والجرائم المتعلقة باختراق الهواتف المحمولة.

حملت هذه الاعتداءات الكثير من الدلائل على أن الأمر تخطى كل الحدود المعتادة، وصار جولات صراع مكشوفة بين الدول وبعضها البعض، حتى أن جرائم المعلومات باتت أداة جديدة في الصراع السياسي والاقتصادي.

1- تقرير The Norton Cybercrime Report 2011 الصادر عن شركة سيمانتك العالمية المتخصصة في أمن المعلومات حول أوضاع جرائم المعلومات في عام 2011، والذي حمل عنوان "صورة إجمالية لأوضاع أمن المعلومات حول العالم.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

فعلى سبيل المثال غذا ما أخذنا ما تم اكتشافه بخصوص فيروس "دوكو Duqu "، فسنجد أن نتائج الدراسات الخاصة بحماية البنية التحتية الحساسة مقلقة، إذ الغرض الذي صمم من أجله الفيروس "دوكو" هو جمع المعلومات الاستخبارية ومعلومات عن الأصول Assets من منظمات معينة مثل الشركات المصنعة للمكونات التي توجد عادة في بيئة التحكم الصناعي، كما أن من يقفون وراء هجوم دوكو كلنوا يبحثون عن معلومات مثل وثائق التصميم التي يمكنها أن تساعد في المستقبل لشن هجوم على المنشآت التحكم الصناعي، ويمثل "دوكو" الجيل الأحدث من "ستكسنت" Stuxnt" الذي ذكرت تقارير عديدة أن الأمريكيين استخدموه في إحداث فوضى داخل البرنامج النووي الإيراني. وفي هذه المرحلة فإنه من غير المبرر الاعتقاد بأن من يقف وراء هجوم "دوكو" لم يتمكن من الحصول على المعلومات الاستخبارية التي يبحث عنها، وإضافة إلى ذلك فمن المحتمل أن هجمات أخرى لجمع المعلومات قد بدأت بالفعل و لم يتم اكتشافها بعد.

وخلال السنوات الأخيرة عرف العالم جماعات متخصصة من القراصنة الإلكترونيين مثل الأنونيموس Anonymos وLulzSec وغيرهما. حيث استهدفت تلك الجماعات الشركات والأفراد لتحقيق مآرب سياسية مختلفة. ويرجح خبراء من شركة تريند ماكرو –إحدى الشركات المتخصصة في أمن المعلومات الاستخبارية –ان تزداد أنشطة مثل هذه الجامعات خلال الأعوام القادمة، بل وأن تتزايد قدرتها على اختراق شبكات الشركات والإفلات من محاولات رصدها ومقاضاتها.[1]

1– جمال محمد غيطاس، الأمن المعلوماتي والجرائم الإلكترونية...أدوات جديدة للصراع، مركز الجزيرة للدراسات، مقال منشور بتاريخ: 1 مارس 2012 للمزيد الاطلاع على الرابط:
http//studies.aljazeera.net/ar/issues/2012/02/201222913222865296O.html
تاريخ الاطلاع: 2016/09/05.

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

وهي مؤشرات قوية على ضعف الإجراءات والقوانين المتخذة لردع الجرائم المعلوماتية عموما والحد من الاعتداءات على التوقيع والمصادقة الإلكترونية خصوصا، خصوصا إذا علمنا انخراط الدول والحكومات في هذه الجرائم بدوافع ومصالح معينة. وهو منحى خطير لجرائم من هذا النوع في هذه السياقات بحيث أنه في كثير من الاعتداءات على أنظمة الحماية والجدران النارية تعمد منظمات ومكومات دولية إلى مجموعات الهاكرز والكراكرز وبدفع مكافئات مجزية من أجل اختراق أنظمة شديدة الحماية والترسنة، فإذا كان الأمر كذلك فماباالك بنظم هشة من قبيل دول العالم الثالث والدول العربية، ونماذج تلك الاختراقات حتى في عقر المارد الأمريكي إذ أثبتت تسريبات ويكيليكس وبنما بابرز أن لا أحد في منآى عن مثل هذه الاختراقات والهجومات الكاسحة لنظم المعلومات والبرمجة. خصوصا إذا علمنا أن هذه المعطيات تمثل جزءا بسيطا من الحقيقة التي تحاول معزم المؤسسات والنظم إلى المدرارة وإخفاء حجم الخسائر التي تتكبدها لما للكشف عنها من أضرار قد تنسف بهذه المؤسسات وتقضي على كيانها مع زبائنها والمتعاملين معها.

الخاتمـــة:

إن التطور المتزايد والمطرد والتحول الكبير نحو استعمال التكنولوجيات الحديثة وفتح المجال واسعا نحو تجارة تواكب التطور والعصر، أحدث نقلة نوعية في أساليب الإجرام وسرعة في تأقلمها مع المتغيرات واستغلال الثغرات من أجل تحقيق مكاسب كبيرة بعيدا عن بطئ التشريع والاعتراض الأمني.

