المسؤولية النظامية لجهات المصادقة الرقمية ـ دراسة تحليلية مقارنة بين النظام السعودي والتشريعات الأجنبية (القانون الإماراتي والأوروبي أنموذجًا)

ياسر أحمد بدر (*)
جامعة المجمعة

(قدم للنشر في 1442/2/9هـ، وقبل للنشر في 1443/2/19هـ)

مستخلص: إن سرية البيانات المتبادلة عبر الوسائط الإلكترونية، وأهمية التعاملات الإلكترونية التي تتم بين المتعاملين؛ دفعتهم للبحث عن وسيلة تؤمن لهم تعاملاتهم، وتمنع الغير من اختراقها والاطلاع على البيانات السرية، وتؤكد لهم هوية الطرف الآخر وصحة توقيعه، وهو ما توفره جهة المصادقة الرقمية من خلال إصدار شهادات التصديق الرقمي؛ لإثبات نسبة التوقيع الإلكتروني إلى شخص معين، وصدور الإرادة منه، وأمام الدور الذي تقوم به جهات المصادقة الرقمية كوسيط مؤتمن بين المتعاملين في البيئة الإلكترونية وخطورة النتائج المترتبة عليه، فقد عمدت معظم التشريعات الوطنية والدولية إلى تنظيم عمل جهات المصادقة الرقمية والشهادات الصادرة عنها، وتحديد التزاماتها والحالات التي تقام فيها مسؤوليتها النظامية.
وفي ظل ذلك ، نهج المنظم السعودي نهجًا يتوافق مع ما ذهبت إليه هذه التشريعات بإقراره نظامًا مستقلاً للتعاملات الإلكترونية لعام 1428هـ، نُظِّم من خلاله كل ماله علاقة بالتصديق الرقمي؛ ابتداءً ببيان المقصود بجهات المصادقة الرقمية والشهادات الصادرة عنها وواجباتها، مع تحديد مسؤوليتها الجزائية من خلال التنصيص على عقوبات جزائية توقع عليها في حال مخالفتها لأحكام النظام متى كانت هذه المخالفة تشكل جريمة جزئية، بالإضافة إلى تحملها المسؤولية المدنية عن الآثار الناجمة عنها، وذلك لخلق بيئة آمنة وموثوقة لكافة المتعاملين.

كلمات مفتاحية: المصادقة الرقمية، التعاملات الإلكترونية، التزامات، المسؤولية المدنية، المسؤولية الجزائية.

*****

The legal liability of Digital Authenticators- A Comparative Analytical Study between the Saudi System and Foreign Legislation

Yasser Ahmed Badr Mohammed (*)
Majmaah University

. *(Received 26/9/2020, accepted 29/9/2021)*

Abstract: The confidentiality of the data exchanged through electronic media and the importance of electronic transactions that take place among clients urged them to search for a way to secure their transactions, prevent others from hacking or accessing confidential data, and confirm the identity of the other party and the validity of his/her signature. This secure way is provided by the digital authentication authority by issuing digital authentication certificates proving the attribution of the electronic signature to a particular willing person. In accordance with the role played by the digital authentication authorities as a trusted intermediary between clients in the electronic environment and the seriousness of the consequences thereof, most national and international legislations have intended to regulate the work of the digital authentication authorities and the certificates issued by them in order to specify their obligations and the cases where statutory liability is held. In light of this, the Saudi legislators, in 1428 AH, adopted an approach consistent with what these legislations have pursued by approving an independent system for electronic transactions, through which all issues related to digital authentication are organized, starting from stating what is meant by digital authentication authorities and the certificates issued by them and what their liability is. In addition, this approach specifies the criminal liability of these authorities by stipulating criminal penalties to be imposed in the event of violating the provisions of the system when this violation constitutes a partial crime, in addition to bearing the civil liability for the consequences resulting from it. As a result, a safe and reliable environment for all clients is created.

Key words: digital authentication, electronic transactions, obligations, civil liability, criminal liability.

(*) للمراسلة:

أستاذ القانون المدني المساعد-قسم القانون-كلية إدارة الأعمال-جامعة المجمعة، المملكة العربية السعودية.

(*) Corresponding Author:

Assistant Professor of Civil Law, College of Business Administration, Majmaah University, Saudi Arabia

DOI: 10.12816/0061530

e-mail:y.badr@mu.edu.sa

مقدمة.

مما لا شك فيه أن التحولات التي شهدها مجال تكنولوجيا المعلومات والاتصال، وتأثيره على التعاملات الإلكترونية عامة، والتوقيع الرقمي على المحررات الإلكترونية خاصة، أظهرت الحاجة إلى إيجاد جهة محايدة تسمى بجهة المصادقة الرقمية، والتي تلعب دور الوسيط المؤتمن بين المتعاملين في البيئة الإلكترونية، فتؤكد هوية المتعاملين وصدور الإرادة عمن نسبت إليه عن طريق إصدار شهادة تصديق رقمي تتضمن التوقيع الإلكتروني للشخص المراد إثبات هويته، ونظراً لما يترتب على عملية المصادقة الرقمية على التعاملات الإلكترونية من آثار قانونية ، فقد تضافرت الجهود الدولية والوطنية لإصدار تشريعات تنظم عمل جهات المصادقة الرقمية والشهادات الصادرة عنها، وتحملها للمسؤولية المدنية عن مخالفتها لأي التزامات فرضها النظام في تعويض الطرف المضرور سواء أكان العميل أو الغير، مع التنصيص على عقوبات جزائية توقع عليها متى كان إخلالها بهذه الالتزامات يشكل جريمة جزائية، وذلك لبث الثقة والأمان في مجال التجارة الإلكترونية.

أهمية البحث:

تبرز أهمية البحث من خلال المحاور الآتية:

1. اعتماد جهات المصادقة الرقمية كوسيلة لتعيين أطراف التعاملات الإلكترونية.
2. تحديد الالتزامات الأساسية التي يجب أن تراعيها جهات المصادقة الرقمية عند ممارسة نشاطها، لكي تبث الثقة لدى المتعاملين وتؤمن التعامل الإلكتروني بينهما.
3. الوقوف على توجهات المنظم السعودي في تنظيم عمل جهات المصادقة الرقمية والمسؤولية النظامية المترتبة عليه، ومقارنتها مع توجهات التشريعات الأجنبية، مما يساعد في بناء تصور حول واقع تنظيم التصديق الرقمي، وأهم الإشكالات التي تواجه في المملكة العربية السعودية.

أهداف البحث:

يسعى البحث إلى تحقيق الأهداف التالية:

1. الوقوف على ماهية المصادقة الرقمية على التعاملات الإلكترونية من خلال التعرف على التصديق الرقمي وطبيعته، ووسائل المصادقة الرقمية على التعاملات الإلكترونية، والجهات المخولة بالمصادقة الرقمية على التعاملات الإلكترونية، والمقصود بشهادة التصديق الرقمي.
2. الوقوف على الالتزامات الأساسية التي فرضتها التشريعات على جهات المصادقة الرقمية، سواء كانت هذه الالتزامات في مواجهة صاحب شهادة التصديق الرقمي أو في مواجهة الغير؟

3. الوقوف على صور المسؤولية النظامية التي تقع على عاتق جهات المصادقة الرقمية، سواء كانت مسؤولية مدنية ناتجة عن إخلالها بالتزاماتها المنصوص عليها في العقد الذي يربطها بعملائها أو التي يفرضها النظام، أو مسؤوليتها الجزائية متى ما كان هذا الإخلال يشكل جريمة جزائية، مع بيان نطاق هذه المسؤولية، وأثر تحققها.

إشكالية البحث:

تبرز إشكالية هذه الدراسة في الجوانب النظامية التي تثيرها المصادقة الرقمية على التعاملات الإلكترونية. وعليه يمكن تحديد مشكلة البحث في التساؤلات الآتية:

1. ما المصادقة الرقمية؟ وما أبرز وسائل المصادقة الرقمية على التعاملات الإلكترونية؟
2. ما الجهات المخولة بالمصادقة الرقمية على التعاملات الإلكترونية؟ وما المقصود بشهادة التصديق الرقمي؟
3. ما الالتزامات النظامية المفروضة على جهات المصادقة الرقمية سواء كانت هذه الالتزامات في مواجهة صاحب شهادة التصديق الرقمي أو في مواجهة الغير؟
4. ما صور المسؤولية النظامية المترتبة التي تثيرها عملية التصديق الرقمي؟ وما نطاق هذه المسؤولية؟ وما أثر تحققها؟
5. مدى كفاية النصوص المنظمة لمسؤولية جهات المصادقة الرقمية، وما القصور التنظيمي الذي يحد من فعالية عملية التصديق الرقمي؟

منهج البحث:

يتبع موضوع البحث المنهج التحليلي المقارن، وذلك من خلال الآتي:

1. قراءة وتحليل مقتضيات نظام التعاملات الإلكترونية السعودي ونظيره من بعض التشريعات المقارنة الأجنبية ذات الصلة بموضوع البحث، ونخص منها قانون الأونسيترال النموذجي، والتوجيه الأوروبي، والقانون الفرنسي، والقانون الإماراتي.
2. الاستعانة بالدراسات والاجتهادات الفقهية، والأنظمة الوطنية، والتشريعات المقارنة الأجنبية التي محصت موضوع البحث؛ للوقوف على كيفية تناولها له.

خطة البحث:

سوف يقسم الباحث خطة البحث إلى المقدمة وتشتمل على بيان موضوع البحث، وأهميته، وأهدافه، وخطته وتقسيماته، ومبحثين، وخاتمة تتضمن أهم نتائج البحث، والتوصيات، وبناء على ما سبق سوف تكون تفاصيل الخطة على النحو التالي:

المبحث الأول: ماهية المصادقة الرقمية والتنظيم القانوني لجهاتها.

المطلب الأول: ماهية المصادقة الرقمية على التعاملات الإلكترونية.

الفرع الأول: تعريف التصديق الرقمي وطبيعته.

الفرع الثاني: وسائل المصادقة الرقمية على التعاملات الإلكترونية.

الفرع الثالث: الجهات المرخص لها بالمصادقة الرقمية على التعاملات الإلكترونية في التشريعات المقارنة.

الفرع الرابع: مفهوم شهادة التصديق الرقمي.

المطلب الثاني: التزامات جهات المصادقة الرقمية.

الفرع الأول: الالتزام بالتحقق من صحة البيانات.

الفرع الثاني: الالتزام بإصدار وتسليم وحفظ شهادة التصديق الرقمي.

الفرع الثالث: الالتزام بالحفاظ على سرية بيانات التصديق.

الفرع الرابع: الالتزام بإلغاء أو إيقاف شهادة التصديق.

- **المبحث الثاني:** صور المسؤولية النظامية لجهات المصادقة الرقمية.

المطلب الأول: المسؤولية المدنية لجهات المصادقة الرقمية.

الفرع الأول: طبيعة التزام جهات المصادقة الرقمية.

الفرع الثاني: التكييف القانوني الأنسب للمسؤولية المدنية لجهات المصادقة الرقمية.

الغصن الأول: المسؤولية العقدية لجهات المصادقة الرقمية.

الغصن الثاني: المسؤولية التقصيرية الجهات المصادقة الرقمية.

المطلب الثاني: المسؤولية الجزائية لجهات المصادقة الرقمية.

الفرع الأول: نطاق المسؤولية الجزائية لجهات المصادقة الرقمية.

الفرع الثاني: أثر تحقق المسؤولية الجزائية لجهات المصادقة الرقمية.

الخاتمة: وتشتمل على أهم نتائج البحث، وتوصياته.

المبحث الأول

ماهية المصادقة الرقمية والتنظيم القانوني لجهاتها

نظراً لما يتمتع به التصديق الرقمي من أهمية سواء على المستوى الاقتصادي أو القانوني؛ فإن ذلك يقتضي من الباحث التطرق لماهية المصادقة الرقمية على التعاملات الإلكترونية (المطلب الأول)، ثم التزامات جهات المصادقة الرقمية (المطلب الثاني).

المطلب الأول

ماهية المصادقة الرقمية على التعاملات الإلكترونية

تظهر الحاجة إلى وجود جهة محايدة في

التعاملات الإلكترونية، تقوم بدور الوسيط المؤتمن بين أطرافها، فتؤكد هويتهم وتحدد أهليتهم للتعامل الإلكتروني، وتضمن سلامة البيانات المتداولة من خلال إجراءات معينة تسمى بـ(المصادقة الرقمية على التعاملات الإلكترونية) (Loeb,1955,p.17)، ولهذا فإن البحث في ماهية المصادقة الرقمية على التعاملات الإلكترونية يقتضي الوقوف على تعريف التصديق الرقمي وطبيعته (الفرع الأول)، مع استعراض وسائل المصادقة الرقمية على التعاملات الإلكترونية (الفرع الثاني)، والتعرف على الجهات المرخص لها بالمصادقة الرقمية على التعاملات الإلكترونية (الفرع الثالث)، ثم مفهوم شهادة التصديق الرقمي (الفرع الرابع).

الفرع الأول

تعريف التصديق الرقمي وطبيعته

لما كان التصديق الرقمي يعمل على خلق بيئة إلكترونية آمنة للتعاملات الإلكترونية؛ لذا سوف يتطرق الباحث في هذا الفرع لتعريفه (أولاً)، ثم لبيان طبيعته (ثانياً).

أولاً-تعريف التصديق الرقمي:

يعرف التصديق بوجه عام بأنه «مجموعة من الأشياء أو العناصر التي تعتمد على الغرض الذي يراد استخدام التوثيق لتحقيقه» (الشنراقي،2013، ص: 79).

