مجلة الدراسات القانونية والسياسية

المجلد 08 العدد 01 جانفي 2022 | ص ص:491-507

خصوصية جريمة تزوير التوقيع الالكتروني في التشريع الجزائري

The Specificity of the Crime of Electronic Signature Forgery in Algerian Legislation

غلاب عبد الحق*

جامعة الجزائر-1

a.ghellab@univ-alger.dz

- تاريخ الإرسال: 11 /2021/08 - تاريخ القبول: 2021/12/31 - تاريخ النشر: 2022/01/05

ملخص:

غني عن البيان أن الإمكانيات المتاحة في هذا العصر أدت إلى تعدد وتنوع ظاهرة الاجرام المستحدث، وذلك بالنظر إلى الأساليب والوسائل الإجرامية التي قد تتجاوز سلوك أو فعل المجرم نفسه، وتعد ظاهرة الإجرام الإلكتروني في مجال المعاملات الرقمية أو الإلكترونية خير دليل على ذلك.

لذلك بعدما أقر المشرع الجزائري حجية للمحررات الالكترونية والتوقيع الالكتروني في المعاملات بين الأفراد، أو بين السلطات العامة والمواطنين، ظهر إجرام جديد يتعلق بالتوقيع الالكتروني، وتعد جريمة تزويره من أخطرها، رغم أن النصوص الجنائية المقارنة عالجتها كجريمة مستقلة بذاتها وهو ما لم يفعله المشرع الجزائري حين عالجها ضمن جرائم التزوير المتعلقة بالجرائم المعلوماتية الأخرى، وهذا ما يطرح العديد من الإشكالات التي سنحاول الإجابة عليها في هذه الورقة البحثية.

الكلمات المفتاحية التوقيع الالكتروني، التزوير، خصوصية، الجرائم المعلوماتية.

ABSTRACT:

Needless to say that the possibilities available in this era have led to the multiplicity and diversity of the phenomenon of newly created crime, considering the criminal methods and means that may exceed the behavior or act of the criminal himself, in which the phenomenon of electronic crime in the field of digital or electronic transactions is good evidence of that. Therefore, after the Algerian legislator approved the authenticity of electronic editors and electronic signatures in transactions between individuals, or between public authorities and

* -المؤلف المرسل:

citizens, a new crime occurred related to electronic signature, in which its forgery is considered one of the most dangerous crimes. Although the comparative criminal texts dealt with it as an independent crime, and this is what the Algerian legislator did not do when he treated it within the crimes of forgery related to other information crimes, and this raises many questions that we will try to answer in this research paper.
key words Electronic Signature, Forgery, Privacy, Information Crimes

مقدمة:

مما لا شك فيه أن التطور الحاصل في العقود الأخيرة في وسائل الإعلام والاتصال، نتيجة انتشار أجهزة الحاسوب وأجهزة الهاتف النقال، وشبكات الاتصال التي قربت البشر من بعضهم البعض، وأتاحت لهم إمكانية الاطلاع على المعلومات وتبادلها في زمن قياسي، انتج عالما افتراضيا يكاد يوازي في حركيته ونشاطه العالم المادي أو قد يفوته في بعض الحالات، حيث أصبحت معظم العلاقات والتعاملات تتم عبر شبكة الانترنت، حيث أضحت جل التعاملات الإدارية والنشاطات التجارية والمعاملات المصرفية والمالية، والخدماتية بمختلف أنواعها تمارس بطريقة إلكترونية لما توفره هذه التقنيات من وقت وجهد وسرعة وتكلفة، كما أن الإدارة أصبحت تمارس بعض النشاط الإداري بشكل الكتروني سواء تعلق الأمر بعقودها أو بقراراتها، او بعض وثائقها الرسمية، هذا ما يجعل الهوية الالكترونية أمرا لابد منه لأجل ممارسة تلك التصرفات التي لها آثار قانونية هامة، ولعل أحد أبرز سمات سلامة هذه الأعمال من الناحية القانونية هو احتوائها على توقيع الكتروني يبين هوية المتعاملين إلكترونيا.

وفي الوقت الذي تطلعت فيه الدول إستغلال هذا التقدم التكنولوجي لتحقيق النماء الاقتصادي والرخاء وتسهيل المعاملات وتلبية الحاجات الخاصة والعامة، إلا أن هناك العديد من المعوقات التي لازالت تحول دون ذلك، وخاصة ظاهرة الاجرام المستحدث في هذا العصر، وذلك بالنظر إلى الإمكانيات المتاحة التي أفرزت أساليب ووسائل إجرامية حديثة قد تتجاوز سلوك أو فعل المجرم نفسه، وخير دليل على ذلك تنامي ظاهرة الإجرام الإلكتروني وتطورها المتسارع بالتزامن مع التطور الحاصل في مجال المعاملات الرقمية أو الإلكترونية، وهذا ما انعكس –حسب المختصين– على تطور أساليب ووسائل ارتكاب الجرائم الإلكترونية، وتعد جرائم الاعتداء على التوقيع الإلكتروني من أخطرها، ومن صورها التقليد او الدخول غير المشروع على أنظمة معلوماتية أو قواعد بيانات خاصة بالتوقيع الإلكتروني، أو تزوير التوقيع الالكتروني، وتعد هذه الأخيرة أحد أهم هذه الجرائم المستحدثة التي تتطلب كفاءة عالية ومهارة تقنية كبيرة لارتكابها، باعتبارها تمر بمراحل تقنية مقعدة، هذا ناهيك عن أساليب الحماية المتنوعة للتوقيع الالكتروني، ولعل أبرز التحديات التي تواجه الجرائم الإلكترونية بشكل عام وجريمة تزوير التوقيع الالكتروني بشكل خاص هو انها لا تخضع للحدود السياسية للدول، وما ينتج عن ذلك من عدم استيعاب التشريعات الوضعية لهذه الظاهرة، هذا ناهيك

على أنها تأخذ عدة أشكال وأساليب تتغير حسب نوع المعاملة، أو التصرف القانوني، أو حسب نوع الحماية المبتكرة للتوقيع الالكتروني في حد ذاته.

ولعلها من أخطر جرائم الاحتيال الإلكتروني نظرا لما لها من أثر في اثبات المعاملات، ولما تحدثه من أضرار سواء على الضحية أو الدولة أو في مجال المعاملات الإدارية، لذلك فإن أهمية هذه الجريمة تبرز خاصة مع توجه الحكومة مؤخرا في إطلاق خدمات التصديق والتوقيع الالكترونيين ومحاولة تفعيل محتوى القانون 15-04 المحدد لقواعدهما، وذلك بعدما اعترف المشرع الجزائري بالتوقيع الإلكتروني[1]، وأضفى عليه حجية إذ يتم من خلاله اثبات مختلف التصرفات القانونية، على غرار التوقيع الكتابي أو اليدوي رغم وجود اختلافات جوهرية بينهما.

وهذا لأجل ضمان زيادة المصداقية وتعزيز أمن المبادلات الالكترونية، ومحاولة توسيع التعامل الالكتروني في مختلف المرافق العامة للدولة وخاصة السيادية منها لتحسين أدائها، والحاجة الملحة لهذا التوجه وفق ما أثبته واقع الحال خاصة في ظل هذه الظروف التي تمر بها الدولة والعالم.

وتبعا لما تقدم يمكن طرح الاشكال الذي مؤداه **الى أي مدى يمكن يستوعب النص الذي يجرم التزوير التقليدي جريمة تزوير التوقيع الإلكتروني في التشريع الجزائري؟**، ويتفرع عن ذلك عدة إشكالات من بينها هل يمكن اعتبارها جريمة في إطار النص العام المتعلق بالجريمة المعلوماتية؟ ام أنها جريمة مستلقة لها احكامها الخاصة وتختلف من مجال إلى آخر؟.

وللإجابة على هذا الإشكال سوف نقسم الموضوع إلى جزئين نتناول في الأول خصائص جريمة تزوير التوقيع الالكتروني (المبحث الاول)، ونخصص الثاني إلى الأحكام المتعلقة بهذه الجريمة (المبحث الثاني)، لنخلص في الأخير إلى أهم ما يميز هذه الجريمة من خصائص في التشريع الجزائري.