لكن ذلك ليس بالمبالغة في استحداث وإصدار النصوص بحسب كل الحالات والأشكال كما فعلت التشريعات العربية، ولكن بمواكبة التقدم الحاصل من خلال مرونة وتطويع النصوص العامة في وجعلها قابلة لمواجهة الجرائم الحديثة؛ لأن الأمر يطول ويصعب في إيجاد عقوبة لكل جريمة كما تفعل التشريعات العربية؛ والسبب هو التعلق

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

بالأساليب القديمة وعدم الثقة والأمان في التحول الحاصل في طرق المعاملات على شبكات النات وعبر المواقع التجارية. ولا بأس من تشريع أو تشريعين لجرائم بعينها كالإتلاف المعلوماتي وذلك بحسب ما ينص به الخبراء وأهل الاختصاص.

لم يخص التشريع الفرنسي والجزائري التوقيع الالكتروني بحماية جنائية خاصة، بل يمكن حمايته في إطار القواعد العامة لقانون العقوبات من خلال جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، وجريمة التزوير، وكذلك الحال بالنسبة للتشريع الفدرالي الأمريكي من خلال جرائم الكمبيوتر، إلا أن تلك الحماية قاصرة كما أسلفنا على مصالح الدولة العليا أو إحدى المؤسسات الاقتصادية. على خلاف تلك التشريعات خصت بعض التشريعات العربية التوقيع الالكتروني بحماية جنائية كالتشريع التونسي الذي جاء بحماية شملت العديد من الجرائم سواء في إطار النصوص العامة أم في النصوص الخاصة ، وجاء بعقوبات مناسبة، كما خصه التشريع المصري بحماية جنائية في إطار القانون رقم 15–2004 المتعلق بالتوقيع الالكتروني في المادتين 12و 23، وشملت تلك الحماية العديد من الجرائم ، لكن المشرع لم يجرم الشروع وبالتالي لا عقاب على الشروع فيها، و لم يميز بين تعطيل التوقيع الالكتروني الذي يترتب عليه توقيف مصلحة خاصة، أو توقيف مصلحة عامة ، كما لم يجرم صنع أو حيازة برامج معدة للاعتداء على التوقيع الالكتروني، وبالتالي لم يكرس الحماية الوقائية .

وعليه فإن أغلب التشريعات العربية باستثناء البعض كالتشريع التونسي والمصري، لم تعدل نصوصها الجنائية و لم تستحدث نصوصا خاصة بتجريم الاعتداء على المستندات الالكترونية بصفة عامة كالتوقيع الالكتروني بصفة خاصة على الرغم من أهميتها العملية، بخلاف التشريعات المقارنة كالقانون الفرنسي الذي عدل نص التجريم الخاص بجريمة التزوير التقليدية على نحو شمل نطاقها معه المستند الإلكتروني، وكذلك الحال بالنسبة

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

للتشريع الألماني الذي أضاف إلى باب التزوير نصوصا خاصة بتزوير المستند الالكتروني. إن التعاون والتنسيق بين الدول لازم لتجاوز هذه العقبات.

وبالنتيجة تظهر ضرورة إصدار قانون خاص بالتوقيعات الالكترونية يتم من خلاله بيان بشكل مفصل شروط صحة التوقيع الإلكتروني، تحديد أنواعه وبيان حجية كل نوع وتحديد الشروط الدنيا على الأقل في المنظومة المستعملة في إنشاء التواقيع الإلكترونية وكيفية استخدامها والأجهزة المستخدمة في ذلك بتنظيم مسألة التشفير. وبيان جرائم الاعتداء على التوقيع الالكتروني .وضرورة انشاء هيأة خاصة بالتصديق الإلكتروني من خلال مرسوم يوضح عملها واختصاصاتها وليس فقط مراسيم لإنشائها ولكن التعجيل في إدخالها حيز الخدمة بتفعيل دورها في العمل التجاري بما يتطلبه السوق والتطور الحاصل .

يتعين على المشرع الجزائري أيضا تحيين جملة من القوانين وعلى رأسها القانون الجنائي، أو اعتماد قانون بشأن التجارة الإلكترونية لمسايرة التطور الحاصل خاصة مع فتح السوق الوطنية على الاستثمار الأجنبي وخاصة ما يخص التجارة الإلكترونية دون خوف ولا توجس وهو ما حصل فعلا باستصدار القانون رقم 04/15 المؤرخ في 01 فيفري 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين قصد التكفل بالمتطلبات القانونية والتنظيمية والتقنيات التي ستسمح بإحداث جو من الثقة لتعميم وتطوير المبادلات الإلكترونية وترسيخ المبادئ العامة المتعلقة بنشاط التوقيع والتصديق الإلكترونيين في الجزائر. يسمح بتعميم وتطوير التبادلات الإلكترونية بين المستعملين في مجالي التجارة الإلكترونية. والذي يسهم في النهاية في تحقيق التنمية الاقتصادية.