أما التصديق الرقمي فقد عرف بأنه «وسيلة فنية آمنة تساهم في التحقق من صحة التوقيع الإلكتروني أو المحرر الإلكتروني، حتى يمكن نسبته إلى شخص أو كيان معين، يصدر عن جهة موثوقة أو طرف محايد يسمى مقدم خدمات التصديق» (البكباشي،2009، ص: 107).

كما عرف بأنه «عملية لتحقيق التأكد والموثوقية في هوية المستخدم باستخدام الأجهزة والكيانات الأخرى من خلال نظم المعلومات والاتصالات» (العبيدي،2012، ص: 161).

وفي إطار ما سبق يُعرف الباحث التصديق الرقمي بأنه «الإجراءات التي من خلالها يتم خلق الثقة في صاحب التوقيع الرقمي والتأكيد على سلامة المحرر الرقمي الذي يحمل هذا التوقيع بهدف ضمان سلامة وتأمين المعاملات الإلكترونية، ويتولى هذه الإجراءات طرف محايد يطلق عليه مقدم خدمات التصديق الرقمي».

ثانياً-طبيعة التصديق الرقمي:

فيما يتعلق بطبيعة عملية التصديق الرقمي، يقول البعض (E. Caprioli ,1998, p.29) (عبد الفتاح،2006، ص: 70). «أن منح شخص ثالث سلطة توثيق التوقيع يقرِّب مهمة الجهات القائمة على هذا الأمر من مهمة الموثّق في النظام الفرنسي، أي التأكد من شخص المتعاقد ومن مضمون التصرف المراد توثيقه» (الحفني،1992، ص: 2).

وانطلاقاً من هذا القول فقد تم معالجة موضوع سلطات التصديق تحت اسم: فكرة الموثق الإلكتروني (Notaire électronique ou cyber notaire)، ومع ذلك يبقى فرق جوهري بين سلطات التصديق الإلكتروني والموثق، يتمثل في أن هذه السلطات لا تملك أو ليس من مهمتها أن تتدخل في إنشاء وتأريخ وحفظ المحررات القانونية طبقًا للإجراءات المنصوص عليها في القانون» (E. Caprioli ,1998,p.30).

ولهذا تقتصر مهمة جهة التصديق على فحص التصرفات النظامية الرقمية، ومنح أصحاب الشأن شهادة بنفس هذا الغرض تسمى شهادة التصديق الرقمي، والعامل المشترك بين جهة المصادقة والموثق هو الالتزامات التي تقع على عاتق كل منهما.

الفرع الثاني

وسائل المصادقة الرقمية على التعاملات الإلكترونية

تجدر الإشارة إلى أن المقصود بالتعاملات الإلكترونية هي كل التعاملات غير الورقية التي يتم إنجازها باستخدام وسيط الكتروني، وبغض النظر عن أطرافها سواء كانوا أشخاص طبيعيين أو اعتباريين.

وقد عَرَف نظام التعاملات الإلكترونية السعودي رقم (م/٨٠) لعام ١٩٢٨، في مادته الأولى التعاملات الإلكترونية بأنها «أي تبادل، أو تراسل، أو تعاقد، أو أي إجراء آخر يُبرم أو يُنفذ بشكل كلي أو جزئي -بوسيلة إلكترونية» كما عَرف قانون إمارة دبي الخاص بالمعاملات والتجارة الإلكترونية رقم (٢) لعام ٢٠٠٢م، في مادته الثانية المعاملات الإلكترونية بأنها «أي تعامل أو عقد أو اتفاقية يتم إبرامها أو تنفيذها بشكل كلي أو جزئي بواسطة المراسلات الإلكترونية».

وإذا تم إمعان النظر في التعريفين السابقين يُلاحظ أنهما بمعنى واحد، مما يتبين معه أن التعاملات الإلكترونية قد تكون تبادلا، أو تراسلا، أو تعاقدًا، أو تعاملا، أو عقدًا، أو اتفاقية، وجميعها ما هو إلا مفهوم مكرر لمضمون العقد، والذي لا يشترط أن يأخذ شكل محرر مكتوب، بل يكفي أن يتم تنفيذه بشكل كلي أو جزئي بواسطة وسيلة إلكترونية أيًّا كانت هذه الوسيلة سواء أكانت إنترنتًا، أو تلكسًا، أو فاكسًا، أو غير ذلك؟ (حجازي،2002، ص: 96).

وفيما يتعلق بوسائل المصادقة على التعاملات الإلكترونية التي تتم عن طريق وسائط إلكترونية، فسوف يستعرض الباحث أهم هذه الوسائل المستخدمة في الوقت الراهن كبديل للتوقيع الخطي اليدوي؛ لملائمتها لطبيعة التعاملات الإلكترونية، وتجدر الإشارة إلى أن المنظم السعودي في تعريفه للتوقيع الإلكتروني قام ببيان ما للتوقيع من وظائف، مع ذكر

أمثلة -فقط- للتوقيع الإلكتروني، ولم يحصره في صور بعينها، تاركاً المجال لإدخال صور جديدة لهذا النوع من التوقيع قد تظهر مستقبلاً، ولذلك سوف نستعرض أهم صور التوقيع الإلكتروني التي تتمثل في الآتي:

أولاً: التوقيع الرقمي أو الكودي (Digital Signature)، وهو ما يتم باستخدام مجموعة من الحروف، والرموز، والأرقام، والمعادلات الرياضية المعقدة، يختارها صاحب التوقيع بنفسه، ويقوم باستعمالها في التوقيع على التعاملات الإلكترونية، ويعتمد هذا النوع من التوقيع على برنامج معين يمنع أي شخص من كشف رسالة البيانات باستثناء من يملك مفتاح فك التشفير، مع التحقق من أن الرسالة قد تم تحويلها باستخدام المفتاح الخاص، بجانب تأكده من عدم إجراء أي تعديل، أو تغيير على مضمون الرسالة الواردة (Chris ,2011,p.53) .

ثانياً: التوقيع بالخواص الذاتية (البيومتري) (Biometric Signature)، وهذا التوقيع يعتمد على تقنية الخواص الحيوية الطبيعية، فيستخدم فيها الصفات الجسدية والسلوكية والفيزيائية والطبيعية لكل إنسان، والتي تميزه عن غيره من الناس.

ويشمل التوقيع البيومتري العديد من الطرق التي تتمثل في البصمة الشخصية، والتحقق من نبرة الصوت، ومسح العين البشرية (بصمة القزحية)، وخواص اليد البشرية، والتعرف على الوجه البشري، والتوقيع الشخصي بواسطة اليد الذي يحول إلى توقيع إلكتروني معتمد (ممدوح،2010، ص: 86).

ثالثاً: التوقيع بالقلم الإلكتروني(op- Pen)، وهو ما يتم عن طريق قيام مرسل الرسالة بإجراء توقيع على شاشة الحاسوب الآلي باستخدام قلم إلكتروني، ويتم حفظ هذا التوقيع في برنامج يأخذ قياسات التوقيع، ويحدد شخص المرسل، ووقت التوقيع، وفي سبيل التحقق من صحة توقيع المرسل يقوم البرنامج بإجراء مقارنة مادية بين توقيعات المرسل المحفوظة بالبرنامج والتوقيعات المحفوظة بالأرشيف، وتتولى جهات المصادقة الرقمية القيام بعملية المقارنة للتحقق من صحة ومطابقة التوقيع، ومنحه الحجية النظامية من خلال إصدار شهادة التصديق الرقمي(فهمي،2008،ص: 59).

رابعاً: التوقيع باستخدام البصمة الرقمية (Electronic footprint)، البصمة الرقمية هي: عبارة عن معادلات رقمية خوارزمية معينة، تسمى اقترانات التمويه. فتطبق هذه الخوارزميات عمليات حسابات رياضية على الرسالة لإنتاج بصمة في صورة مستند أو رسالة إلكترونية، ويكون لهذه البصمة القدرة على التعرف على الرسالة الأصلية بدقة فائقة

وتمييزها عن غيرها، ولهذا فإن إجراء أي تغيير أو تعديل في الرسالة سوف يترتب عليه إنشاء بصمة جديدة مغايرة تماماً للرسالة الأصلية، وهو الأمر الذي يجعل من التوقيع باستخدام البصمة الرقمية أكثر دقة وأمانًا في التعاملات الإلكترونية (عبد المجيد،2007، ص: 57).

ولكي تتمتع كلٌّ من التعاملات الإلكترونية والتوقيع الإلكتروني عليها بالحجة النظامية في الإثبات الذي يتمتع به المحرر الورقي والتوقيع اليدوي لابد من توافر عدة شروط بالنسبة لكل منهما:

فأما بالنسبة للتعاملات الإلكترونية فإنه يلزم أن يكون المحرر الإلكتروني مقروءاً ومعبراً عن محتواه كما هو الحال في المحرر الورقي التقليدي، مع قدرة المحرر الإلكتروني على الاحتفاظ بما فيه من بيانات لمدة زمنية طويلة، وعدم قابلية إجراء أي تعديل أو تغيير في محتوى المحرر الإلكتروني.

وبالنسبة للتوقيع الإلكتروني يلزم أن تتوافر فيه عدة شروط تُمَكنه من القيام بنفس وظائف التوقيع اليدوي فيما يتعلق بتحديد هوية المُوقَع على المحررات أو التعاملات الإلكترونية، والتعبير عن إرادة المُوقّع في الالتزام بما وقّع عليه، والقبول بمضمون التعامل الإلكتروني المراد إثباته (Bruce ,2010, p.49).

وإن كان المنظم السعودي لم يحدد أي صورة من صور التوقيع الإلكتروني المعتمدة بشكل صريح إلا أنه جعل اعتمادها كحجة معتبرة في الإثبات مرهونًا بتوافر شروط معينة تناولها في المادة (9) من نظام التعاملات الإلكترونية السعودي التي تنص على أنه

1. «يقبل التعامل الإلكتروني أو التوقيع الإلكتروني دليلاً في الإثبات إذا استوفى سجله الإلكتروني متطلبات حكم المادة (الثامنة) من هذا النظام.
2. يجوز قبول التعامل الإلكتروني أو التوقيع الإلكتروني قرينة في الإثبات؛ حتى وإن لم يستوف سجله الإلكتروني متطلبات حكم المادة الثامنة من هذا النظام.
3. يعد كل من التعامل الإلكتروني، والتوقيع الإلكتروني، والسجل الإلكتروني حجة يعتد بها في التعاملات، وأنّ كلا منها على أصله (لم يتغير منذ إنشائه) ما لم يظهر خلاف ذلك.»

كما أوردت الفقرة الثالثة من المادة (14) من ذات النظام عدة شروط للإقرار بصحة التوقيع الإلكتروني والتعامل المرتبط به، وتتمثل في الآتي:

(أ)« أن التوقيع الإلكتروني هو توقيع الشخص المحدد في شهادة التصديق الرقمي.

(ب) أن التوقيع الإلكتروني قد وضعه الشخص المحدد في شهادة التصديق الرقمي، وبحسب

الغرض المحدد فيها.

(ج) أن التوقيع الإلكتروني لم يطرأ عليه تغيير منذ وضع التوقيع الإلكتروني عليه».

وقد حذا المشرع الإماراتي حذو المنظم السعودي في هذا الخصوص؛ ذلك أن قانون إمارة دبي رقم (٢) لعام ٢٠٠٢ م بشأن المعاملات والتجارة الإلكترونية قد اشترط في الفقرة الأولى من المادة (٢٠) منه لإسباغ الحجية في الإثبات على التوقيع الإلكتروني، أن يتوافر فيه ما يلي:

1. « ينفرد به الشخص الذي استخدمه.
2. ومن الممكن أن يثبت التوقيع هوية ذلك الشخص.
3. وأن يكون تحت سيطرته سواء بالنسبة لإنشائه، أو وسيلة استعماله وقت التوقيع.
4. ويرتبط بالرسالة الإلكترونية ذات الصلة به، وبطريقة توفر تأكيداً يُعول عليه حول سلامة التوقيع».

ونستقي مما تقدم أنه في حال توافر الشروط التي وضعتها التشريعات السابقة في التوقيع الإلكتروني فإنه يصبح بذلك توقيعًا معتمدًا ومحميًّا، ويتمتع بالحجية النظامية في الإثبات شأنه في ذلك شأن التوقيع اليدوي التقليدي، ولاسيما أن التقدم التقني قد دعم الثقة فيه، ناهيك عن وجود جهات مصادقة رقمية تقوم بالتحقق من صحة التوقيع الإلكتروني ونسبته إلى صاحبه، وإصدار شهادة تصديق رقمي خاصة تفيد ذلك (George ,2001, p.237).

الفرع الثالث

الجهات المرخص لها بالمصادقة الرقمية على التعاملات الإلكترونية في التشريعات المقارنة

من خلال هذا الفرع سوف نقف على التعريفات التي وضعت للجهات المرخص لها بالمصادقة الرقمية على التعاملات الإلكترونية (أولاً)، ثم نتعرف على الهيئة المختصة بمنح التراخيص لجهات المصادقة الرقمية ومراقبة أعمالها (ثانياً).