المبحث الأول: خصائص جريمة بتزوير التوقيع الالكتروني

يعتبر التوقيع الالكتروني جزءا من عقد الكتروني او قرار إداري إلكتروني او أي تصرف إلكتروني آخر فإذا أثبتنا مشروعية التصرف أثبتنا معه سلامة وصحة التوقيع الإلكتروني، وبهذا فإن التوقيع الإلكتروني يحقق وظيفة التوقيع الكتابي أو العادي[2]، ذلك ان صياغة معطيات معينة أو أعمال وتصرفات في سند ما لا تتمتع بالفعالية الثبوتية الكاملة إلا بعد إقرانها بتوقيع ما، فالتوقيع يعطي السند قوته الثبوتية، ويعبر عن التزام صاحبه بمضمونه، ويضفي على المعلومات صفة المصداقية[3]، وكذا تحديد هوية الشخص ونسبة الوثيقة للشخص الموقع والذي يتحمل مسؤولية تجاهها،

[1] – تنص المادة 2/327 من القانون المدني الجزائري والمعدلة بموجب القانون رقم 05-10 حيث قضت بأنه: «**يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر**».

[2] – Fares Wafaa, Signature électronique : Sécurité des données, revue de droit marocain, n°07, 2009, p 35

[3] – عثمان حيدر أبو زيد، القيمة الاثباتية للتوقيع اليدوي والتوقيع الإلكتروني، مقال منشور، مجلة العدل، الصادرة عن وزارة العدل السودانية، ع 18، السنة الثامنة، ص 227.

فمتى وقع تزوير في التوقيع اختلت تلك المسائل، لذلك يلعب التوقيع الإلكتروني دورا مهما بالنسبة للوثيقة المعلوماتية، فهو أحد العناصر المهمة التي تجعل هذه الوثيقة تمتع بحجية، وحتى يؤدي التوقيع الالكتروني وظائف التوقيع العادي كان لابد من إضفاء حماية قانونية عليه في بيئته الرقمية وهو ما سعت إليه التشريعات الدولية والوطنية[1].

لذلك تتميز جريمة تزوير التوقيع الإلكتروني بخصائص تجعلها تختلف عن جريمة تزوير التوقيع العادي، ولعل التزوير المعلوماتي هو تغيير الحقيقة على مخرجات الحاسب الآلي أي كان نوعها وبغض النظر عن اللغة او الأداة المستخدمة، ويشترط في ذلك اثبات حق او أثر قانوني معين، ويتسع الامر ليشمل أي وثيقة معلوماتية حتى ولو كانت باطلة، وإن كان الفقه يميز بين الوثائق المبرمجة والوثائق غير المبرمجة، خاصة في حالة وجود جهات أخرى معنية بالتصديق[2]، لذلك يتضح أن من اهم خصائص جريمة تزوير التوقيع الإلكتروني هي صعوبة الكشف عن التزوير وذلك راجع لاستخدام أساليب تقنية دقيقة مقارنة بالتزوير العادي (المطلب الأول)، وكذلك ارتباط هذه الجريمة بجرائم أخرى كجريمة السرقة وجريمة الاختراق (المطلب الثاني).

المطلب الأول: استخدام أساليب تقنية في تزوير التوقيع الإلكتروني

عرف المشرع الجزائري التوقيع الالكتروني في القانون 15-04 المؤرخ في 01 فبراير 2015 والذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[3]، في الفقرة الثانية من المادة الثانية منه على أنه: «**بيانات إلكترونية في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق**»، وهو بذلك جعل التوقيع الالكتروني وسيلة للتوثيق الإلكتروني تتمثل في مجموعة من البيانات التي يجب أن تكون مرتبطة منطقيا، وتشكل وحدة متكاملة مرفقة، أو متصلة منطقيا بوثيقة إلكترونية، هذه الأخيرة التي تعد مجموعة تتألف من محتوى وبنية منطقية وسمات العرض تسمح بتمثيلها، واستغلالها من قبل الشخص عبر نظام إلكتروني، وفق ما نصت

[1] – حاول المشرع الفرنسي في المادة 1316 من القانون المدني بعد تعديلها سنة 2000، تعريف التوقيع الالكتروني على أنه: «التوقيع الذي يميز هوية صاحبة.... وإذا ما تم التوقيع في شكل إلكتروني وجب استخدام طريقة موثوق بها لتمييز صاحبه»، وقد تم استبدالها بالمادة 1367 سنة 2016، والمعدل بـ
Modifié par Ordonnance n°2016-131 du 10 février 2016 - art. 4
Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, JORF, N° 35 du 11 février 2016, p26.
أما المشرع المصري فعرف التوقيع الالكتروني في القانون رقم 15 لسنة 2004 في المادة الأولى بقوله: «هو ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره.»، وفي ذلك يساير التشريعات الحديثة الخاصة بالتجارة الالكترونية، ومن التشريعات الحديثة التي وضعت تعريفا للتوقيع الالكتروني قوانين دول كثيرة مثل فرنسا وأمريكا وكندا والصين وإنجلترا ومصر وتونس والبحرين وغيرها، راجع في ذلك خالد ممدوح إبراهيم، إبرام العقد الالكتروني، دراسة مقارنة دار الفكر الجامعي، الإسكندرية، 2011، ص244.

[2] – راجع في هذا المعنى: محمد خالد ممدوح إبراهيم، الحماية الجنائية للتوقيع الالكتروني في القانون الاتحادي رقم 02 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات، مقال منشور مجلة الفكر الشرطي، م 23، ع 88، ص 156.

[3] – ج ر ع 06، المؤرخة في 10 فيفري 2015، ص6.

عليه المادة 02 في مطتها الأولى والثانية من المرسوم التنفيذي 16-142 المؤرخ في 05 مايو 2016 الذي يحدد كيفيات حفظ الوثيقة الموقعة إلكترونيا[1].

وبذلك أصبح للتوقيع الإلكتروني دورا واسعا في مجال المعاملات والتوثيق وفي مجال التجارة والعقود بمختلف أنواعها، وكذلك في مجال التعامل مع الادارة نتيجة الاعتماد على المعلوماتية، والتوجه نحو إدارة بلا ورق من خلال الاعتماد على الارشفة الإلكترونية والأدلة والمفكرات الالكترونية، والرسائل الصوتية للوصول إلى إدارة بلا مكان تعتمد أساسا على الهاتف المحمول، وإدارة بلا زمان تعمل في كل الأوقات[2]، لذلك كان لزاما البحث عن بديل للتوقيع التقليدي لأجل أن تؤدي ذات الوظيفة والتكيف مع وسائل الإدارة الحديثة، ويمكن أن يكون رقما سريا أو رمزا محددا وهو ما يسمى بالتوقيع الإلكتروني[3]، أي التوقيع الناتج عن اتباع اجراءات محددة تكنولوجيا تؤدي في النهاية إلى نتيجة معينة معروفة مقدما فيكون مجموع هذه الإجراءات هو البديل الحديث للتوقيع بمفهومه التقليدي وهو ما نسميه بالتوقيع الإجرائي.

وتبعا لذلك استجاب الفقه أيضا للإدارة في ممارسة بعض نشاطها بالشكل الالكتروني وخاصة في إصدار قراراته، وذلك بشرط إنجاز تلك القرارات الإدارية مطابقة لقواعد اتخاذ القرار الإداري وبأسلوب لا يفقد القرار الإداري، أو يبعده عن أركانه وعناصره القانونية التقليدية، وبما أن القرار الإداري بدأ يصدر بطريقة إلكترونية كما هو

[1] - ج ر ع 28، المؤرخة في 08 مايو 2016، ص 12.