ورغم كل هذه الإجراءات فالتوجه نحو البحوث والدراسات التي تهتم بهذا الجانب من العلوم وإنشاء مراكز متخصصة هو أمر لا مفر منه لأنه من جهة جانب مدر

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

للأرباح من حيث التعامل في البرمجيات، ومن جانب آخر من أجل تقوية النظم الوقائية والدفاعية ومحاصرة الجريمة المعلوماتية والتصدي للهجمات والاختراقات الممكنة وأنظمة الردع والحماية ومواكبة التطور الهائل في هذا الاتجاه. وتبقى الإمكانيات المسخرة ضعيفة بالنظر للخسائر الفادحة التي تتكبدها الشركات والأفراد والحكومات والتي تفضل عدم التصريح بها في غالب الأحيان تحاشيا لعواقب أكثر من فقدان الائتمان وخسار السمعة.

قائمة المصادر والمراجع:

الكتب:

1- إبراهيم الدسوقي، الجوانب القانونية للتعاملات الالكترونية ، مجلس النشر العلمي ، جامعة الكويت، 2003، ص: 158 .

2- حسن طاهر داوود، الحاسب وأمن المعلومات، معهد الإدارة العامة، مكتبة الملك فهد الوطنية، الرياض.

3- سامح عبد الواحد التهامي، التعاقد عبر الانترنت، دراسة مقارنة، دار الكتاب القانونية، مصر، 2008.

4- صالح شنين، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، رسالة دكتوراه، جامعة بوبكر بلقايد، تلمسان، الجزائر،2013، (مذكرة منشورة).

5- عبد الحميد ثروت، التوقيع الالكتروني، دار الإسكندرية، مصر، 2007.

6- عبد الفتاح بيومي الحجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني: الحماية الجنائية للتجارة الالكترونية ، دار الفكر الجامعي، مصر 2002.

7- عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الاسكندرية، 2005.

8- عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الانترنت، دار الفكر الجامعي، الاسكندرية، مصر، 2006 .

مجلة جامعة الأمير عبد القادر للعلوم الإسلامية –قسنطينة الجزائر–
ر ت م د : 1112–4040، ر ت م د إ : 2588–X204
المجلد: 32 العدد: 01 السنة: 2018 الصفحة: 411–459

9- عبد الفتاح حجازي، التوقيع الالكتروني، دار الفكر الجامعي، الاسكندرية، مصر، 2006،

10- عدنان برانبو، أبحاث في القانون وتقنية المعلومات، شعاع للنشر والعلوم، سوريا، 2007.

11- عصام عبد الفتاح مطر، التجارة الالكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة للنشر، مصر، 2009، ص: 211.

12- القاضي يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات، دار وائل للنشر، الأردن، 2007.

13- المحامي ياسين غانم، قواعد الاثبات وحرية المحررات القانونية الإلكترونية، مجلة المحامون(سوريا)، عدد5– 6، لسنة 2004.

14- محمد عبيد الكعبي ، الجرائم الناشئة عن الإستخدام غير المشروع للأنترنت ، رسالة دكتوراه في الحقوق جامعة القاهرة، 2009.

15- ممدوح محمد علي مبروك ، مدى حجية التوقيع الالكتروني في الاثبات، دار النهضة العربية، القاهرة، 2005، ص: 17.

16- نضال إسماعيل برهم، أحكام عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، 2005، عمان

17- نهلا عبد القادر مومني ، الجرائم المعلوماتية ، دار الثقافة ، عمان، 2008 .

القوانين والقرارات:

1- قانون التوقيع الالكتروني الفرنسي رقم 2000/23 الصادر في 2000/03/13.

2- القانون الصادر بموجب الأمر 75–58 لـــ 26 سبتمر 1975 المتضمن القانون المدني الجزائري المعدل والمتمم.

3- قانون الأنسترال بشأن التوقيعات الالكترونية لعام 1996.

4- La loi n° 2000-2230 du 13 mars 2000, J.O. 14 mars 2000.P.3986.J.C.P.2000, III, 20259.

5- Report to the governor and legislature on New York Stat's Electronic Signatures and records act,

6- Report to the governor and legislature on New York Stat's Electronic Signatures and records act, op-cit,p: 7 ,note: 4.

7- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الالكتروني (دراسة مقارنة)، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، منظم المؤتمر: أكاديمية شرطة دبي ، مركز البحوث والدراسات، رقم العدد: 1 ،من 26 إلى 28 نيسان ، 2003 بدبي – الإمارات العربية المتحدة .

8- تقرير The Norton Cybercrime Report 2011 الصادر عن شركة سيمانتك العالمية المتخصصة في أمن المعلومات حول أوضاع جرائم المعلومات في عام 2011، والذي حمل عنوان "صورة إجمالية لأوضاع أمن المعلومات حول العالم.

الكتب الأجنبية:

1. Statutory Instrument 2002 No. 318, The Electronic Signatures Regulations 2002.

2. Gassin, ®. la protection pénale d'une nouvelle universalité de fait en droit français: le système de traitement automatisé des données, Dalloz 1989, 4ème cahier.

3. SolangeGhernaouti-Hélie, Internet,, stratégie et technologie, Edition Dunod, Paris,2000.

المواقع الإلكترونية:

1- www.arablaw.org

2- https: // web.facebook.com/permalink.php.

3- http: // newsmaktoub.com/article

4- http: //studies.aljazeera.net/ar/issues/2012/02/2012229132228652960.html