أولاً-تعريف جهات المصادقة الرقمية:

تجدر الإشارة إلى أنه لا توجد تسمية موحدة لهذه الجهات في تشريعات الدول المختلفة التي نظمت عمل هذه الجهات ومسؤوليتها، كما أنه لا يوجد تعريف فقهي متفق عليه لهذه الجهات. لذلك سوف يعرض الباحث بعض التعريفات القانونية التي جاءت بها تشريعات بعض الدول مع التسميات المختلفة لجهات المصادقة الرقمية، ثم يليها أهم التعريفات الفقهية لتلك الجهات:

1-التعريفات القانونية لجهات المصادقة الرقمية في التشريعات المقارنة:

أطلق قانون الأونسيترال النموذجي المتعلق بالتوقيعات الإلكترونية على جهة المصادقة الرقمية اسم (مقدم خدمات التصديق) وقد عرفه في المادة (٢/ هـ) منه على أنه «شخص يصدر

الشـهادات ويجـوز أن يقـدم خدمـات أخـرى ذات صلـة بالتوقيعـات الإلكترونيـة». نلاحـظ علـى هـذا التعريـف بأنـه ألـزم جهـة المصادقـة الرقميـة بضـرورة توفيـر خدمـات التصديـق الرقمـي كحـد أدنـى، هـذا مـع وجـود إمكانيـة لتقديـم خدمـات أخـرى يكـون لهـا صلـة بالتوقيـع الإلكترونـي، وهـذا يعنـي إمكانيـة أن تكـون خدمـة التصديـق الرقمـي هـي النشـاط الوحيـد الرئيسـي لجهـة المصادقـة الرقميـة، كمـا مـن المتصـور أن يكـون هـذا النشـاط فرعيًّـا بجانـب الأنشـطة لهـذه الجهـة. كمـا أطلـق التوجيـه الأوروبـي الصـادر فـي 1999/12/13م بشـأن التوقيعـات الإلكترونيـة على جهـة المصادقـة الرقميـة مصطلـح «مقدم خدمـات التصديـق» فـي المـادة (٢) فقـرة (١١) منـه، وعرفـه بأنـه « كل كيـان أو شـخص طبيعـي أو معنـوي يقدم شـهادات تصديـق إلكترونيـة أو تقديـم خدمـات أخـرى متصلـة بالتوقيعـات الإلكترونيـة». ويقصـد بالخدمـات المرتبطـة بالتوقيـع الإلكترونـي التقنيـات التـي تكـون قـادرة علـى إصـدار توقيـع نموذجـي، أو خدمـات الاطـلاع والنشـر والخدمـات المعلوماتيـة الأخـرى مثـل أرشـفة البيانـات.

وعـرف المشـرع الفرنسـي جهـة المصادقـة الرقميـة تحـت مسـمى (المكلـف بخدمـة التصديـق الإلكترونـي) فـي المـادة (11/1) مـن المرسـوم رقـم 272 /2002 الصـادر فـي 30 مـارس 2002 بأنـه «مقـدم خدمـة التصديـق: -أي شـخص يقـدم شـهادات التصديـق أو خدمـات أخـرى فـي مجـال التوقيـع الإلكترونـي».

11. -Prestataire de services de certification électronique : toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique).

بينمـا أطلق قانـون المعاملات والتجـارة الإلكترونية لإمـارة دبـي رقـم 2 لسـنة 2002 م علـى جهـة المصادقـة الرقميـة (مـزود خدمـات التصديـق) فـي المـادة (2) منـه، وعرفـه بأنـه «أي شـخص أو جهـة معتمـدة أو معتـرف بهـا تقـوم بإصـدار شـهادات تصديـق إلكترونيـة أو أيـة خدمـات أو مهمـات متعلقـة بهـا وبالتواقيـع الإلكترونيـة». ونلاحـظ أن التعريفات الأربعة السـابقة والواردة في كلٍّ مـن قانـون الأونسـيترال، والتوجيـه الأوروبـي، والقانـون الفرنسـي، وقانـون المعامـلات والتجـارة الإلكترونيـة لإمـارة دبـي، اتفقـوا علـى أن مـن يقـدم خدمـات المصادقـة الرقميـة يمكـن أن يكون شـخصاً طبيعيـاً أو معنويـاً وإن كان التوجيـه الأوروبـي قـد ذكـر ذلـك صراحة، فـإن القانـون الفرنسـي، وقانون الأونسـيترال ذكـرا كلمـة «شـخص فقـط»، فهـي عامـة تشـمل الشـخص الطبيعـي والمعنـوي. ويعتقد الباحـث أنـه ليـس مـن المتصـور فـي الواقـع العملي أن يقـوم الشـخص الطبيعـي بهـذا العمـل؛ وذلـك لأن

خدمات التصديق الرقمي تحتاج إلى إمكانيات مادية ضخمة، وتقنية مكلفة وعالية الجودة لا يستطيع القيام بهذا إلا الشخص المعنوي، سواء أكان شخصا معنوياً عاماً أم كان شخصاً معنوياً خاصاً؟

وأما بالنسبة للمنظم السعودي فقد عرف في الفقرة (21) من المادة الأولى من نظام التعاملات الإلكترونية رقم (م/80) لعام 1428هـ مصطلح «مقدم خدمات التصديق الرقمي» بأنه «شخص مرخص له بإصدار شهادات التصديق الرقمي، أو أي خدمة أو مهمة متعلقة بها وبالتوقيعات الإلكترونية وفقاً لهذا النظام».

ويلاحظ على ما ورد ذكره من تعريفات أن معظم التشريعات ركزت في تحديدها لمفهوم جهات المصادقة الرقمية على بيان الوظيفة الأساسية لهذه الجهات والمتعلقة بإصدار شهادات التصديق الرقمي، بالإضافة لتقديم أي خدمات أخرى ذات صلة بالتوقيع الإلكتروني.

2. التعريفات الفقهية لجهات المصادقة الرقمية:

سوف يستعرض البحث بعض التعريفات الفقهية المتعلقة بجهات المصادقة الرقمية

أولاً: عُرفت جهة المصادقة الرقمية بأنها «طرف ثالث محايد وموثوق به، يقوم بطرقه الخاصة بالتأكد من صحة صدور الإرادة التعاقدية ممن تنسب إليه» (Froomkin ,1996, p.5).

ثانياً: وعُرفت جهات المصادقة الرقمية بأنها «هي الجهات التي تصدر شهادة تربط بين المُوقَع وبيانات إنشاء التوقيع وتلك الشهادات هي جهات مرخص لها في داخل الجمهورية أو خارجها بتقديم خدمات تتعلق بالتوقيع الإلكتروني» (يوسف،2008، ص: 52).

ثالثاً: كما عُرفت جهة المصادقة الرقمية بأنها «هيئة عامة أو خاصة تعمل تحت إشراف السلطة التنفيذية وتكون غالبا من ثلاث مستويات مختلفة من السلطة، تتمثل الأولى في السلطة الرئيسية، والثانية في سلطة التصديق، أما الثالثة فهي سلطة التسجيل المحلية» (منصور،2016، ص: 73).

رابعاً: وكذلك عُرفت جهة المصادقة الرقمية بأنها «هيئة عامة أو خاصة تسعى إلى ملء الحاجة الملحة لوجود طرف ثالث موثوق به، يقدم خدمات أمنية في التجارة الإلكترونية، من خلال إصدار شهادات تثبت صحة حقيقة معينة متعلقة بموضوع التبادل الإلكتروني، لتوثيق هوية الأشخاص مستخدمي التوقيع الرقمي، وكذلك نسبة المفتاح العام المستخدم إلى صاحبه (البياتي،2014، ص: 263).

وفي إطار ما سبق يمكن للباحث أن يُعرف جهة المصادقة الرقمية بأنها «عبارة عن جهة محايدة، تخضع لإشراف الدولة ورقابتها، وتقوم من خلال إصدارها لشهادة المصادقة

الرقمية بعملية التصديق والتأكد من صحة التوقيع الإلكتروني وربطه بالبيانات الواردة بالسند الإلكتروني والمعلومات الواردة بها، بالإضافة إلى أي خدمات أخرى تتعلق بالتوقيع الإلكتروني».

ثانياً -الهيئة المختصة بمنح التراخيص لجهات المصادقة الرقمية ومراقبة أعمالها في التشريعات المقارنة:

اعتمدت بعض التشريعات نظام الترخيص المسبق لمقدمي خدمات المصادقة الرقمية كما هو معمول به في النظام السعودي والتشريع الإماراتي، وهذا يعني أنه لكي تتمكن جهة المصادقة الرقمية من مزاولة عملها فإن عليها الحصول على ترخيص من الجهة التي حددها هذا النظام، فنجد أن نظام التعاملات الإلكترونية السعودي قد أناط مهمة منح إصدار شهادات التصديق الرقمي إلى هيئة الاتصالات وتقنية المعلومات وذلك ضمن الفقرة الثانية من المادة (15) منه، وجاء فيها «تتولى الهيئة تطبيق هذا النظام، ولها في سبيل تحقيق ذلك الاختصاصات الآتية:

(أ) إصدار التراخيص لمزاولة نشاط (مقدم خدمات التصديق)، وتجديدها، وإيقاف العمل بها، وإلغاؤها. وتوضح اللائحة الشروط والإجراءات اللازمة للحصول على الترخيص، ومدته، وتجديده، ووقفه، وإلغائه، والتنازل عنه، والتزامات المرخص له، وضوابط إيقاف نشاط المرخص له وإجراءاته، والآثار المترتبة على ذلك.

(ب) التحقق من التزام مقدمي خدمات التصديق بالتراخيص الممنوحة لهم، وبأحكام هذا النظام واللائحة، والقرارات التي تصدرها الهيئة.

(ج) اتخاذ الإجراءات اللازمة وفقاً لما تحدده اللائحة لضمان استمرار الخدمات المقدمة إلى الأشخاص المتعاملين مع مقدم خدمات التصديق عند موافقتها على إيقاف نشاطه، أو إلغاء ترخيصه أو عدم تجديده.

وأما بالنسبة للتشريع الإماراتي فنجد أن القانون الاتحادي الإماراتي بشأن المعاملات والتجارة الإلكترونية قد وضع الإطار العام والهيئة المختصة بمنح الترخيص، حيث منحت المادة الأولى من هذا القانون للسلطة المحلية المختصة في كل إمارة من إمارات الدولة، صلاحية تحديد الهيئة المختصة بمنح التراخيص.

فنجد أن قانون المعاملات والتجارة الإلكترونية لإمارة دبي قد نص في المادة رقم (٢) على أن الهيئة المختصة بمنح التراخيص، هو «رئيس سلطة منطقة دبي الحرة للتكنولوجيا والتجارة الإلكترونية والإعلام». وعلى هذا الرئيس

بوصفه السلطة المخول بها تطبيق هذا القانون أن يعين مراقباً لخدمات المصادقة الرقمية، وقد حددت المادة (20) من القانون السابق اختصاصات هذا المراقب بنصها على أن «يضع المراقب قواعد لتنظيم وترخيص عمل مزودي خدمات التصديق الذين يعملون في الإمارة ويرفعها للرئيس لاعتمادها، بما في ذلك ما يلي: 1-طلبات تراخيص أو تجديد تراخيص مزودي خدمات التصديق وممثليهم المفوضين والأمور المتعلقة بذلك.

2-أنشطة مزودي خدمات التصديق، ويشمل ذلك طريقة ومكان وأسلوب الحصول على أعمالهم وجذب الجمهور لها».

ويتبين من النص السابق أن المشرع الإماراتي أسند للمراقب خدمات التصديق مهمة القيام بعملية الترخيص، والتصديق، والمراقبة لأنشطة جهات المصادقة الرقمية، والإشراف عليها، سواء كانت الجهة طالبة الترخيص تؤدي خدمة المصادقة على التوقيعات الإلكترونية وإصدار شهادات التصديق الرقمي بذلك أو غيرها من خدمات المصادقة الرقمية.

بينما أخذ المشرع الفرنسي موقفاً مغايراً لما سبق حيث أنه اعتمد المبدأ الذي جاء به التوجيه الأوروبي رقم 93 لسنة ١٩٩٩م الخاص بالتوقيعات الإلكترونية ضمن المادة (2/3) والذي ألزم الدول الأعضاء بعدم فرض أي قيود على إنشاء سلطات التصديق أو تطلب أي ترخيص مسبق، ووفقاً لهذا المبدأ تكون هناك حرية في ممارسة نشاط إصدار شهادات التصديق الرقمي حيث يحق لأي هيئة أن تمارس هذا النشاط دون حاجة للحصول على ترخيص مسبق من السلطات الفرنسية، وضمن المشرع الفرنسي هذا المبدأ في المرسوم رقم 272 لسنة 2001 وفي مقابل ذلك سمح التوجيه الأوروبي أعلاه للدول الأعضاء بإنشاء أنظمة الاعتماد وجهات المصادقة الرقمية، وبالفعل أنشأ المشرع الفرنسي نظاماً لاعتماد جهات المصادقة لكن هذا النظام اختياري، أي: يكون بمقدور جهة المصادقة الرقمية أن تمارس نشاطها دون حاجة للحصول على اعتماد من قبل الهيئة التي أنشأتها الدولة، ومقابل ذلك لها الحق في تقديم طلب لاعتمادها، ولكن يجب أن تتوافر فيها الشروط التي ينص عليها القانون، بينما يلاحظ أن الواقع العملي يجبر جهات المصادقة الرقمية على تقديم طلب لاعتمادها والسبب في ذلك هو أن القانون الفرنسي اشترط لكي يتمتع التوقيع الإلكتروني بالحجية يجب أن يتم التأكد من صحته بمقتضى شهادة التصديق الرقمي المعتمدة (أي صادرة من جهة معتمدة) وبالتالي فإن القانون الفرنسي قد ربط حجية التوقيع الإلكتروني باعتماد جهة المصادقة الرقمية (التهامي،2008، ص: 416).