[2] -كانت تشير المادة 1316 من القانون المدني الفرنسي قبل تعديلها سنة 2016 أن اقتران المحرر بتوقيع إلكتروني لموظف عام يضفي الصبغة الرسمية على المحرر، كما صدر المرسوم 973-2005 المؤرخ في 10 أوت 2005 الخاص بالمحررات الموثقة، ووضع شروط إنشاء وحفظ هذه المحررات التي يمكن أن تنشأ على دعامة الكترونية وفق ما قضت به الفقرة الثانية من المادة 1317 من القانون المدني والمتعلقة بالمحررات الرسمية، وقد ساعد على إصدار هذا المرسوم السابق وجود شبكة داخلية تربط بين مكاتب الموثقين تسمىREAL، وهي شبكة تسمح بتداول الوثائق، وتتم عملية التوثيق بين أكثر من موثق، بعد أن يوقع الأطراف على المحرر بصيغة رقمية عن طريق نقل التوقيع الخطي بالماسح الضوئي على المحرر أو عن طريق القلم الإلكتروني، حيث يقوم الموثق بالتوقيع على المحرر الكترونيا بفضل الشريحة الإلكترونية REAL التي تعتبر إجراء للتوقيع الرقمي الآمن والذي وضعه المجلس الأعلى للموثقين، ويخص التوقيع من طرف الموثقين على العقود الرسمية الإلكترونية، ونسخها راجع في ذلك حنان براهيمي، المحررات الالكترونية كدليل إثبات، مقال منشور، مجلة المفكر، ع9، كلية الحقوق، جامعة محمد خيضر بسكرة، ص 143.

3- حاول بعض الفقه تعريف التوقيع الالكتروني على أنه: « جزء صغير مشفر من بيانات يضاف إلى رسالة الكترونية، فهو مجتزأ من الرسالة ذاتها يشفر ويرسل مع الرسالة، ليتم التوثق من صحة الرسالة بفك التشفير وانطباق محتواه على الرسالة»، راجع خالد عبد الفتاح محمد، التنظيم القانوني للتوقيع الإلكتروني، ط1، المركز القومي للإصدارات القانونية،2009، ص 15، وعرفه أخر على أنه: « كل حروف أو أرقام أو رموز أو أصوات أو نظام معالجة ذي شكل الكتروني أو غيرها يكون له طابع متفرد يسمح بتحديد شخص الموقع وتميزه عن غيره، بحيث يعبر عن رضاء الموقع بمضمون التصرف ويضمن سلامته»، أنظر حنان براهمي، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة دكتوراه علوم في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2015، ص 142، كما يعرفه أخرون على انه: «عبارة عن حروف أو أرقام أو رموز أو إشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره، وهو الوسيلة الضرورية للمعاملات الإلكترونية في إبرامها وتنفيذها، والمحافظة على سرية المعلومات والرسائل»، راجع في ذلك عبد الكريم عبد اللاوي، التوقيع الالكتروني، مقال منشور مجلة منازعات الاعمال ع 19، ص 70.

ملاحظ في الجريدة الرسمية، وتبليغه في بعض الأحيان يتم بالطريق الإلكتروني أيضا[1]، وهو ما جرى العمل به في مواقع التواصل الاجتماعي من نشر واسع للعديد من القرارات الادارية في ظروف الوباء الحالية، وإن كانت تلك القرارات الإدارية ممسوحة ضوئيا أو مصورة، وهذا ما يزيد احتمالية تزويرها، وإن كان المشرع الجزائري ذهب في هذا الاطار من خلال اعتماد الشكل الالكتروني في العديد من الوزارات والإدارات، وحتى في القضاء من خلال قانون عصرنة العدالة 15-03[2].

هذا، وغني عن البيان أنه توجد جهات سواء كانت شخصية أو اعتبارية يرخص لها، باعتماد التوقيعات الإلكترونية، بإصدار شهادات مصدق عليها منهم على النحو الذي أشارت اليه المادة 02 من القانون 15-04 سابق الذكر[3]، ويترتب عليها آثار قانونية تتمثل في إنشاء التزامات وإثبات حقوق في حالة اعتماد التوقيع الإلكتروني بينهما، ولذلك فإن تزوير أو تقليد شهادات التصديق على التوقيع الإلكتروني يعادل في خطورته تزوير أو تقليد التوقيع الإلكتروني ذاته.

هذا ونشير أن تزوير التوقيع الإلكتروني لا يترك أثارا ظاهرة باعتباره ختم إلكتروني مشفر يملك مفاتحه صاحب التوقيع، ويتم تزويره باعتماد التوقيع نفسه عن طريق الحصول عليه، كما أنه يعد من قبيل البيانات الإلكترونية في صورها المختلفة والتي تستخدم الرموز والحروف والتشفير، كما أنه ليس من قبيل البصمة لأن هذا التوقيع يقوم على تقنيات لا تعد جزء من جسم الإنسان باستثناء التوقيع البيومتري[4]، وهذا ما يجعل تزويره أمرا صعبا باعتباره عبارة عن منظومة رقمية مرتبطة بأنظمة أمان تقنية، حيث يعتمد أهم صور التوقيع الإلكتروني – التوقيع الرقمي– على الدوال الرياضية واللوغاريتمات، كما أنه يعتمد على نظام المفاتيح العامة والخاصة، فالمفتاح العام يتم الإعلان عنه في شهادة التصديق الصادرة من جهة مختصة، وهو مفتاح يخص الموقع وحده دون غيره لكنه ينشر لكل ذي شأن، لذلك يشكل بطاقة إثبات هوية للموقع، وأما المفتاح الخاص فهو عبارة عن مجموعة من البيانات يستأثر الموقع وحده بحيازتها، ويعتبر بمثابة قلم التوقيع الذي يقوم الموقع من خلاله بتكوين بيانات توقيعه، وهذا يفترض أن يعرض الموقع كيفية استخدامه، لذلك يلزم لتزوير التوقيع الإلكتروني أن يستخدم المزور نفس قلم الموقع (المفتاح الخاص)، ويلزم أيضا أن يعرف بيانات

[1] – راجع في هذ الاطار الحسيني فالح عبد الرضا، أثر شكلية التوقيع الالكتروني في القرار الإداري، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن ص 77 وص 82.

[2] –ج ر ع 006، المؤرخة في 10 فبراير 2015، ص 4

[3] – وقد أنشأت المادة 16 من القانون15-04 السلطة الوطنية للتصديق الالكتروني لدى الوزير الأول بوصفها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية، والذمة المالية المستقلة بهدف ترقية استعمال التوقيع والتصديق الإلكترونيين وضمان موثوقية استعمالهما، كما أنشأت المادة 26 من نفس القانون السلطة الحكومية لدى وزير البريد وتكنولوجيا الاعلام والاتصال مكلفة بتوفير خدمة التصديق الالكتروني لفائدة المتدخلين في الفرع الحكومي، إضافة الى السلطة الاقتصادية للتصديق الالكتروني المنشأة بموجب المادة 29 من نفس القانون كسلطة البريد والمواصلات السلكية واللاسلكية، ومكلفة متابعة ومراقبة مؤدي خدمات التصديق الالكتروني الذين يقدمون خدمات التوقيع والتصديق الالكترونيين لصالح الجمهور وفق ما قضت به المادة 30 من ذات القانون.

[4] – غازي أبو عرابي، فياض القضاة، حجية التوقيع الإلكتروني، مجلة جامعة دمشق الإقتصادية والقانونية، العدد الأول، 2004، ص182.

التوقيع الإلكتروني نفسه (الرقم السري) بالإضافة إلى بيانات المفتاح العام، وهو أمر غير متاح إلا للموقع دون غيره، كما أن للتوقيع الإلكتروني ضمان صحة، خاصة بعد تشفيره برمز معين فيكون هناك ثلاثة قيود يجب تجاوزها لتكوين او تزوير التوقيع الإلكتروني، أولها بيانات المفتاح الخاص، وثانيها بيانات التوقيع الإلكتروني (الرقم السري)، وثالثها الرمز سري لفتح المفتاح الخاص، وبذلك يكون التوقيع الإلكتروني معبرا عن هوية الموقع، لأنه هو وحده الذي يملك أدوات وآليات هذا التوقيع[1]، على عكس التوقيع العادي الذي يعد كتابة يقوم بها الشخص وتتخذ شكلا معينا ومميزا يعتمده الشخص في التعبير عن التزامه بوثيقة ما، ويكون تزويره من خلال تقليد التوقيع أو الختم بطريقة تشبه التوقيع الأصلي واكتشافه يتم عن طريق مضاهاة الخطوط، وهذا مما يتطلب من الجاني معرفة فنية، بخلاف تزوير التوقيع الإلكتروني الذي يتطلب خبرة علمية في مجال الحاسوب والبرامج لأن طبيعة هذا التوقيع مختلفة تماما عن الأول[2].

وتبعا لذلك فإنه بعد المقارنة بين أهم وظيفة للتوقيع سواء أكان إلكترونيا أو تقليديا والمتمثلة في التحقق من شخصية الموقع، وإقراره بمضمون الوثيقة وعدم إنكارها، يمكن اعتبار أن التوقيع الإلكتروني أشد ثقة من التوقيع التقليدي، فهو لا يدلنا فقط على شخصية الموقع وإنما يؤكد لنا أيضا أن الوثيقة لم تحرف بعد توقيعها، خاصة عندما يتعلق الأمر بالتوقيع الرقمي المعتمد على تقنية المفاتيح[3]، التي تعتمد على اللوغاريتمات التي تستعمل بطريقة متكاملة فيما بينها، حيث تتعلق الأولى باللوغاريتم الأسيمتري[4]، وهذا النظام يقوم على زوج مفاتيح رقمية مبنية بطريقة لا يمكن إيجاد إحدى هذه المفاتيح إلا من خلال الآخر[5]، وتسمح هذه المفاتيح بالتوقيع الكترونيا على الوثيقة، كما تستعمل في فك تشفير المعطيات لضمان السرية، فإذا أراد شخص إرسال رسالة مشفرة فإنه يستعمل المفتاح العام للمرسل لتشفير المحتوى، غير أن المفتاح الخاص المرتبط بالمفتاح العام وحده قادر على فك التشفير.

المطلب الثاني: ارتباط جريمة تزوير التوقيع الإلكتروني بجرائم أخرى

إن التوقيع الإلكتروني هو منظومة مكونة من رموز وأرقام تميز صاحبها وتحدد هويته، ومن بين صور هذا التوقيع المعتمدة على فكرة الرموز نجد التوقيع بالرقم السري[6] الذي يرتبط غالبا بالبطاقات الممغنطة وغيرها من البطاقات الحديثة المشابهة والمزودة بذاكرة الكترونية، حيث يتم تزويره بعد تعرضه للسرقة ومن ثم استخدام الرقم والبطاقة في بعض

[1] – محمد خالد ممدوح إبراهيم، المقال السابق، ص 158 وص159.

[2] – حنان براهيمي، الأطروحة السابقة، ص 256 وما بعدها.

[3] – الأطروحة نفسها، ص 143.

[4] – اللوغاريتم هو مسار حسابي يسمح بالوصول إلى نتيجة نهائية محددة

«Un ensemble de chiffre qui résulte d'un calcul algorithmique déclenché ou initie par la frappe d'un code confidentiel» voir: JEAN_BAPTISTE Michelle, «créer et exploiter un commerce électronique, Edition LITEC, Paris, 1998, p 12.

[5]– Carine Bernard, L'utilisation de la signature électronique au CNRS,(stage d'application), Institut régional d'administration de Lille, 2004, P20.

[6] – راجع في ذلك، ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، 2007، ص 57

العمليات أو المعاملات[1]، ولذلك يبقى العميل ملزم بالمحافظة على رقمه السري للبطاقة، والإبقاء عليه في الكتمان لأنه بمثابة مفتاح خزانة النقود، ما دام أنه يمكن من دخول الحساب المصرفي للعميل لدى البنك الذي أصدر البطاقة، ومن إجراء أية عملية تحويل أو خصم أو سحب، لذلك غالبا ما يوصي البنك باتخاذ بعض الاحتياطات والتحلي بالحيطة والحذر عند أي استعمال للرقم السري للبطاقة[2].

أما فيما يتعلق بالتوقيع البيومتري (Système Biométrique) الذي يعتمد على الخواص الذاتية للشخص كقزحية العين، بصمة الأصبع ونبرة الصوت وغيرها[3]، فيتم التقاط صورة دقيقة لعين المستخدم أو بصمة يده أو صوته ثم تخزن بطريقة مشفرة في ذاكرة الحاسب الآلي الذي يقوم بمطابقة صفات المستخدم مع هذه الصفات المخزنة ولا يسمح له بالتعامل إلا في حال المطابقة، وفي هذه المرحلة يتم التحقق من صحة التوقيع عن طريق فك الشفرة البيومترية، ثم تقارن المعلومات مع التوقيع المخزن وترسلها إلى برنامج الكومبيوتر الذي يعطي الإشارة فيما إذا كان التوقيع صحيحا أم لا، وفي هذه النوع من التشفير هو التحقق من الشخصية عن طريق الاعتماد على الخواص الفيزيائية والطبيعية والسلوكية للأفراد، مما يجعلها تتعدى النطاق التجاري في التعامل لتشمل مجالات أخرى، ورغم ذلك فقد تتعرض هذه الصورة من التوقيع للاختراق بفك تشفير هذه البيانات ونسخها، ويمكن مهاجمتها أو نسخها بواسطة الطرق المختلفة المستخدمة في القرصنة الإلكترونية أو فك نظم التشفير أو الترميز[4]، وهو ما يجعل تزوير التوقيع التوقيع البيومتري أمرا واردا رغم الدقة التي يمتاز بها في تحديد شخصية الموقع، وقد نبه الفقه القانوني إلى ضرورة الاحتياط متى استعمل هذا النوع من التوقيع ذلك ان الذبذبات الحاملة للصوت أو الصورة أو بصمة الإصبع أو شبكة العين يمكن أن تخضع للاستنساخ وإعادة الاستعمال، لذلك فإن هذا النوع من التوقيع مثله مثل كل أنواع التوقيع الإلكتروني إن كان يؤمن الثقة به كونه يوفر التكنولوجيا التي تؤمن انتقاله دون القدرة على التلاعب به، وذلك باعتراف المشرع والقضاء بكفاءة هذه التكنولوجيا في تأمينه وبالتالي الاعتداد به في الإثبات[5].

---

[1] – من المحتمل أيضا التقاط أرقام البطاقات عبر شبكة الإنترنيت بعد عملية اختراق واستخدامها باسم مالك البطاقة، وهو ما أثبت الواقع العملي أنه يتم استخدام تقنية تفجير الموقع التي تعتمد على ضخ مئات الآلاف من الرسائل الإلكترونية من جهاز القرصان إلى الجهاز المستهدف للتأثير على السعة التخزينية مما يشكل ضغطا يؤدي إلى تفجير الموقع وتشتيت البيانات المخزنة فيه، لتنتقل بعد ذلك إلى جهاز القرصان ليتجول في الموقع بسهولة، ويحصل على كل ما يحتاجه من أرقام وبيانات خاصة ببطاقات الوفاء، راجع حنان براهيمي، الأطروحة السابقة، ص 254 وما بعدها.

[2] – جميل عبد الباقي، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية، الإسكندرية، 2003 ص172.

[3] –يمكن التمييز في هذا المجال بين ثلاث فئات من الخصائص البيومترية وهي الخصائص البيولوجية مثل الدم، اللعاب، الرائحة، الحمض النووي والخصائص الذاتية مثل التوقيع، حركات الجسم، والخصائص الشكلية مثل بصمات الأصابع، الوجه، العين، وشكل اليد راجع في ذلك

Hocine Boutella, Système Biométrique de Vérification de Signature Manuscrite en Ligne, Mémoire de Magister, Systèmes informatiques, Ecole Nationale d'informatique, Alger, P5.

[4] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 247.

[5] – حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية. القاهرة 2000. ص42.

فرغم أن معظم الشركات المصنعة للنظم البيومترية ترى أن دقة هذا النظام في تحقيق الشخصية بلغت نسب كبيرة جدا، إلا أنه في الوقت الحالي تجد حالات احتيال باستخدام البصمة الشخصية المقلدة ببصمة بلاستيكية أو مقلدة، وكذا عدم استطاعة بعض أجهزة التحقق البصري المصنوعة من رقائق السليكون من كشفها أو تمييزها، هذا ناهيك عن جرائم الغش الإلكتروني والتي من بينها تزوير التوقيع الالكتروني البيومتري[1].