الفرع الرابع

مفهوم شهادة التصديق الرقمي

للوقوف على مفهوم شهادة التصديق الرقمي لابد من التطرق لتعريف هذه الشهادة (أولاً) وما تتضمنه من بيانات (ثانياً) وذلك على النحو التالي:

أولاً-تعريف شهادة التصديق الرقمي:

عُرفت شهادة التصديق الرقمي بأنها «صك أمان صادر عن جهة مختصة يفيد صحة وضمان المعاملة الإلكترونية وذلك من حيث صحة البيانات ومضمون المعاملة وأطرافها» (حجازي،2008، ص: 454).

وعُرفت شهادة التصديق الرقمي بأنها «مستند إلكتروني يربط المفتاح العام وشخصًا معينًا ويحدد هوية ذلك الشخص» (التهامي،2008، ص: 777).

كما عُرفت بأنها «الشهادة التي تصدرها جهات التصديق المرخص لها من قبل الجهات المسئولة في الدولة لتشهد بأن التوقيع الإلكتروني هو توقيع صحيح ينسب إلى من أصدره ويستوفي الشروط والضوابط المطلوبة فيه باعتباره دليل إثبات يُعول عليه» (أبو الليل،2002، ص: 83).

ويتبين من التعريفات السابقة أن:

- شهادة التصديق الرقمي عبارة عن هوية شخصية للموقع.
- لابد أن تصدر شهادة التصديق الرقمي من جهة مرخص لها بممارسة هذا النشاط ومحايدة.
- أن الهدف من شهادة التصديق الرقمي هو تأكيد صحة وقانونية كلٍّ من البيانات التي تتضمنها الشهادة والتوقيع الإلكتروني (Burr et al. ,2013, p.8).

أما بالنسبة لتعريف التشريعات لشهادة التصديق فقد عرف المنظم السعودي شهادة التصديق الرقمي في الفقرة (17) من المادة الأولى من نظام التعاملات الإلكترونية بأنها «وثيقة إلكترونية يصدرها مقدم خدمات تصديق، تستخدم لتأكيد هوية الشخص الحائز على منظومة التوقيع الإلكتروني، وتحتوي على بيانات التحقق من توقيعه».

وعرف قانون المعاملات والتجارة الإلكترونية لإمارة دبي رقم 2 لسنة 2002 مصطلح (شهادة المصادقة الإلكترونية) بأنها شهادة يصدرها مزود خدمات التصديق يفيد فيها تأكيد هوية الشخص أو الجهة الحائزة على أداة توقيع معينة».

بينما عرفها التوجيه الأوروبي رقم 93 لسنة 1999 الخاص بالتوقيعات الإلكترونية ضمن المادة (٣) بأنها «تلك التي تربط بين أداة التوقيع وبين شخص معين وتؤكد شخصية المُوقَع».

ويتضح مما سبق أنّ كلا من النظام السعودي وقانون إمارة دبي قد اعتمدا التعريف الوارد في التوجيه الأوروبي؛ نظرا لكونه تعريفًا

يتضح من خلاله بشكل جلي الهدف المرجو من شهادة التصديق الرقمي، وهو بيان هوية شخص المُوقَع، بالإضافة إلى أنه يؤكد وظيفتها الأساسية في نسبة التوقيع الإلكتروني إلى شخص معين، وذلك بأسلوب بسيط ومحدد.

كما نجد أن المشرع الفرنسي عرف شهادة التصديق في المادة (1-1) من المرسوم رقم 272 لسنة 2001 بأنها «مستند إلكتروني يربط بين بيانات التحقق من التوقيع الإلكتروني وبين المُوقَع».

(9. Certificat électronique : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire).

ويلاحظ على تعريف المشرع الفرنسي لشهادة التصديق الرقمي أنه اكتفى بتحديد الهدف من إصدار شهادة التصديق الرقمي والذي يتمثل بتأكيد الارتباط بين التوقيع وبين بيانات إنشاء التوقيع الإلكتروني الذي يؤدي بدوره إلى بيان شخصية المُوقَع وهويته، والسبب في ذلك أنّ جهة التصديق في فرنسا قد تكون معتمدة، وقد تكون بسيطة، وفي هذه الحالة سوف يكون لدينا نوعان من شهادة التصديق: الأولى شهادة تصديق رقمي معتمدة، والثانية شهادة تصديق رقمي بسيطة، وهذا على خلاف ما هو موجود في النظام السعودي حيث إن شهادة التصديق واحدة متمثلة في شهادة التصديق التي تصدر من جهة التصديق المعتمدة.

ثانياً-البيانات التي يشترط توافرها في شهادة التصديق الرقمي:

قد أحال نظام التعاملات الإلكترونية السعودي للائحته التنفيذية مهمة تحديد البيانات التي يجب أن تحتويها شهادة التصديق الرقمي حيث نصت المادة (١٩) من اللائحة التنفيذية للنظام على هذه البيانات، وهذه الأخيرة منها ما هو متعلق بصاحب شهادة التصديق الرقمي، ومنها ما يتعلق بجهة المصادقة الرقمية، ومنها ما يتعلق بشهادة التصديق نفسها.

1-البيانات التي تتعلق بصاحب شهادة التصديق الرقمي: -

وهي البيانات التي تتعلق بهوية صاحب الشهادة التي تشمل اسمه، وعنوانه بالكامل، وأي معلومات شخصية أخرى.

وعلى جهة المصادقة الرقمية التحقق من هوية شخص المُوقَع، وإدراجها في الشهادة سواء كانت شخصية أو وظيفية، والمفتاح الشفري العام لصاحب الشهادة، والمناظر للمفتاح الشفري الخاص به، والغرض من ذكر هذا المفتاح هو قيام الطرف الآخر المتعامل مع المُوقَع بمطابقة المفتاح العام المرسل إليه مع المفتاح العام المثبت في شهادة التصديق، وبالتالي التأكد من

هوية المُوقَع.

2-البيانات التي تتعلق بجهة المصادقة الرقمية :-

تتضمن شهادة التصديق كافة البيانات الدالة على جهة المصادقة الرقمية، ومنها رقم الترخيص الصادر لها، ونطاقه، وتاريخ إصداره، وفترة سريانه، واسم وعنوان الجهة التي أصدرت الشهادة، ومقرها الرئيسي، وكيانها القانوني، والدولة التابعة لها إن وجدت، والهدف كما يبدو من هذا البيان هو التعريف بالجهة وتحديد صفتها ومشروعيتها.

هذا بالإضافة إلى التوقيع الإلكتروني لجهة المصادقة الرقمية، والهدف من ذلك هو لإثبات تصديق جهة المصادقة الرقمية على صحة التوقيع الإلكتروني الموجود على المحرر الإلكتروني وما يتضمنه من بيانات.

3-البيانات التي تتعلق بصلاحية شهادة التصديق الرقمي: -

هي البيانات التي تفيد صلاحية شهادة التصديق الرقمي للاستخدام في التوقيع الإلكتروني، وهذا يعني أن شهادة التصديق تستعمل لأغراض التوقيع الإلكتروني دون الأغراض الأخرى خارج إطار أنشطة التصديق الرقمي، فالشهادة تستخدم للتأكد من هوية الموقع، وللتأكيد على صحة البيانات الواردة فيها.

وتتمثل البيانات المتعلقة بصلاحية شهادة التصديق في تاريخ إصدار الشهادة، وفترة سريانها، حيث عادة ما تصدر الشهاد بفترة صلاحية محددة، وبمجرد انتهاء هذه الفترة تصبح الشهادة غير صالحة للاستخدام، ويتم رفضها بشكل تلقائي من قبل برمجيات المرسل إليه، والهدف من وضع هذا البيان في الشهادة هو التأكد من أن التوقيع الإلكتروني قد تم إنشاءه أثناء فترة صلاحيتها.

المطلب الثاني

التزامات جهات المصادقة الرقمية

نظراً للدور الذي تقوم به جهات المصادقة الرقمية وخطورة الآثار المترتبة عليها، فقد عمدت أغلب تشريعات الدول إلى وضع مجموعة من الالتزامات يجب على هذه الجهات التقيد بها، وإلا سوف تنعقد مسؤوليتها النظامية في حالة إخلالها بتنفيذ هذه الالتزامات، ولذلك سوف يتناول الباحث ضمن فروع هذا المطلب أهم الالتزامات التي تتولد فيها مسؤولية هذه الجهات في معرض تقديمها خدمة المصادقة الرقمية.

الفرع الأول

الالتزام بالتحقق من صحة البيانات

تلتزم جهات المصادقة الرقمية بالتحقق من صحة البيانات المقدمة من الأشخاص التي

تصدر لهم شهادات التصديق، وبالتأكد من صفاتهم المميزة، والتي تمت المصادقة عليها وتضمينها في الشهادة، وهذا ما تضمنته الفقرة السادسة من المادة (18) من نظام التعاملات الإلكترونية السعودي التي جاء فيها «يجب على مقدم خدمات التصديق الالتزام بما يأتي: ... ٢-أخذ المعلومات ذات الصفة الشخصية من طالب الشهادة مباشرة، أو من غيره بشرط أخذ موافقة كتابية من طالب الشهادة على ذلك». كما نصت المادة (٢٠) من نفس النظام على أنه «يتحمل مقدم خدمات التصديق مسؤولية ضمان صحة المعلومات المصدقة التي تضمنتها الشهادة وقت تسليمها، وصحة العلاقة بين صاحب الشهادة وبياناتها الإلكترونية. وتقع مسؤولية الضرر الذي يحدث لأي شخص وثق- بحسن نية – بصحة ذلك».

ويعتبر الالتزام بالتحقق من صحة البيانات من أشد الالتزامات التي تقع على عاتق جهات المصادقة الرقمية، إذ يحتاج تنفيذه إلى عمال متخصصين يتمتعون بالمهارة الفنية والخبرة المهنية في هذا المجال للتحقق من صحة البيانات التي يقدمها طالب إصدار الشهادة وأهليته للتعاقد (الطوال،2010، ص: 75). أي التحقق من توافق بيانات الإنشاء مع بيانات التحقق من التوقيع، من خلال فحص الوثائق الرسمية كالهوية الوطنية وجواز السفر (كميل،2008، ص: 256)، والتي تحصل عليها جهة المصادقة عن طريق البريد العادي، أو بالاتصال المباشر، أو الإلكتروني، أو بحضور العميل شخصية أمام جهة المصادقة (التميمي،2011، ص: 53).

ونظراً لما قد يترتب على الإخلال بهذا الالتزام من أضرار جسيمة تؤثر بشكل سلبي على التجارة الإلكترونية، لذا يجب على جهات المصادقة تعويض المضرور الذي استند إلى شهادة تصديق الرقمي تتضمن بيانات غير صحيحة ما دام المتعامل ليس لديه وسيلة للتحقق من صحة تلك البيانات (حجازي،2002، ص: 17).

ويثار هنا تساؤل آخر وهو هل التزام جهة المصادقة الرقمية في هذا الصدد هو التزام بتحقيق نتيجة أم بذل عناية؟ للإجابة على هذا التساؤل ينبغي الرجوع إلى المادة (1/9ب) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية التي تنص على أنه «حيثما يُوفر مقدم خدمات التصديق خدمات التأييد توقيع الكتروني يجوز استخدامه لإعطاء مفعول قانوني بصفته توقيعا، يتعين على مقدم خدمات التصديق المشار إليه: (أ) .... (ب) أن يولي قدراً معقولاً من العناية لضمان دقة واكتمال كل ما يقدمه من تأكيدات جوهرية ذات صلة بالشهادة طيلة دورة سريانها، أو مدرجة في الشهادة».

كما نصت (24/ب) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي، على «أن يمارس عناية معقولة لضمان دقة واكتمال ما يقدمه واكتمال ما يقدمه من بيانات جوهرية ذات صلة بالشهادة أو مدرجة فيها طيلة سريانه». والبين من المادتين السابقتين أنهما قد اعتبرا التزام جهة المصادقة الرقمية من قبيل الالتزام ببذل عناية استناداً إلى أن كل ما تلتزم به هو بذل العناية الكافية للتحقق من مدى صحة البيانات المقدمة من العميل، ويترتب على ذلك أنه لا مسؤولية تذكر على جهة المصادقة في حال قيامها بالعناية اللازمة والمعقولة، وخاصة حينما يكون ظاهر الحال لا يدل على أن البيانات المقدمة لها من العميل تدعو إلى الشك في احتمال عدم توافقها مع الوثائق المرسلة، وبالتالي إذا أثبتت أن البيانات المقدمة يشوبها التزوير لسبب راجع إلى صاحبها، أو انتهاء سريانها فإنه لا تقع على عاتق جهة المصادقة أية مسؤولية، ويرى الباحث أن هذا الاتجاه القانوني محل نظر؛ لأنه بذلك يتيح الفرصة لجهة المصادقة الرقمية للتملص من مسؤوليتها بكل سهولة بمجرد أن تنفي وقوع ثمة إهمال وقع من جانبها، وأنها بذلت العناية المعتادة اللازمة واتخذت الاحتياطات الكافية للتأكد من صحة البيانات المقدمة إليها خاصة وأن ما يتوافر لدى جهة المصادقة الرقمية من إمكانيات مادية وموارد بشرية كفيل بأن تساعدها بكافة الوسائل على نفي أي إهمال قد ينسب إليها.