أما في حالة التوقيع الرقمي فيعتبر أحدث أشكال التوقيع الإلكتروني وأكثرها أمانا نظرا للشروط الفنية والتقنية الخاضع لها[2]، وينشأ التوقيع الرقمي ويتحقق من صحته باستخدام التشفير (الترميز)، فإذا أراد الموقع إرسال رسالة بيانات عبر البريد الإلكتروني مثلا فإنه يقوم بإعداد ملخص الرسالة باستخدام برنامج تشفير وباستخدام المفتاح الخاص، وإرسالها للشخص المستلم الذي يستخدم المفتاح العام للتحقق من صحة التوقيع الرقمي، ثم ينشئ المرسل إليه ملخص رسالة باستخدام نفس برنامج التشفير ويقارن بين ملخصي الرسالتين، فإذا كانتا متطابقتين فهذا دليل على ان الرسالة وصلت سليمة كما هي، أما إذا تم إحداث تغير في الرسالة فسيكون ملخص الرسالة التي أنشأها المستلم مختلفة عن ملخص الرسالة التي أنشأها الموقع[3]، وهو امر وارد الحدوث.

أما في يتعلق التوقيع بالقلم الإلكتروني الذي يعتبر صورة من صور التوقيع البيومتري لأنه يعتمد على التوقيع الشخصي باستخدام طريقة Pen-Op، وهو قلم إلكتروني يمكن من الكتابة على الشاشة باستخدام برنامج خاص للكومبيوتر دوره قياس خصائص التوقيع بالضغط على مفاتيح معينة تظهر له على الشاشة بأنه موافق أو غير موافق على هذا التوقيع ثم يقوم البرنامج بتخزينها[4]، ويقوم هذا الاخير بوظيفتين الأولى هي خدمة التقاط التوقيع، والثانية التحقق من صحة هذا التوقيع، غير أن هذا التوقيع لم يعرف على نطاق واسع في مجال التجارة الإلكترونية باعتباره يحتاج جهاز كمبيوتر بمواصفات خاصة تمكنه من التقاط التوقيع والتأكد من صحته ومطابقته للتوقيع المخزن في الذاكرة[5]، لذلك مسألة تزويره صعبة اللهم الا تم بعد ارتكاب جريمة الكترونية أخرى سواء الاختراق أو السرقة.

ومما تقدم يتضح أنه من أشهر الوسائل التي يمكن الاعتماد عليها في تقليد أو تزوير التوقيع الإلكتروني هو استخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك، يتم تصميمها على غرار البرامج والأنظمة المشروعة أو محاولة البعض كسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني، والقيام بنسخها، وإعادة استخدامها بعد ذلك، لذلك يمكن القول ان جريمة تزوير التوقيع الالكتروني ترتبط بجريمة سرقة البيانات المخزنة وترتبط أيضا بجريمة

[1] – المرجع نفسه، ص 32.
[2] – حنان براهمي، الأطروحة السابقة، ص 150.
[3] – محمد خالد ممدوح إبراهيم، المرجع السابق، ص 254.
[4] – عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، نظام التجارة الإلكترونية وحمايتها مدنيا. دار الفكر الجامعي، الإسكندرية 2004، ص 246.
[5] – خالد عبد الفتاح محمد، المرجع السابق، ص 25.

الاختراق إذ لا يمكن تصور قيامها بصورة مستقلة إلا في حدود ضيقة وبأفعال تجعل ارتكابها أو قيامها كجريمة أمرا صعب للغاية.

المبحث الثاني: الأحكام العامة المتعلقة بجريمة تزوير التوقيع الالكتروني

تعتبر جريمة تزوير التوقيع الالكتروني من بين أحدث الجرائم الالكترونية ولا شك انها تختلف عن تزوير التوقيع العادي مما يجعل اثبات وقوع هذه الجريمة سهلا في إمكانية تتبعها متى تركت أثرا وصعبا إذا كان العكس، لهذا يكون لزاما أن نبين أركان جريمة تزوير التوقيع الالكتروني في (المطلب الأول)، ثم نبين العقوبات المقررة لمرتكب جريمة تزوير التوقيع الالكتروني (المطلب الثاني).

المطلب الأول: أركان جريمة تزوير التوقيع الالكتروني

تقوم جريمة تزوير التوقيع الالكتروني في ركنها المادي على المحرر المعلوماتي الموقع الكترونيا، ويكون الهدف من التزوير هو تغيير الحقيقة، ولابد من وجود ضرر في مجال التوقيع الالكتروني، كما لابد من توفر القصد الجنائي بالنسبة لهذه الجريمة والذي يمتاز بنوع من الخصوصية، لذا سوف يتم التطرق إلى الركن المادي لجريمة تزوير التوقيع الالكتروني في (الفرع الأول)، ثم إلى الركن المعنوي لجريمة تزوير التوقيع الإلكتروني في (الفرع الثاني).

الفرع الأول: الركن المادي لجريمة تزوير التوقيع الالكتروني

يجب الإشارة إلى أن جريمة تزوير التوقيع الالكتروني من الجرائم التي يدور فعل التزوير المعلوماتي على تغيير الحقيقة في محرر الكتروني بطريق الغش، مما ينتج عنه مضمون مختلف للمحرر وللمعاملات القانونية القائمة على صحة المعلومات التي توفرها هذه البيانات التي تكون محلا للغش ويكون من شأنه احداث ضرر[1]، والتوقيع هو توقيع الكتروني على محرر الكتروني، فتقوم جريمة التزوير في ركنها المادي منه بتغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون على نحو يسبب ضررا للغير[2]، لذلك يقتضي الركن المادي ان نتطرق الى المحرر المعلوماتي الموقع الكترونيا (أولا)، ثم فعل تغيير الحقيقة (ثانيا).

أولا: المحرر المعلوماتي الموقع الكترونيا

تختلف جريمة تزوير التوقيع الالكتروني عن تزوير التوقيع التقليدي، ففي الأول يقوم الشخص بالحصول على منظومة التوقيع الالكتروني الخاصة بشخص آخر بغرض استخدامها في توقيع مستندات الكترونية، أو وثائق إلكترونية[3]، فالوثيقة الموقعة إلكترونيا هي الوثيقة الالكترونية المرفقة أو المتصلة بتوقيع إلكتروني، لذلك يكون التوقيع

[1] – محمد خالد ممدوح إبراهيم، المقال السابق، ص 157.

[2] – عباس حفصي، جرائم التزوير الالكترونية دراسة مقارنة، أطروحة دكتوراه علوم في العلوم الإسلامية، تخصص شريعة وقانون، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة أحمد بن بلة – وهران 1، 2015، ص 97.

[3] – والوثيقة الالكترونية كما عرفتها المادة الثانية من المرسوم التنفيذي 16-142 بأنها: «**مجموعة تتآلف من محتوى وبنية منطقية وسمات العرض، تسمح بتمثيلها واستغلالها من قبل الشخص عبر نظام إلكتروني**».

الالكتروني سليما متى كان مالك منظومة التوقيع قد قام بالتوقيع بواسطتها، وتكمن المشكلة هنا في حصول الشخص على المنظومة بواسطة التجسس الالكتروني أو غيرها من الطرق الأخرى، وعليه فجريمة تزوير التوقيع الالكتروني تختلف اختلافا كليا أو جزئيا عن تزوير التوقيع التقليدي سواء في طريقة التزوير أو في طريقة الكشف عنها[1].

وتبعا لذلك فإنه لتمتع التوقيع الالكتروني بالحجية في الإثبات يشرط تمتعه بالحماية الجنائية، فالقاعدة العامة تنص على أن التوقيع الالكتروني الذي لا يتمتع بالحجية في الإثبات لا يكون محلا للتزوير، وعليه فالتمتع بالحجية في الإثبات شرط حصول التوقيع على الحماية الجزائية المقررة إذا ما تم تزويره.

ولا تعتبر الكتابة سواء كانت الكترونية أو على دعامة[2] حجة في الإثبات إلا إذا كانت موقعة توقيعا الكترونيا، لذلك يعتبر التوقيع الالكتروني عنصرا من عناصرا الدليل الكتابي المعد للإثبات، وهو ما أكده القانون المدني في نص المادة 327 الفقرة 2 من القانون المدني الجزائري[3]، والتوقيع الالكتروني بشرطه المذكور في المادة 323 مكرر 1 من القانون المدني الجزائري حجة في الإثبات، ومنه يكون المشرع قد اعترف بحجية التوقيع الالكتروني[4].

ثانيا: الفعل المادي المتعلق بتغيير الحقيقة

يتمثل الركن المادي لجريمة تزوير التوقيع الإلكتروني في فعل تغيير الحقيقة في توقيع الكتروني وذلك بأي وسيلة كانت، ولعل من 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 بغرض استخدامها[5]، وقد يكون التغيير ماديا أو بالتقليد ومعناه المشابهة، أو بالتزييف في الإمضاءات أو البصمة أو الكتابة بما في ذلك الزيادة أو الحذف، وإما بانتحال شخصية الغير أو الحلول محلها، فالتغيير المادي تدركه الحواس وتثبته الخبرة، كما قد يكون التغيير معنويا، عن طريق اصطناع اتفاقات أو التزامات أو مخالفات صورية، أو إدراجها لاحقا في محررات معدة لتلقى البيانات، فالتزوير في هذه الحالة يوجد في المعنى والمضمون، ومن ذلك اصطناع أحكاما قضائيا أو وثائق مما تصدره الإدارات العمومية، وهي مزورة من حيث البيانات أو التوقيع، ويكون التزوير بإحدى الطرق المحددة على سبيل الحصر في نص المادة 216 من قانون العقوبات سواء تعلق الأمر بتزوير الواقع في المحررات الرسمية أو العرفية[6].

---

[1] – عباس حفصي، الأطروحة السابقة، ص 98.

[2] – الدعامة هي أي وسيلة مادية أيا كان شكلها او خصائصها المادية، تسمح باستلام وحفظ واسترجاع الوثيقة الموقعة إلكترونيا.

[3] – تنص المادة 2/327 ق م على أنه: «**يعتبر العقد العرفي صادرا ممن كتبه أو وقعه أو وضع عليه بصمة أصبعه ما لم ينكر صراحة ما هو منسوب إليه أما ورثته أو خلفه فلا يطلب منهم الإنكار ويكفي أن يحلفوا يمينا بأنهم لا يعلمون أن الخط أو الإمضاء أو البصمة هو لمن تلقوا منه هذا الحق**».

[4] – راجع في ذلك عماد محمد علي البلوي، جريمة تزوير التوقيع الالكتروني، جامعة نايف العربية للعلوم الأمنية، رسالة ماجستير، 2009، ص 56.

[5] –ياسين جبيري، الحماية الجنائية والتوقيع الإلكتروني دراسة مقارنة، مقال منشور، ع01، م 32، مجلة جامعة الأمير عبد القادر، قسنطينة 2018، ص 434.

[6] – حيث تتمثل هذه الطريقة في تقليد الكتابة أو التوقيع أو باصطناع اتفاقات أو نصوص أو التزامات أو مخالصات، أو بإدراجها في هذه المحررات فيما بعد، كما قد تكون طريقة التزوير بإضافة أو بإسقاط أو بتزييف الشروط أو الإقرارات أو الوقائع التي أعدت هذه المحررات لتلقيها أو إثباتها، وإما عن طريق انتحال شخصية الغير أو الحلول محلها.

وتبعا لذلك فإن لم يكن هناك تغيير للحقيقة فلا تزوير، ومن ذلك تقليد إمضاء شخص على محرر ولكن بموافقته وإذنه، لذلك يجب أن ينصب التزوير على البيانات الجوهرية التي يتضمنها المحرر، وأما البيانات غير الجوهرية التي لا تؤثر فيما أعد المحرر من أجله، فإن تغييرها أو تحريفها أو إضافتها أو إزالتها لا يعد من قبل التزوير المعاقب عليه، لأنه لا ينتج أي ضرر عن ذلك[1]، وهو ما ينطبق على جريمة تزوير التوقيع الالكتروني أيضا.

أما عن طرق التزوير فقد يكون إما عن تزويرا ماديا أو تزوير معنويا، وتكمن أهمية التفرقة بينهما من حيث الإثبات ومن حيث العقاب، فالتزوير المادي هو ذلك الأسلوب الذي يترك أثرا ماديا في المحرر يدل على تغيير الحقيقة فيه[2]، أو هو ما ترك أثرا ماديا يدل على العبث بالمحرر وهي علامات مادية مستخلصة من الفحص والدالة تشويه بيانات المحرر والتوقيع الإلكتروني[3]، ويدخل تحت هذا الإطار أيضا إضافة شروط وإدخالها في صلب المحرر الإلكتروني بعد إنشاءه، وكذا إنشاء محرر مزور بأكمله بما فيه التوقيع الالكتروني، فهنا يعاقب على التزوير حتي ولو كان محتوى المحرر صحيحا دون أن تكون هناك حاجة لإثبات تزوير الوقائع أو الأرقام أو الشيفرات[4].

أما التزوير المعنوي هو ذلك التزوير الذي لا يتضمن أية مظاهر مادية يستدل بها على العبث بالمحرر الالكتروني او توقيعه، إذ أنه يتحقق بتشويه فحواه ومضمونه، فمظهر المحرر لا يكشف عن تزويره ولا تزوير توقيعه الإلكتروني، وإنما يقتضي التحقيق من التزوير معرفة الحقيقة من مصادر أخرى، كالكشف عن إرادة من نسب إليه المحرر، أو التحري عن الوقائع الحقيقية ومقارنتها بالوقائع التي تم تدوينها في المحرر فإذا وجد اختلاف بينهما، كان هذا هو الدليل على التزوير[5]، وهو ما ينطبق على التوقيع الإلكتروني أيضا.

الفرع الثاني: الركن المعنوي لجريمة تزوير التوقيع الإلكتروني

لا تكتمل جريمة التزوير في وثيقة معلوماتية إلا إذا توافر الركن المعنوي إلى جانب الركن المادي على غرار باقي الجرائم، وتعتبر جريمة تزوير التوقيع الإلكتروني من الجرائم العمدية حيث لا بد من توافر القصد الجنائي فيقوم في جريمة التزوير إذا انصرفت إرادة الجاني إلى تغيير الحقيقة في المحرر بإحدى الطرق التي بينها القانون مع توقعه احتمال حدوث ضرر مادي أو أدبي نتيجة لهذا الفعل[6]، فالقصد العام يقوم على عنصري العلم والإرادة، وعنصر العلم يرتبط بعلم الجاني أنه يغير الحقيقة في محرر يحظى بحماية القانون، ويستوي في ذلك أن يكون المحرر ورقيا أو وثيقة معلوماتية،

[1] – عمر فاروق الحسيني، شرح قانون العقوبات، القسم الخاص، جرائم الاعتداء على المصلحة العامة، يناير 2009، ص 84.
[2] – رمسيس بهنام، قانون العقوبات جرائم القسم الخاص، منشأة المعارف، الإسكندرية 1999، ص 451.
[3] – أمغار خديجة، جريمة التزوير في المحررات الرسمية دراسة تحليلية مقارنة، مذكرة ماجستير في القانون الجنائي، كلية الحقوق والعلوم الإدارية، الجزائر-1 2014، ص 36.
[4] – محمود نجيب حسني، شرح قانون العقوبات القسم الخاص وفقا لأحدث التعديلات التشريعية، دار النهضة العربية، القاهرة، 2019، ص 229.
[5] – أمغار خديجة، مرجع سابق، ص 37.
[6] – عمر السعد رمضان، شرح قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، 1986، ص 294.