الفرع الثاني

الالتزام بإصدار وتسليم وحفظ شهادة التصديق الرقمي

بعد تحقق جهة المصادقة الرقمية من هوية شخص المُوقَع، فإنه يقع على عاتقها التزام بإصدار وتسليم شهادة تصديق رقمي لصاحبها، وتفيد هذه الشهادة بالتصديق على التوقيع الإلكتروني، في تعامل إلكتروني معين، تشهد بموجبها جهة المصادقة بصحة التوقيع ونسبته إلى من صدر عنه، حيث إن الهدف من لجوء الأشخاص إلى جهات المصادقة الرقمية هو إضفاء الثقة والأمان على تواقيعهم؛ لحث الغير على التعامل معهم بعد التحقق من هويتهم الشخصية.

وعن طبيعة هذا الالتزام فإنه يعتبر التزامًا بتحقيق نتيجة فلا يقتصر على بذل العناية، وتتمثل هذه النتيجة في صدور وتسليم شهادة تصديق رقمي مستوفية كافة البيانات الأساسية التي يحددها النظام.

لذا فإنه حينما تمتنع جهة المصادقة عن إصدار وتسليم شهادة التصديق الرقمي بدون عذر، فإن ذلك سيصيب طالب الشهادة بالضرر على اعتبار أن هذه الشهادة هي قوام التوقيع الإلكتروني وسبب تعويل الغير واعتماده عليه،

وبالتالي فإن هذا الامتناع سوف يجرد التوقيع الإلكتروني من كل قيمة نظامية له (Parisienne ,1996, p.113).

وفي هذا الصدد نصت الفقرتان(2و7) من المادة (18) من نظام التعاملات الإلكترونية السعودي على أنه «يجب على مقدم خدمات التصديق الالتزام بما يأتي: ٢-إصدار شهادات التصديق الرقمي وتسليمها، وحفظها، وفقا للترخيص الصادر له من الهيئة والضوابط والإجراءات التي تحددها اللائحة...

7-إصدار الشهادات متضمنة البيانات الموضحة في اللائحة، ومطابقة لشروط أمن الأنظمة وحمايتها، وقواعد شهادة التصديق الرقمي التي يضعها المركز».

كما تلتزم جهة المصادقة الرقمية بإنشاء قاعدة بيانات لشهادات التصديق الرقمية التي قامت بإصدارها، سواء كانت سارية الصلاحية، أو تم إيقافها، أو إلغائها، مع حفظ أي تعديل يطرأ عليها، وأيضاً تلتزم بتوفير الوسائل الإلكترونية التي تتيح لكل من يُعول على الشهادة في التعامل من الاطلاع على ما تتضمنه من بيانات باستمرار.

وفي ذلك نصت الفقرة (4) من المادة (١٨) من نظام التعاملات الإلكترونية السعودي على أنه «يجب على مقدم خدمات التصديق الالتزام بما يأتي: 4- إنشاء قاعدة بيانات الشهادات التي أصدرها، وحفظ تلك البيانات وما يطرأ عليها من تعديل، بما في ذلك الشهادات الموقوفة والملغاة. وأن يتيح الاطلاع إلكترونياً على تلك البيانات بصفة مستمرة».

ومن جهة أخرى نصت المادة (9/ ج) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية على أن مقدم خدمات التصديق «يُوفر وسائل يكون الوصول إليها متيسراً بقدر معقول، وتُمَكن الطرف المعتمد على الشهادة من التأكد منها، أو من سواها من الطريقة المستخدمة في تعيين هوية المُوقَع، ومن وجود أي تقييد على الغرض أو القيمة التي يجوز أن تستخدم من أجلها بيانات إنشاء التوقيع أو تستخدم من أجلها الشهادة، وأن بيانات إنشاء التوقيع صحيحة، ولم تتعرض لما يثير الشبهة، والتأكد من وجود أي تقييد على نطاق أو مدى المسؤولية التي اشترطها مقدم خدمات التصديق، وما إذا كانت هناك وسائل متاحة للموقع لتقديم إشعار بمقتضى الفقرة (1) من المادة (8) من هذا القانون، وما إذا كانت تتاح خدمة إلغاء آلية».

ويعد هذا الالتزام بحسب الفقه الفرنسي من أهم وظائف والتزامات جهة المصادقة الرقمية على اعتبار «أن الشهادة تنشئ علاقة بين هوية المُوقَع والمعطيات المستخدمة من أجل التحقق من سلامة التوقيع» (Didier ,2001, p.19).

الفرع الثالث

الالتزام بالحفاظ على سرية بيانات التصديق

يعتبر الالتزام بالحفاظ على سرية بيانات التصديق من أشد الالتزامات الملقاة على جهات المصادقة الرقمية؛ لأنه يعد بمثابة ضمانة تدعم ثقة المتعاملين في التعاملات الإلكترونية، حيث أن التعاملات الإلكترونية قد تتم في أغلب الأحيان بين أشخاص لا توجد بينهم معرفة سابقة ولم يلتقوا من قبل في الواقع المادي (An-gle ,1999, p.2) وبالتالي فإن عدم توافر هذه الضمانة سيؤدي إلى إعراض الأشخاص عن إبرام عقودهم، وإتمام تعاملاتهم عبر الوسائل الإلكترونية.

والالتزام بالحفاظ على سرية يشمل كافة البيانات التي تقدم لجهات المصادقة الرقمية سواء أكانت بيانات شخصية تتعلق بطالبي شهادات التصديق الرقمي أو بيانات تتعلق بالعقود التجارية التي يُبرمها هؤلاء ويطلبون شهادات التصديق لإثبات صحة رسائلهم وتواقيعهم الإلكترونية وحظر إفشاء سرية هذه البيانات يشمل جهات المصادقة الرقمية والعاملين بها طالما أنهم حصلوا على هذه البيانات أثناء عملهم أو بسببه، فلا يجوز لهم إفشاؤها ما لم يحصل على موافقة صاحب الشهادة الخطية أو الإلكترونية أو بقوة النظام، كما لو صدر حكم قضائي بإفشاء بيانات العميل.

وبالرجوع إلى المنظم السعودي نجد أنه ألزم جهات المصادقة الرقمية بالمحافظة على سرية البيانات بموجب الفقرة (5) من المادة (١٨) من نظام التعاملات الإلكترونية والتي تنص على أنه « يجب على مقدم خدمات التصديق الالتزام بما يأتي: ... محافظته -ومن يتبعه من العاملين على سرية المعلومات التي حصل عليها بسبب نشاطه، باستثناء المعلومات التي سمح صاحب الشهادة -كتابياً أو إلكترونياً-بنشرها أو الإعلام بها، أو في الحالات المنصوص عليها نظاماً». وحسبما هو مبين من النص السابق يعد التزام جهة المصادقة الرقمية بالمحافظة على سرية البيانات المقدمة على هذا النحو هو التزام ببذل عناية، وليس التزام بتحقيق نتيجة، وهذا يعني أنه لا تنعقد مسؤولية جهة المصادقة الرقمية عن الإخلال بهذا الالتزام إلا في حالة وقوع خطأ من أحد العاملين التابعين لها. ولهذا يهيب الباحث بالقضاء السعودي التشدد في إمكانية قبول نفي الخطأ من جانب جهة المصادقة الرقمية بغرض التملص من المسؤولية ومن جهة أخرى ألزم المشرع الأوروبي في المادة (٨/ ٢) من التوجيه الصادر بشأن التوقيعات الإلكترونية جهات المصادقة الرقمية بالحفاظ على سرية البيانات الشخصية للعملاء بحيث لا يمكن إفشاء هذه البيانات لشخص آخر غير صاحبها، أو برضا الأخير صراحة، ومتى

كانت هذه البيانات ضرورية لإصدار شهادة التصديق الرقمي وإن كان المشرع الأوروبي لم يحدد نوعية البيانات التي يحظر إفشاؤها، فإن الباحث يرى أنها تشمل كل البيانات التي تتعلق بتحديد الهوية الشخصية لصاحب شهادة التصديق.

الفرع الرابع

الالتزام بإلغاء أو إيقاف شهادة التصديق

من الالتزامات الرئيسية التي تقع على عاتق جهات المصادقة الرقمية هو إلغاء شهادة التصديق الرقمي عند وجود سبب يحتم ذلك، أو إيقاف شهادة التصديق أي يجعلها -بشكل مؤقت-كأن لم تكن، حتى يتحدد مصيرها سواء بإلغاء العمل بها أو استئناف سريانها في حال ثبوت عدم صحة السبب الذي أدى إلى تعليق هذه الشهادة (حجازي،2005، ص: 174).

ولما كان الإخلال بهذا الالتزام قد تترتب عليه أضرار جسيمة، كإبرام صفقات تجارية مشبوهة، أو سحب، أو إيداع، أو تحويل أموال، أو صدور أوامر بالشراء، أو البيع لسلع، أو منتجات بناء على شهادات تصديق مزيفة أو غير صحيحة.

ولذلك نص نظام التعاملات الإلكترونية السعودي في المادة (٢١) منه على الحالات التي يتعين فيها على جهات المصادقة الرقمية إلغاء أو إيقاف شهادة التصديق، فجاء فيها «يجب على مقدم خدمات التصديق إلغاء الشهادة أو إيقاف العمل بها عند طلب صاحبها ذلك، أو في الحالات التي تحددها اللائحة كما يجب عليه إبلاغ صاحب الشهادة فوراً بالإلغاء أو بالإيقاف وسبب ذلك، ورفع أي منها فوراً إذا انتفى السبب، ويكون مقدم خدمات التصديق مسؤولاً عن الضرر الذي يحدث لأي شخص حسن النية، نتيجة لعدم وقف العمل بالشهادة أو إلغائها».

ومن حالات إلغاء الشهادة أو إيقاف شهادة التصديق التي حددتها اللائحة التنفيذية لنظام التعاملات الإلكترونية السعودي في المادة (٢٣) منها حالة طلب صاحب الشهادة ذلك، أو بناء على أمر من هيئة الاتصالات وتقنية المعلومات، أو غيرها من الجهات ذات الاختصاص.

بالمقابل نجد أن التوجيه الأوروبي بشأن التوقيعات الإلكترونية لم يشر إلى التزام جهات المصادقة الرقمية بإلغاء أو إيقاف شهادة التصديق الرقمي عند وجود سبب يبرر ذلك. وعليه فإنه إذا توافرت أي حالة منها يتم إلغاء أو إيقاف العمل بالشهادة، ويتبين من ذلك أن التزام جهة المصادقة الرقمية بإلغاء أو إيقاف العمل بشهادة التصديق هو التزام بتحقيق نتيجة، بمعنى أن مسؤولية جهة المصادقة الرقمية تنعقد إذا لم تقم بإلغاء الشهادة أو إيقاف العمل بها متى وجد مبرر يدعو لذلك.

المبحث الثاني

صور المسؤولية النظامية لجهات المصادقة الرقمية

نظرًا لأهمية المصادقة الرقمية على التعاملات الإلكترونية، وما يترتب عليها من آثار نظامية في حق من قام بها وفي حق الغير، لذلك كان من الضروري تحديد صور المسؤولية التي قد تقع على عاتق جهات المصادقة الرقمية نتيجة مخالفة أحكام المصادقة على التعاملات الإلكترونية، ولهذا سيتم تناول هذا في المطلب الأول المسؤولية المدنية لجهات المصادقة الرقمية، ونخصص المطلب الثاني للمسؤولية الجزائية لجهات المصادقة الرقمية.

المطلب الأول

المسؤولية المدنية لجهات المصادقة الرقمية

تعد جهات المصادقة الرقمية مسؤولة عن صحة البيانات التي تضعها في شهادة التصديق الرقمي، وكذلك صحة التوقيع الوارد فيها بحيث يمكن الاعتماد على هذه الشهادة من قبل الغير للدخول في علاقة تعاقدية مع صاحب التوقيع، لذلك تتحرى هذه الجهات عن البيانات التي تتضمنها الشهادة قبل إصدارها، ولكن في بعض الأحيان قد يتبين أن المعلومات الواردة في هذه الشهادة غير صحيحة، مما يترتب عليه إلحاق أضرار بالغير، مما يثير التساؤل حول طبيعة التزام جهات المصادقة الرقمية (الفرع الأول)، والتكييف القانوني الأنسب للمسؤولية المدنية لجهات المصادقة الرقمية (الفرع الثاني).

الفرع الأول

طبيعة التزام جهات المصادقة الرقمية

إن تحديد مسؤولية جهة المصادقة الرقمية يتطلب الوقوف على حدود مسؤولية جهة المصادقة الرقمية، وأن نبين طبيعة التزامها، هل هو التزام بتحقيق نتيجة أم مجرد التزام ببذل عناية؟ لقد اختلفت آراء الفقهاء بخصوص طبيعة التزام جهة المصادقة الرقمية فقد ذهب رأي إلى أن تحديد طبيعة التزام جهة المصادقة الرقمية يتوقف على الأسلوب الذي صيغ به التزام جهة المصادقة الرقمية في العقد مشيراً إلى أنه إذا كان العقد يلزم جهة المصادقة بضمان صحة البيانات التي تتضمنها الشهادة، فإنها بذلك تلتزم بتحقيق نتيجة بعينها، وبالتالي تتحقق مسؤوليتها العقدية بمجرد إثبات المضرور عدم صحة البيانات المصدقة التي تتضمنها الشهادة. ولكن إذا كان الأسلوب الذي صيغ به التزام جهة المصادقة الرقمية في العقد يحملها بمجرد بذل العناية المعقولة للتحقق من صحة البيانات التي تتضمنها الشهادة، أي أنها تتحمل التزاماً ببذل عناية، ففي هذه الحالة يقع على عاتق المضرور عبء إثبات الإخلال أي إثبات الخطأ العقدي. وإلا فلن تنعقد مسؤولية جهة المصادقة الرقمية (التميمي،2012، ص: 213).