ولذلك فإن عدم علم الجاني أنه يغير الحقيقة في محرر يتمتع بحماية القانون ينفي القصد الجنائي لديه[1]، وهذا العلم مفترض فلا يدفع مسؤوليته عن ذلك بجهله[2]، إذ يفترض علم الجاني أن ما حصل من تغيير الحقيقة فيه يعتبر محررا في نظر القانون، وان هذا التغيير قد حصل بطريقة من الطرق المنصوص عليها في القانون[3]، كما يجب أن يدرك الجاني أنه يغير الحقيقة في محرر[4]، أما في جريمة تزوير التوقيع الالكتروني في وثيقة رسمية إدارية معلوماتية فيتوافر القصد العام بانصراف إرادة الجاني إلى تغيير الحقيقة في وثيقة رسمية إدارية معلوماتية، مهما كانت الطريقة التي استخدمها لإيقاع التغيير ،حيث لم تعد هذه الطرق محصورة كما هي في جريمة التزوير في المحرر العادي أو التوقيع العادي فهي بذلك لا تختلف عن جريمة التزوير الالكتروني بشكل عام.

وهذا هو الإتجاه الحديث للتشريعات المقارنة من أجل تحقيق المرونة في الصياغة التشريعية لتجريم التزوير بما ينسجم مع التعدد التقني لأشكال الوثائق المعلوماتية ووسائل تغيير الحقيقة فيها وكذا التطور المستمر في هذا المجال، إلا أنه رغم كل ذلك يجب أن يرتبط علم الجاني بأنه يغير الحقيقة في وثيقة لها قيمة قانونية، ولذلك هي تتمتع بالحماية القانونية ضد هذا التغيير، ويفترض علم الجاني أن ما قام به من تغيير للحقيقة قد تم فيما يعتبر وثيقة من الناحية القانونية، حيث لا أثر لطبيعتها المعلوماتية في اعتبارها كذلك قانونا، ولا أثر لطبيعة الوسيلة أو الطريقة التي تم بها التغيير، فالقصد الجنائي العام بعنصريه العلم والإرادة يجب توافره لدى الجاني حتى يمكن نسبة جريمة التزوير المعلوماتي إليه بما فيها جريمة تزوير التوقيع الالكتروني، حيث يجب أن يكون عالما بأن إدخال المعلومات والبيانات إلى مضمون المحررات أو محو تلك المعلومات أو تحويرها وإتلافها أو القيام بأية أفعال أخرى من شأنها أن تؤدي إلى التأثير على المجرى الطبيعي لمعالجة البيانات فإذا كان جاهلا بأن الفعل الذي يرتكبه غير مشروع فلا يتحقق القصد[5].

هذا، ولا يكفي لقيام الركن المعنوي في جريمة تزوير التوقيع الالكتروني توافر القصد الجنائي العام، إذ لا يكفي توافر الإرادة والعلم بمكونات الجريمة، بل لابد أن تكون نية الجاني قد اتجهت وقت ارتكاب هذا الفعل إلى استعمال المحرر الذي يشتمل على توقيع الكتروني مزور في الغرض الذي زور من أجله، أي بمعنى الاحتجاج به على اعتبار أنه صحيح[6].

---

[1] – عبد الفتاح بيومي حجازي، الحكومة الالكترونية، الكتاب الثاني، دار الكتب القانونية، د.م، 2007، ص 249.

[2] – فتوح الشاذلي وعفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات حلبي الحقوقية، بيروت2003، ص 258.

[3] – أحمد خليفة الملط، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، الإسكندرية، 2006، ص 475.

[4] – براهمي حنان، الأطروحة السابقة، ص 225.

[5] – راجع في ذلك براهيمي حنان، الأطروحة السابقة، ص 226.

[6] – إيهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، دار الجامعة الجديدة، الإسكندرية 2008، ص 59.

المطلب الثاني: العقوبات المقررة لمرتكب جريمة تزوير التوقيع الالكتروني

تعتبر العقوبات الجزاء الذي يوضع تنفيذا لحكم قضائي، ولا يمكن تنفيذها عليه إلا إذا نص عليها القاضي في حكمه، ويمكن أن يقتصر عليها الحكم، ومن المعلوم أن العقوبة طبقا للمادة 05 من قانون العقوبات المعدلة بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، تكون إما أن تكون أصلية أو تكميلية، لذا يتم التطرق إلى العقوبات الأصلية (الفرع الأول)، ثم إلى العقوبات التكميلية (الفرع الثاني).

الفرع الأول: العقوبات الأصلية

من المعلوم العقوبة الأصلية هي الجزاء الأصلي – أي الأساسي – المقرر للجريمة والذي يحكم به القاضي بثبوت إدانة المتهم وهي على عدة أنواع إما أن تكون بدنية أو جسدية كالإعدام وإما أن تكون مالية كالغرامة وإما أن تكون سالبة للحرية كالسجن أو الحبس بنوعيه، أما بالنسبة الى العقوبة المقررة لجريمة التزوير التقليدي بشكل عام فمنصوص عليها ضمن المواد من 214 إلى المادة 218 من قانون العقوبات وتتمثل بالسجن والحبس والغرامة، أما فيما تعلق بالتزوير التوقيع الإلكتروني فمنصوص عليها في المواد من 394 مكرر إلى المادة 394 مكرر 7، وهو يدخل ضمن الجرائم المعلوماتية بشكل عام ولا تختلف عن العقوبات السابقة

الفرع الثاني: العقوبات التكميلية

العقوبة التكميلية إما أن تكون إجبارية أو اختيارية، ونصت على هذه العقوبات المادة 09 من قانون العقوبات، ومن بينها نذكر منها عقوبة الحجز القانوني وعقوبة الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية المذكورتين في المادتين 9 مكرر والمادة 9 مكرر1 اللتين أضافهما القانون رقم 06-23[1].

إن هذا النوع من العقوبات لا يمكن تطبيقه إلا بقرار من القاضي ويمكن تطبيقه على مرتكب التزوير الالكتروني كالحرمان من تولي بعض الوظائف وغيرها من العقوبات المذكورة في المادة 9 مكرر والمادة 9 مكرر1.

وتطبق عقوبة المصادرة على هذا النوع من الإجرام بمصادرة الاجهزة التي استعملت في ارتكاب جريمة التزوير كجهاز الكمبيوتر وغيرها من المعدات المستعملة في الجريمة، أو كانت معدة للاستعمال. وهو ما ذكرته المادة 394 مكرر 3 بنصها العقوبات التكميلية إلى جانب العقوبات الأصلية والمتمثلة في:

المصادرة: وهي عقوبات تكميلية تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير حسن النية.

[1] – القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، ج ر ع 84، المؤرخة في 24 ديسمبر 2006، ص11.

إغلاق المواقع والأمر يتعلق بالمواقع (Les sites) التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية، وكذلك إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، ومثال ذلك إغلاق المقهى الالكتروني الذي ترتكب منه مثل هذه الجرائم الماسة بالأنظمة المعلوماتية.

هذا، وتطبق العقوبات التبعية على مجرمي التزوير المعلوماتي للحكم عليه بعقوبة أصلية ما يجعلها ملحقة بعقوبة تبعية، وللقاضي الحق بالحكم بعقوبة تبعية أو أكثر طبقا لأحكام المادة 9 مكرر1 لمدة أقصاها عشر سنوات تسري من يوم انقضاء العقوبة الأصلية، أو الإفراج عن المحكوم عليه بعقوبة جناية[1]، وتنص المادة 14 من نفس القانون والمعدلة بالقانون رقم 06-23 على أنه: "يجوز للمحكمة عند قضائها في جنحة، وفي الحالات المذكورة في المادة 9 مكرر 1، وذلك لمدة لا تزيد عن خمس 5 سنوات، وتسري هذه العقوبة من يوم انقضاء العقوبة السالبة للحرية أو الإفراج عن المحكوم عليه"[2].

الخاتمة:

مما تقدم اتضح ان جريمة تزوير التوقيع الالكتروني تتميز بخصوصية عن باقي الجرائم المعلوماتية الأخرى باختلاف أنواعها وطرق ارتكابها، إذ لا يمكن ارتكابها بشكل مستقل فهي ترتكب بالتبعية لجرائم أخرى كجريمة السرقة وجريمة الاحتراق، لذلك تشكل أبرز صور الاعتداء على التوقيع الإلكتروني والتي من بينها إتلاف التوقيع الإلكتروني والدخول غير المشروع على أنظمة المعلوماتية أو قواعد البيانات الخاصة بالتوقيع الالكتروني.