وذهب رأي آخر إلى أن تحديد طبيعة التزام جهة المصادقة الرقمية يتوقف على طبيعة عقدها المبرم مع صاحب الشهادة. حيث يرى أن عقد التصديق الرقمي هو بمثابة عقد مقاولة، وقد خلص هذا الرأي إلى أن الالتزام الملقى على عاتق جهة المصادقة الرقمية يعد التزامًا ببذل عناية وبصرف النظر عن مقدار العناية المطلوبة، سواء أكانت عناية الشخص المعتاد أم كانت عناية الشخص المحترف؟ (منصور،2008، ص: 129).

ويعتقد الباحث أنه لا يصح القول -كما ذهب الرأي الأول-بأن طبيعة الالتزام تتوقف على الأسلوب الذي صيغ به العقد، فطبيعة الالتزام تتوقف على ماهية الالتزام ذاته وكذلك طبيعة المصلحة المراد حمايتها.

كما لا يجوز القول بأن كافة الالتزامات الناشئة عن عقد التصديق الرقمي تعد من قبيل الالتزامات ببذل عناية -كما ذهب الرأي الثاني- فعقد التصديق تترتب عليه التزامات بتحقيق نتيجة معينة كالالتزام بإيقاف أو إلغاء شهادة التصديق عند توافر حالة من حالات الوقف أو الإلغاء.

وبالنظر إلى عقد التصديق الرقمي يمكن القول بأن التزام جهة المصادقة الرقمية بإيقاف أو إلغاء الشهادة هو التزام بتحقيق نتيجة بحسب طبيعته ولا يتصور أن يكون غير ذلك وعليه فإن تحديد طبيعة التزام جهة المصادقة الرقمية يتطلب في واقع الأمر الرجوع إلى مضمون العقد وأيضا المصلحة التي يسعى طرفاه إلى تحقيقها من خلاله، كما أنه بالرجوع إلى نظام التعاملات الإلكترونية السعودي نجد أنه لم يتخذ منهجاً محدداً من أجل تحديد طبيعة التزام جهة المصادقة الرقمية، لذا يرى الباحث أنه يجب تحديد طبيعة التزامات جهات المصادقة الرقمية بشكل دقيق من خلال بنود العقود التي تبرمها مع عملائها.

بينما نص قانون المعاملات والتجارة الإلكترونية لإمارة دبي في الفقرة (1/ب) من المادة (24) على أنه «أن يمارس عناية معقولة لضمان دقة واكتمال كل ما يقدمه من بيانات جوهرية ذات صلة بالشهادة أو مدرجة فيها طيلة سريانها».

واستناداً إلى هذه المادة يمكن القول أن ماهية الالتزام المفروض على جهة المصادقة الرقمية بضمان دقة البيانات التي تتضمنها الشهادة هي التزام ببذل العناية المعقولة للتحقق من صحة البيانات، وهذا الالتزام لا يخرج عن كونه التزامًا ببذل عناية، وبالتالي فإن مسؤولية جهة المصادقة الرقمية لا تقوم إلا في حالة إثبات إهماله في ممارسة عناية معقولة لضمان دقة البيانات، وهذا الالتزام على خلاف الالتزام بتحقيق نتيجة حيث يجب على المضرور الذي اعتمد على صحة شهادة التصديق الرقمي

الصادرة من جهة المصادقة الرقمية أن يقوم بإثبات الضرر الذي لحق به بسبب هذه الشهادة، وإلا فإن مسؤولية جهة المصادقة لا تنعقد، أي أن الاعتماد على ما تضمنته المادة السابقة يؤدي إلى القول أن مسؤولية جهة المصادقة الرقمية هي مسؤولية تقصيرية وليست تعاقدية، إذا لا يوجد أي عقد بين الغير المضرور الذي اعتمد على الشهادة وبين جهة المصادقة الرقمية، وبالتالي يجب إثبات الخطأ والضرر الواقع لانعقاد مسؤولية جهة المصادقة واستحقاق المضرور للتعويض.

وأياً كان الأمر فإن الباحث يرى أن التزام جهة المصادقة الرقمية هو التزام ذو طبيعة مزدوجة، حيث يمكن أن يكون التزامها هو التزام بتحقيق نتيجة وذلك فيما يتعلق بإصدار الشهادة حين طلبها من الشخص الذي اعتمد عليها، ويكون التزاماً ببذل عناية في التحقق من مضمون شهادة التصديق وبياناتها.

الفرع الثاني

التكييف القانوني لمسؤولية جهات المصادقة الرقمية المدنية

يعد التكييف القانوني لأي وضع من أدق وأصعب المشاكل التي تجابه رجال القانون كافة قضاة وفقهاء؛ لأنه ينبغي توضيح طبيعته للوقوف على مفهومه وتحديد أساسه لرسم ملامحه، وعلى هدى هذا التكييف يتوقف تحديد الأحكام التي سوف تطبق على التصرفات والأوضاع والمعطيات القانونية المعروضة.

ولبيان التكييف القانوني لمسؤولية جهات المصادقة الرقمية المدنية لابد من دراسة طبيعة هذه المسؤولية التي تقتضي الوقوف على ماهيتها وإعطائها وصفها الحقيقي.

فمن المتصور أن ترتكب جهة المصادقة الرقمية أخطاء حال إخلالها بأحد التزاماتها الناشئة عن النظام أو عقد التصديق الرقمي، وهنا يثور التساؤل حول أحكام المسؤولية التي تحاسب على ضوئها: هل هي المسؤولية العقدية (الغصن الأول) أم التقصيرية (الغصن الثاني)؟

الغصن الأول

المسؤولية العقدية لجهات المصادقة الرقمية

تثور المسؤولية العقدية لجهة المصادقة الرقمية التي ترتبط مع المُوقَع بعقد يتم بموجبه منحه شهادة التصديق الرقمي، وبالتالي يحق لصاحب الشهادة تحريك المسؤولية العقدية في حالة عدول جهة المصادقة عن تنفيذ التزاماتها المبينة في العقد، أو تأخرها في تنفيذها، أو تنفيذها بشكل معيب، أو غير صحيح. ووفقا لنظام التعاملات الإلكترونية السعودي تقوم المسؤولية العقدية لجهات المصادقة الرقمية في الحالات التالية:

١-إخلال جهات المصادقة الرقمية بالضمانات المنصوص عليها في المادة (٢٠) من نظام

التعاملات الإلكترونية، وتتمثل هذه الضمانات في:

أ-ضمان صحة المعلومات المصادق عليها التي تضمنتها شهادة التصديق الرقمي من وقت تسليمها .

ب-ضمان صحة العلاقة بين صاحب الشهادة وبياناتها الإلكترونية.

2-إخلال جهات المصادقة الرقمية بتعليق أو إلغاء شهادة التصديق الرقمي متى توافرت الأسباب الموجبة لهما وفقًا للمادة (٢١) من نفس النظام.

ويستتبع ذلك مسؤولية جهات المصادقة الرقمية عن تعويض الضرر الناشئ عن إخلالها بهذه الالتزامات، وإذا كانت المسؤولية العقدية تثار بصدد العلاقة بين جهة المصادقة الرقمية وصاحب شهادة التصديق، فهنا يثور التساؤل حول ماهية التكييف النظامي للعقد المبرم بين صاحب الشهادة وجهة المصادقة الرقمية: هل يعد عقد بيع سلعة ما أم يعد عقد تقديم خدمة؟ وفي هذا ذهب اتجاه إلى أن عملية إصدار شهادات التصديق الرقمي تعد بمثابة عقد بيع سلعة ما من جانب جهة المصادقة الرقمية (البائع) إلى العميل (المشتري) باعتباره شخصًا ما من أصحاب التواقيع الإلكترونية المعولين عليه (أبو الليل،2002، ص:190).

بينما ذهب اتجاه آخر إلى أن هذا العقد يعد عقد تقديم خدمة؛ لأن ما تقدمه جهة المصادقة للعميل أو للغير من خدمات المصادقة الرقمية من شأنها أن تدعم مصداقية الشهادات التي تصدرها جهة المصادقة، والبيانات التي تتضمنها الشهادات، وبالأخص التواقيع الإلكترونية وتوثيقها. كل هذا يحد من المخاطر المحتملة التي قد تنجم عن نظم الدفع الرقمي (Anne ,2002, p.2060).

بينما يرى الباحث أن العقد المبرم بين صاحب الشهادة وجهة المصادقة الرقمية هو عقد مقاولة حيث إن جهة المصادقة الرقمية تقوم بعمل معين يتمثل مضمونه في إنجاز عمل محدد وهو تصديقها على التوقيع الإلكتروني للعميل (صاحب الشهادة) وذلك عبر إصدار شهادة التصديق الرقمي، وتلتزم الجهة المصادقة بهذا العمل من أجل إشباع رغبة العميل في تأكيد هويته وصحة ونسبة التوقيع الإلكتروني إليه لقاء أجر يلتزم به العميل (صاحب الشهادة).

وإذا كانت المسؤولية العقدية لجهة المصادقة الرقمية تثور في مجال العلاقة بينها وبين صاحب شهادة التصديق نظراً لوجود عقد بينهما، فإنه يمكن تصور المسؤولية العقدية كذلك في إطار العلاقة بين جهة المصادقة والغير الذي اعتمد على شهادة التصديق الرقمي. إذ قد يتضرر الغير من إصدار مثل هذه الشهادة التي تتضمن بيانات غير صحيحة، فمجرد طلب الغير للشهادة يعني أنه يُعول

عليها في اتخاذ قراره بالتعامل مع صاحبها.

كما يمكن أن تثور المسؤولية العقدية لجهة المصادقة الرقمية عندما تكون هناك رابطة مباشرة بينها وبين الغير، كما في حالة تلقي الغير لشهادة التصديق الرقمي والمفتاح العام من جهة المصادقة الرقمية نفسها من خلال اتصاله بها مباشرة أو عبر موقعها الإلكتروني على شبكة الإنترنت.

وأيضاً يمكن أن تثار المسؤولية العقدية لجهة المصادقة الرقمية قبل الغير، وذلك في حالة تضمن عقد التصديق المبرم بين جهة المصادقة الرقمية وصاحب شهادة التصديق الرقمي اشتراطًا لمصلحة الغير، ويحدث ذلك عندما يشترط صاحب الشهادة في عقد التصديق أن تضمن جهة المصادقة تجاه الغير الأضرار التي قد تصيب الأخير نتيجة اعتماده أو تعويله على صحة البيانات المصدقة التي تضمنتها شهادة التصديق، وعندئذ ينشئ عقد التصديق التزامًا قانونيًّا في مواجهة جهة المصادقة لصالح الغير تتحمله جهة المصادقة استناداً للقواعد العامة في الاشتراط لمصلحة الغير (أبو الليل،2003، ص: 1887).

وبهذا نلاحظ أن المسؤولية العقدية لجهة المصادقة تقوم على أساس تعاقدي، ولكي تقام هذه المسؤولية لابد من توافر عناصر ثلاثة، وهي: الخطأ والضرر وعلاقة السببية بينهما.

أولاً-الخطأ العقدي:

يتحقق الخطأ العقدي لجهة المصادقة الرقمية في حالة إخلالها بأحد التزاماتها الناشئة عن عقد التصديق الرقمي، وتبعاً لذلك فإن الإخلال بهذه الالتزامات يؤدي إلى قيام المسؤولية العقدية لجهة المصادقة، مع تحملها عبء التعويض عن الأضرار الناجمة عن هذا الإخلال.

كما أن الأصل في المسؤولية العقدية لجهة المصادقة الرقمية هو افتراض وقوع الخطأ من جانبها في حال إخلالها بتنفيذ التزاماتها في مجملها أو في جزء منها، أو تأخرها في تنفيذها، ولا يمكنها نفي افتراض الخطأ من جانبها إلا إذا أثبتت أن عدم التنفيذ أو التأخير فيه ناشئ عن سبب أجنبي لا دخل لها فيه، كأن تثبت جهة المصادقة الرقمية أن عدم تنفيذ التزامها بضمان صحة البيانات المصدقة التي تتضمنها الشهادة سببه فعل صاحب الشهادة نفسه نتيجة تقديمه لأوراق مزورة أو وهمية، أو أن عدم إصدارها لشهادة تصديق في الوقت المتفق عليه راجع إلى تأخر صاحب الشهادة في تسليم المعلومات المتعلقة بهويته الشخصية، أو إذا كان قيام جهة المصادقة الرقمية بإفشاء أي من المعلومات المتعلقة بصاحب الشهادة قد تم بناء على إذن منه أو في الحالات التي يسمح بها النظام.

ومن جهة أخرى فإنه على الرغم من تحقق المسؤولية العقدية لجهة المصادقة الرقمية

بثبوت خطئها العقدي إلا أنه يجوز الاتفاق على تقييد أو تخفيف هذه المسؤولية أو حتى إسقاطها، وذلك بأن يتم الاتفاق في العقد على تقييد أو تخفيف مسؤولية جهة المصادقة الرقمية بحيث تنعقد مسؤوليتها فقط عن خطئها الجسيم دون اليسير، كما يمكن لها أن تشترط في العقد إعفاءها من المسؤولية عن الخطأ الجسيم والغش الصادر من أحد التابعين لها. وهو ما نصت عليه الفقرة (5/أ) من المادة (24) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي من أنه «لا يكون مزود خدمات التصديق مسئولاً عن أي ضرر (أ): إذا أدرج في الشهادة بياناً يقيد نطاق ومدى مسئوليته تجاه أي شخص ذي صلة، ومدى ذلك القيد».

ثانياً-الضرر العقدي:

يعد الضرر العقدي الركن الثاني في المسؤولية العقدية، لذا يجب لقيام المسؤولية العقدية لجهة المصادقة الرقمية أن يترتب على إخلالها بأحد التزاماتها المفروضة عليها بموجب عقد التصديق الرقمي حدوث ضرر، كما هو الحال بالنسبة للضرر الناتج عن عدم تنفيذ جهة المصادقة الرقمية لالتزامها أو التأخير في تنفيذه أو تنفيذ الالتزام بشكل معيب، فإذا توافر سبب يحتم إيقاف أو إلغاء الشهادة ولم تقم جهة المصادقة الرقمية بهذا الإيقاف أو الإلغاء تكون قد أخلت بالتزام مفروض عليها، ولكي تتم مساءلتها وفقا لأحكام المسؤولية العقدية يجب أن يصيب صاحب الشهادة ضرر نتيجة عدم إيقاف أو إلغاء الشهادة، وهنا يكون ركن الضرر قد تحقق مما يترتب عليه قيام المسؤولية العقدية في مواجهة جهة المصادقة لتعويض صاحب الشهادة عن الضرر الذي أصابه.

والضرر قد يكون مادياً يصيب صاحب الشهادة في مصلحة مالية أو يكون ضرراً معنوياً يمس شرف واعتباره، كما يشترط أن يكون الضرر مباشراً متوقع الحدوث ومحققاً أي وقع بالفعل، إما إذا كان مستقبلاً فلابد أن يكون محقق الوقوع لرفع دعوى للمطالبة بالتعويض عنه، ولكن إذا كان الضرر المستقبلي محتمل الوقوع فلا يصلح أن يكون أساساً لطلب التعويض (كيسي،2012، ص: 12). وعلى العموم لا يوجد نص نظامي يحدد على وجه الدقة أنواع الضرر العقدي الموجب لمسؤولية جهات المصادقة الرقمية التعاقدية، كما لا يوجد تحديد معين للأفعال الضارة التي تقع نتيجة للخطأ العقدي الذي يتحقق في حالة إخلال تلك الجهات بأحد التزاماتها التعاقدية، وبالتالي فإن هذا الأمر متروك للسلطة التقديرية لقاضي الموضوع.

ويقع على عاتق صاحب الشهادة المضرور من جراء إخلال جهة المصادقة بأحد التزاماتها العقدية عبء إثبات الضرر العقدي، فلا يكفي إثبات عدم تنفيذ جهة المصادقة الرقمية

لالتزامها لافتراض وقوع هذا الضرر، لأنه من المتصور أن تخل جهة المصادقة بأحد التزاماتها ولا يترتب على هذا الإخلال حدوث أي ضرر.

ثالثاً-رابطة السببية بين الخطأ والضرر:

يشترط لقيام المسؤولية العقدية لجهة المصادقة الرقمية أن يكون خطؤها هو السبب في الضرر الواقع، أي أن تكون هناك رابطة سببية بينهما، بمعنى أنه لابد لتعويض صاحب الشهادة عن الضرر الذي لحق به أن يكون هذا الضرر قد وقع بسبب خطأ جهة المصادقة الرقمية والمتمثل في إخلالها بإحدى التزاماتها العقدية، كما في حالة امتناع جهة المصادقة الرقمية عن إصدار شهادة التصديق المطلوبة أو إصدار شهادة معيبة أو التأخر في إصدارها مما يؤدي إلى ضياع وقت طالب الشهادة على نحو يعرضه لمخاطر عدة، منها تفويت فرصة التعاقد الإلكتروني على صفقة رابحة كان قد حصل على وعد بهذا التعاقد خلال فترة عرض محددة مما يؤدي لتعرضه لخسائر مادية جسيمة (Didier) (Pierre ,2006,p.37 ,2020,p.11). كما قد تتسبب جهة المصادقة الرقمية في وقوع ضرر لطالب الشهادة العميل في حال كون جهة المصادقة من أصحاب العلامات التجارية المشهورة عالمياً مما يضفي على شهادة التصديق الرقمي قدراً كبيراً من المصداقية والأمان، ويجعل من امتناع جهة المصادقة عن إصدار تلك الشهادة أو التأخر في إصدارها سببا في حرمان طالب الشهادة من تلك الميزة (Thomas ,2000, p.20) (Antoine ,2020, p.15). أما إذا كان الضرر اللاحق بصاحب الشهادة راجع لسبب آخر لا علاقة له بإخلال جهة المصادقة الرقمية بأحد التزاماتها الناشئة عن العقد فإنه تنتفي معه رابطة السببية وبالتالي لا تنعقد المسؤولية العقدية لجهة المصادقة الرقمية، كما إذا تبين أن الضرر الذي أصاب صاحب شهادة التصديق لم يكن مرده إصدار جهة المصادقة الرقمية لشهادة معيبة وإنما بسبب راجع إلى إفشاء صاحب الشهادة لسر أحد الأنظمة المتعلقة بإنشاء توقيعه الإلكتروني بالمخالفة لما تضمنته الفقرة الأولى من المادة (٢٢) من نظام التعاملات الإلكترونية السعودي، والتي تنص على أنه «يعد صاحب الشهادة مسؤولاً عن سلامة منظومة التوقيع الإلكتروني الخاصة به وعن سريتها، ويعد صادراً منه كل استعمال لهذه المنظومة. وعليه التقيد بشروط استعمال شهادته، وشروط إنشاء توقيعه الإلكتروني».

ووفقاً لهذا النص لا يمكن نسبة الخطأ لجهة المصادقة طالما أنها قامت بالتزاماتها على أكمل وجه، ووفقاً للشروط والمعايير المقررة قانوناً.

أضف إلى ذلك أن رابطة السببية ما بين الخطأ

والضرر تعد مفترضة، فلا يكلف المضرور بإثباتها، بل إن جهة المصادقة الرقمية هي المكلفة بنفي هذه الرابطة إذا ادعت أنها غير قائمة، ولا يكون بمقدور جهة المصادقة الرقمية نفي رابطة السببية إلا بإثبات أن الضرر نشأ عن سبب أجنبي، أو قوة قاهرة، أو حادث فجائي، أو خطأ الغير، أو بسبب خطأ المضرور نفسه.

وفي هذا المعنى نصت الفقرة (5/ب) من المادة (24) من قانون المعاملات والتجارة الإلكترونية الإمارة دبي رقم 2 لسنة 2002، على أنه «لا يكون مزود خدمات التصديق مسئولاً عن أي ضرر(ب): إذا أثبت بأنه لم يقترف أي خطأ أو همال، أو أن الضرر نشأ عن سبب أجنبي لا يد له فيه».

الغصن الثاني

المسؤولية التقصيرية لجهات المصادقة الرقمية

يتطلب الوقوف على المسؤولية التقصيرية لجهات المصادقة الرقمية التعرف على ماهيتها وحالات انعقادها وعناصرها، على النحو التالي:

أولاً-ماهية المسؤولية التقصيرية:

المسؤولية التقصيرية لجهات المصادقة الرقمية تعني مسؤوليتها عن تعويض الأضرار التي قد تلحق بالغير الذي عول على البيانات الواردة في شهادة التصديق الرقمي وأخذها بعين الاعتبار عند تعامله الإلكتروني مع صاحب الشهادة، ثم يكتشف الغير فيما بعد عدم صحة هذه البيانات بسبب نقلها من قاعدة بيانات معيبة نشرتها جهة المصادقة أو يشوب البيانات التزييف والتزوير، كما هو منصوص عليه بالمادة (20) من نظام التعاملات الإلكترونية السعودي التي جاء فيها «يتحمل مقدم خدمات التصديق مسؤولية ضمان صحة المعلومات المصدقة التي تضمنتها الشهادة وقت تسليمها، وصحة العلاقة بين صاحب الشهادة وبياناتها الإلكترونية. وتقع مسؤولية الضرر الذي يحدث لأي شخص وثق-بحسن نية -بصحة ذلك».

ووفقاً لهذا النص فإن جهة المصادقة الرقمية تكون مسؤولة عن الأضرار التي تلحق بالغير في حالة إخلالها بالتزامها بالتحقق من صحة البيانات المصدقة التي تحتويها شهادة التصديق الرقمي في تاريخ تسليمها، وكذلك صحة الصلة بين صاحب الشهادة وبياناتها، أما إذا قامت جهة المصادقة الرقمية بالتزامها على أكمل وجه في التحقق من صحة البيانات، وصحة العلاقة بين صاحب الشهادة وبياناتها، واتضح فيما بعد أن البيانات المقدمة لها مزورة، هنا لا تكون جهة المصادقة الرقمية مسؤولة عن التعويض عن الأضرار الناتجة عن هذا التزوير، حيث إن التزامها بالتحقق من صحة البيانات هو التزام ببذل عناية وليس بتحقيق نتيجة معينة.

ثانياً-حالات انعقاد المسؤولية التقصيرية:

تنعقد المسؤولية التقصيرية لجهة المصادقة

الرقمية قبل الغير الذي أصابه ضرر ناتج عن إخلالها بالتزامها بإلغاء شهادة التصديق الرقمي أو تعليق العمل بها في الحالات الموجبة لذلك وفقاً للمادة (21) من نظام التعاملات الإلكترونية السعودي، وبالتالي تكون جهة المصادقة الرقمية مسؤولة عن تعويض الغير عن هذا الضرر، ولكن إذا كان الإلغاء أو التعليق بناء على طلب صاحب الشهادة وترتب عليه حدوث ضرر للغير، فإن صاحب الشهادة يصبح هو المسؤول عن تعويض هذا الضرر وليس جهة المصادقة.

وبناء على ما تقدم فإنه يحق للغير الذي أصيب بضرر نتيجة لاعتماده في تعامله الإلكتروني على صحة الشهادة، ولا تربطه بجهة المصادقة أي علاقة تعاقدية، أن يعود وفقاً لقواعد المسؤولية التقصيرية على جهة المصادقة لمطالبتها بتعويض الضرر الناشئ عن إخلالها بالتزاماتها؛ استناداً في ذلك لما نصت عليه المادة (٢٧) من نظام التعاملات الإلكترونية السعودي، من أنه «يحتفظ الشخص الذي لحقه ضرر ناتج من المخالفات المنصوص عليها في هذا النظام، أو عدم التقيد بأي من الضوابط والالتزامات الواردة فيه بحقه في رفع دعوى أمام الجهة القضائية المختصة بطلب تعويضه عن الأضرار التي لحقت به».

كما نظم قانون المعاملات والتجارة الإلكترونية لإمارة دبي في الفقرة (4/ب) من المادة (24) منه، المسؤولية التقصيرية الجهات المصادقة الرقمية في مواجهة الغير الذي اعتمد على شهادة التصديق بصورة معقولة (حجازي،2002، ص: 314). وتقوم هذه المسؤولية في مواجهة أي شخص اعتمد بصورة معقولة على الشهادة التي أصدرتها جهة التصديق إذ تنص على أنه «إذا حدثت أية أضرار نتيجة لعدم صحة الشهادة أو نتيجة لأي عيب فيها، يكون مزود خدمات التصديق مسئولا عن الخسائر التي يتكبدها (ب) إذا اثبت بأنه لم يقترف أي خطأ أو اهمال، أو أن الضرر نشأ عن سبب أجنبي لا بد له فيه».

ويتبين من ذلك أنه إذا كان اعتماد الغير على التوقيع الإلكتروني وشهادة التصديق قد تم بصورة معقولة، فإنه تقام مسؤولية جهة المصادقة عن الضرر الذي لحق بالغير، أما إذا كان اعتماد الغير بصورة غير معقولة في ظل الظروف التي تحيط بطبيعة التعامل الإلكتروني مع صاحب الشهادة فإن الغير الذي اعتمد على التوقيع الإلكتروني وشهادة التصديق يتحمل مخاطر عدم صحتهما، وتلك هي الاعتبارات التي بتوافرها يعتبر الاعتماد على التوقيع وشهادة التصديق الرقمي معقولاً، وبالتالي تقوم مسؤولية جهة المصادقة إذا ألحقت ضرر بالغير الذي اعتمد بصورة معقولة على الشهادة، أما إذا كان اعتماده غير معقول في الظروف المحيطة بطبيعة التعامل الإلكتروني مع صاحب الشهادة،

فإن الغير الذي اعتمد على الشهادة يتحمل مخاطر عدم صحتها.

وهنا يجب على الغير اتخاذ كافة الاحتياطات المعقولة واللازمة قبل الاعتماد على التوقيع الإلكتروني وشهادة التصديق الرقمي في تعامله الإلكتروني مع صاحب الشهادة (W. Harry ,2001, p.1).