وتبين ان المشرع الجزائري لم يحدد لها نظاما خاصا من حيث الاثبات او المتابعة أو التجريم أو حتى العقوبة المقررة لهذه الجريمة المستحدثة، فهي لا تختلف عن الجرائم الالكترونية الأخرى في العديد من الجوانب على غرار الركن المعنوي لهذا النوع من الجرائم، وإن صورها وأفعالها تختلف من نوع إلى آخر، ورغم ذلك فإنه مع التطور العلمي والتكنولوجي وزيادة الأدوات المسهلة في ارتكاب هذه الجريمة قد يصبح الأمر متاحا حتى لمن يملك خبرة قليلة في ميدان الاعلام الآلي خاصة في ظل البرمجة الحديثة التي تعتمد على أساليب متطورة ومتكاملة وتعتمد على تقنيات عالية الدقة تسهل من ارتكاب هذا النوع من الجرائم، لذا فإننا نهيب بالمشرع أن يضبط مصطلح جريمة التزوير الالكتروني ضبطا دقيقا، خاصة بعد صدور قانون التجارة الإلكترونية، واعتماد التوقيع والتصديق الإلكترونيين مؤخرا.

إذ على المشرع أن يكيّف النصوص الجنائية ليحدد جريمة تزوير التوقيع الالكتروني بشكل دقيق وعدم الاكتفاء بأحكام عامة تتعلق بكافة جرائم المعلوماتية على غرار ما فعله المشرع الفرنسي أين عدل النص المتعلق بجريمة التزوير التقليدي على نحو يشمل التزوير الالكتروني، ولعل إضافة مادة تنص على جريمة التزوير الإلكتروني كجريمة مستقلة بحد ذاتها، وتحدد لها عقوبة خاصة بالنظر الى خطورتها وخاصة إذا استعملت في تزوير المحررات الرسمية الإدارية الصادرة عن

[1] – حفصي عباس، المرجع السابق، ص 162 وص 163.

[2] – المادة 14 عدلت بموجب المادة 5، من القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، ج ر ع 84، المؤرخة في 2006/12/24

مختلف السلطات، أو في مختلف المعاملات الإلكترونية الأخرى، وذلك لتكريس أهم المبادئ التي جاء بها التعديل الدستوري لسنة 2020، وفي ظل اعتماده الحكومة الالكترونية والسير نحو الرقمنة في مختلف المجالات.

قائمة المصادر والمراجع:

1)- الأمر 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، ج ر ع 49، المؤرخة في 11 يونيو 1966، المعدل والمتمم عدة مرات.

2)- القانون رقم 05-10 المؤرخ في 20 يونيو 2005 المعدل والمتمم للأمر 75-58 المتضمن القانون المدني، ج ر ع 44 المؤرخة في 26 يونيو 2005، ص17.

3)- القانون 06-23 المؤرخ في 20 ديسمبر 2006 المعدل والمتم للأمر 66-156 المتضمن قانون العقوبات، ج ر ع 84، المؤرخة في 24 ديسمبر 2006.

4)- القانون 15-03 المؤرخ في 01 فبراير 2015، المتعلق بعصرنة العدالة، ج ر ع 06، المؤرخة في 10 فبراير 2015.

5)- القانون 15-04 المؤرخ في 01 فبراير 2015 والذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين ج ر ع 06، المؤرخة في 10 فيفري 2015.

6)- المرسوم التنفيذي 16-142 المؤرخ في 05 مايو2016 الذي يحدد كيفيات حفظ الوثيقة الموقعة إلكترونيا، ج ر ع 28، المؤرخة في 08 مايو 2016، ص 12.

7)- أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية 2006.

8)- الحسيني فالح عبد الرضا، أثر شكلية التوقيع الالكتروني في القرار الإداري، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن2015.

9)- خديجة أمغار، جريمة التزوير في المحررات الرسمية دراسة تحليلية مقارنة، مذكرة ماجستير في القانون الجنائي، كلية الحقوق والعلوم الإدارية، الجزائر-1، 2014.

10)- إيهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، دار الجامعة الجديدة، الإسكندرية 2008.

11)- حنان براهمي، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة دكتوراه علوم في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة 2015.

12)- حنان براهمي، المحررات الالكترونية كدليل إثبات، مقال منشور، مجلة المفكر، ع9، كلية لحقوق جامعة بسكرة.

13)- توح الشاذلي وَعفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات حلبي الحقوقية، بيروت، لبنان 2003

14)- ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، 2007، ص 57.

15)- جميل عبد الباقي، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية، الإسكندرية، 2003.

16)- حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، دار النهضة العربية. القاهرة 2000.

17)- عباس حفصي، جرائم التزوير الالكترونية دراسة مقارنة، أطروحة دكتوراه علوم في العلوم الإسلامية، تخصص شريعة وقانون، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة أحمد بن بلة – وهران 1، 2015.
18)- ناصر حمودي، النظام القانوني لعقد البيع الدولي الإلكتروني عبر الانترنت، أطروحة دكتوراه، جامعة مولود معمري تيزي وزو، 2009.
19)- خالد عبد الفتاح محمد، التنظيم القانوني للتوقيع الإلكتروني، المركز القومي للإصدارات القانونية، ط1، 2009.
20)- خالد ممدوح إبراهيم، إبرام العقد الالكتروني، دراسة مقارنة دار الفكر الجامعي، الإسكندرية، 2011.
21)- رمسيس بهنام، قانون العقوبات جرائم القسم الخاص، منشأة المعارف، الإسكندرية 1999.
22)- عبد الفتاح بيومي حجازي، الحكومة الالكترونية، الكتاب الثاني، دار الكتب القانونية، د.م، 2007
23)- عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، نظام التجارة الإلكترونية وحمايتها مدنيا. دار الفكر الجامعي، الإسكندرية 2004.
24)- عبد الكريم عبد اللاوي، التوقيع الالكتروني، مقال منشور مجلة منازعات الاعمال ع 19، ديسمبر 2016.
(https://revues.imist.ma/index.php/Contentieux-Affaires/article/view/8384/4778) تم تصفح الموقع بتاريخ: 2021/07/20 في الساعة 17:00 مساء.
25)- عماد محمد علي البلوي، جريمة تزوير التوقيع الالكتروني، جامعة نايف العربية للعلوم الأمنية، رسالة ماجستير 2009
26)- عمر السعد رمضان، شرح قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، 1995.
27)- عمر فاروق الحسيني، شرح قانون العقوبات، القسم الخاص، جرائم الاعتداء على المصلحة العامة، يناير2009.
28)- غازي أبو عرابي، فياش القضاة، حجية التوقيع الإلكتروني، مجلة جامعة دمشق الإقتصادية والقانونية، العدد الأول، 2004
29)- محمد خالد ممدوح إبراهيم، الحماية الجنائية للتوقيع الالكتروني في القانون الاتحادي رقم 02 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات، مقال منشور مجلة الفكر الشرطي، المجلد 23، عدد 88.
30)- محمود نجيب حسني، شرح قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، 2019.
31)- ياسين جبيري، الحماية الجنائية والتوقيع الإلكتروني دراسة مقارنة، مقال منشور، ع01، م 32، مجلة جامعة الأمير عبد القادر، قسنطينة 2018.
32)- Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, JORF, N° 35 du 11 février 2016.
33)- Carine Bernard, L'utilisation de la signature électronique au CNRS, (stage d'application), Institut régional d'administration de Lille, 2004.JEAN_BAPTISTE 34) - Michelle, créer et exploiter un commerce électronique, Edition LITEC, Paris, 1998.
35)- Hocine Boutella, Système Biométrique de Vérification de Signature Manuscrite en Ligne, Mémoire de Magister, Systèmes informatiques, Ecole Nationale d'informatique, Alger.