ثالثاً-عناصر المسؤولية التقصيرية:

تنعقد المسؤولية التقصيرية لجهة المصادقة الرقمية متى توافرت عناصرها المتمثلة في الخطأ التقصيري والضرر ورابطة السببية بينهما، والخطأ التقصيري يعني الإخلال بالالتزام القانوني العام باحترام حقوق الغير وعدم الإضرار بهم، وهذا الالتزام بطبيعته هو التزام ببذل عناية تلتزم به جهة المصادقة لصالح الغير، ويعد الإخلال به نتيجة الإهمال أو التقصير خطأ يوجب مسؤوليتها، ويقع عبء إثبات ذلك على الغير المضرور، وذلك بأن يقيم الدليل على أن جهة المصادقة لم تبذل العناية المعتادة وفقا لمعيار موضوعي وهو معيار الشخص العادي، وإثبات ذلك ليس بالأمر اليسير، إذ سيواجه الغير العديد من الصعوبات لإثبات خطا جهة المصادقة فالأمر متعلق بإثبات عمل تقني دقيق، وقد لا يكون باستطاعة الغير القيام بذلك، حيث إنه بالنظر لما تتمتع به جهة المصادقة من إمكانيات تقنية ومالية وخبرة عملية، فإن لديها القدرة على إثبات قيامها ببذل العناية الكافية، واتخاذ كافة الإجراءات اللازمة للحيلولة دون وقوع أخطاء من جانبها، أو بأن الضرر واقع لا محالة مهما بذلت من عناية أي بسبب خارج عن إراداتها، وعلى افتراض مقدرة الغير على إثبات خطأ جهة المصادقة بإقامة الدليل على قصورها في بذل العناية المعتادة للتحقق من صحة البيانات المقدمة لها والمدرجة بشهادة التصديق، فعلى الغير المضرور أن يثبت أيضاً أن ما لحق به من ضرر كان محقق الوقوع وناجمًا عن الخطأ التقصيري لجهة المصادقة، وهو ما يجعل إمكانية تعويض المضرور ضربا من المستحيل (شرف الدين،2000، ص: 284). لذا يرى الباحث أن هذا يعد قصورًا في إطار الحماية المراد تقديمه للغير في مجال التعاملات الإلكترونية، ويجب إعفاء المضرور من إثبات الخطأ في جانب جهة المصادقة الرقمية.

هذا مع اعتبار أن مسؤولية جهة المصادقة قائمة على الخطأ المفترض، وذلك اتساقا مع القواعد العامة في المسؤولية المفترضة، وعلى جهة المصادقة نفي المسؤولية الكاملة عن الخطأ الذي نتج عنه الضرر، إذ يكفي وقوع الضرر بسبب تهاون جهة المصادقة أو قصورها المهني لتترتب مسؤوليتها التقصيرية، وبغض النظر عن نوع التزامها تجاه الغير.

كما يقترح الباحث فرض تأمين إجباري عن المسؤولية الناجمة عن أعمال جهات المصادقة الرقمية، إذ إنّ تأمين مسؤولية جهة المصادقة الرقمية من شأنه أن يحدد طبيعة هذه المسؤولية وحالات الإعفاء منها.

وفي هذا السياق وضعت الفقرة الثانية من المادة (6) من التوجيه الأوروبي بشأن التوقيعات الإلكترونية لسنة 1999م قرينة على مسؤولية جهات المصادقة الرقمية (التميمي،2011، ص: 83). حيث جاء في الفقرة سالفة الذكر «تسهر الدول الأعضاء على أن يكون المكلف بخدمة التوثيق الذي أصدر شهادة معتمدة للجمهور مسئولاً عن الضرر الذي يصيب الشخص الطبيعي أو المعنوي مستفيداً من الشهادة إلا إذا برهن على أنه لم يرتكب أي إهمال»، وهذه تعد قرينة مفترضة على مسؤولية جهة المصادقة التي أصدرت الشهادة في حالة وقوع إهمال منها يترتب عليه ضرر يصيب أي شخص اعتمد على شهادة التصديق بشكل معقول (أبو الليل،2002، ص: 1902).

وهنا يرى جانب من الفقه الفرنسي أنه لا يكفي قيام جهة المصادقة الرقمية بإثبات عدم خطئها لكي تدفع مسؤوليتها المفترضة عن الضرر، وإنما ينبغي أن تثبت كذلك أنها قد راعت أثناء قيامها بمهامها أصول وقواعد المهنة، أي: إن تنفيذها لمهامها كان مطابقاً لأفضل الأساليب المتعارف عليها وقت تقديم خدمة التصديق على الشهادة (أبو الليل،2002، ص: 223).

المطلب الثاني

المسؤولية الجزائية الجهات المصادقة الرقمية

فرضت معظم التشريعات على جهات المصادقة الرقمية التزامات محددة عند ممارستها لنشاطها، وفي سبيل احترامها وإكسابها طابع الإلزام والاجبار قامت بوضع عقوبات جزائية توقع على جهات المصادقة الرقمية في حالة مخالفة الالتزامات المفروضة عليها متى ما كانت هذه المخالفة تشكل جريمة جزائية، ولهذا فإن بيان المسؤولية الجزائية لجهات المصادقة الرقمية يتطلب استعراض نطاق المسؤولية الجزائية لجهات المصادقة الرقمية (الفرع الأول)، وأثر تحقق المسؤولية الجزائية لجهات المصادقة الرقمية (الفرع الثاني).

الفرع الأول

نطاق المسؤولية الجزائية لجهات المصادقة الرقمية

لما كانت هناك شروطاً معينة لابد من توافرها حتى يتسنى لجهات المصادقة الرقمية مزاولة نشاطها، فإنه في مقابل ذلك تُجرم التشريعات الأفعال التي تعد مخالفة لهذه الشروط، وذلك لضمان أمن واستقرار التعاملات الإلكترونية،

وفيما يلي توضيح لأهم المخالفات التي يمكن أن ترتكبها جهات المصادقة الرقمية أثناء ممارسة نشاط وتشكل في نفس الوقت جرائم جزائية يعاقب عليها النظام:

أولاً-ممارسة نشاط جهات المصادقة الرقمية بدون ترخيص:

لقد جرم المنظم السعودي هذا الفعل لما فيه من مخالفة للشروط الواجب توافرها بجهات المصادقة الرقمية لممارسة نشاطها، ولقيام هذه الجريمة لابد من توافر كل من الركن المادي والركن المعنوي على اعتبار أن ممارسة نشاط جهات المصادقة الرقمية بدون ترخيص هي من الجرائم الشكلية التي يتطلب قيامها توافر السلوك الإجرامي فقط.

1-الركن المادي:

يتمثل السلوك الإجرامي لهذا الفعل في أن الجاني ينتحل صفة مقدم خدمات المصادقة الرقمية (جهة المصادقة) مرخص له على خلاف الحقيقة، ويصدر شهادات تصديق رقمية بدون ترخيص بذلك من هيئة الاتصالات وتقنية المعلومات، كما أن الجاني يخالف حكماً صريحاً قررته الفقرة الأولى من المادة (٢٣) من نظام التعاملات الإلكترونية السعودي التي جاء فيها أنه «يعد مخالفة لأحكام هذا النظام... (١) ممارسة نشاط مقدم خدمات التصديق دون الحصول على ترخيص من الهيئة».

ويعود السبب في تجريم هذا الفعل إلى الأضرار التي قد تصيب الغير نتيجة لإصدار شهادة تصديق رقمي غير صحيحة حيث يكون مضمونها التسليم بصحة بيانات التعامل لإصدار تلك الشهادة عنه، ولا شك أن هذا السلوك يؤدي إلى إهدار الثقة الواجب توافرها في التعاملات الإلكترونية (أحمد،2011، ص: 131).

وتعد هذه الجريمة من جرائم الخطر أو جرائم السلوك المجرد حيث يتحقق الركن المادي فيها بمجرد ارتكاب الجاني للسلوك الإجرامي المتمثل في ممارسة نشاط جهات المصادقة الرقمية بدون ترخيص، وبدون تطلب حدوث ضرر للغير.

2-الركن المعنوي:

تعد هذه الجريمة من الجرائم العمدية؛ إذ يتطلب توافر القصد الجنائي العام بعنصريه العلم والإرادة وذلك بأن يعلم الجاني بأنه يمارس نشاط جهات المصادقة الرقمية بدون ترخيص، وأن تتجه إراداته إلى إتيان هذا السلوك الإجرامي، ويقبل النتائج المترتبة عليها.

ويلاحظ أن هذه الجريمة لا تقع عن طريق الخطأ لأن صياغة الفقرة الأولى من المادة (٢٣) من نظام التعاملات الإلكترونية السعودي قد بدأت بعبارة «ممارسة نشاط مقدم خدمات التصديق» بما يفيد التعمد أو انصراف الإرادة إلى إتيان هذا السلوك المخالف.

ثانياً-إساءة استغلال جهات المصادقة الرقمية لنشاطها:

اعتبر المنظم السعودي استعمال أو استغلال جهات المصادقة الرقمية للمعلومات الشخصية لصاحب شهادة التصديق الرقمي في مجال آخر غير خدمات المصادقة وإصدار الشهادة بدون موافقة كتابية أو إلكترونية من صاحب الشهادة، سلوكاً إجرامياً يعاقب عليه نظام التعاملات الإلكترونية، إذ نصت الفقرة الثانية من المادة (23) من هذا النظام على أنه «يعد مخالفة لأحكام هذا النظام... (2) استغلال مقدم خدمات التصديق المعلومات التي جمعها عن طالب الشهادة لأغراض أخرى خارج إطار أنشطة التصديق، دون موافقة كتابية أو إلكترونية من صاحبها».

ويتبين من النص السابق أن المنظم السعودي اشترط لقيام هذه الجريمة توافر صفة معينة في الجاني هي أن يكون مقدم خدمات التصديق (جهة المصادقة الرقمية) أو أحد العاملين التابعين له، كما اشترط توافر الركنين المادي والمعنوي.

1-الركن المادي:

يتحقق الركن المادي في هذه الجريمة بإتيان الجاني فعل إيجابي يتمثل في استغلال المعلومات المتعلقة بطالب الشهادة لأغراض أخرى غير أنشطة التصديق، دون الحصول على موافقة كتابية أو إلكترونية من صاحبها. والهدف من تجريم هذا الفعل هو لضمان سلامة استعمال المعلومات الشخصية المتعلقة بصاحب شهادة التصديق الرقمي (حجازي،2005، ص: 504).

2-الركن المعنوي:

لا تكتمل هذه الجريمة إلا بتوافر الركن المعنوي إلى جانب الركن المادي، وصورة الركن المعنوي فيها هي القصد الجنائي بنوعيه، القصد الجنائي العام والمتمثل في علم الجاني (جهة المصادقة الرقمية أو أحد العاملين التابعين لها) باستغلال المعلومات المتعلقة بطالب الشهادة لأغراض أخرى غير أنشطة التصديق الرقمي بدون موافقة من صاحبها، وأن من شأن فعله هذا إحداث الضرر بصاحبها، وأن هذا الفعل مخالف للنظام ومع ذلك يقبل القيام به.

أما القصد الجنائي الخاص فيتمثل في اتجاه نية الجاني إلى تحقيق نتيجة معينة وهي استغلال المعلومات المتعلقة بطالب الشهادة لأغراض أخرى غير أنشطة التصديق الرقمي.

ثالثاً-إفشاء جهات المصادقة الرقمية المعلومات المتعلقة بصاحب شهادة:

إن إفشاء جهات المصادقة الرقمية للمعلومات المتعلقة بصاحب شهادة التصديق، والتي لها سلطة الاطلاع عليها بحكم نشاطها أثناء تدوين أو معالجة هذه المعلومات، يعتبر

سلوكاً إجرامياً، ويشترط في المعلومات التي يتم إفشاؤها أن تتعلق بشخص صاحب شهادة التصديق، ويكون إفشاء تلك المعلومات من خلال إذاعتها أو اطلاع الغير عليها، وفي هذا الشأن نصت الفقرة الثانية من المادة (٢٣) من نظام التعاملات الإلكترونية السعودي على أنه «يعد مخالفة لأحكام هذا النظام... (٣) إفشاء مقدم خدمات التصديق المعلومات التي اطلع عليها بحكم عمله، ما لم يأذن له صاحب الشهادة - كتابياً أو إلكترونياً - بإفشائها، أو في الحالات التي يسمح له بذلك نظاماً».

ونجد أيضاً أن المشرع الإماراتي نص على هذه الجريمة في المادة (1/31) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي رقم ٢ لسنة ٢٠٠٢ التي جاء فيها «يعاقب كل شخص تُمَكن بموجب أية سلطة ممنوحة له في هذا القانون من الاطلاع على المعلومات في سجلات أو مستندات أو مراسلات إلكترونياً، وأفشى متعمداً أياً من هذه المعلومات، بالحبس وبغرامة لا تجاوز100,000درهم، أو بإحدى هاتين العقوبتين...».

يتضح من النصوص السابقة أن النموذج القانوني لهذه الجريمة اشترط إضافة إلى الركنين المادي والمعنوي توافر صفة الجاني ممثلاً في كل شخص يكون له بحكم عمله سلطة الاطلاع على المعلومات التي تتضمنها شهادة التصديق الرقمي، وتعد هذه الجريمة من الجرائم الشكلية التي يكفي لقيامها إتيان السلوك الإجرامي دون الحاجة إلى تحقيق نتيجة إجرامية. وعليه تعد هذه الجريمة من جرائم السلوك، وقيامها يتطلب توافر الركنين المادي والمعنوي:

1-الركن المادي:

يتضح أن الركن المادي لهذه الجريمة يتحقق بفعل إفشاء الجاني للمعلومات التي اطلع عليها بحكم عمله بدون إذن صاحب شهادة التصديق الرقمي، أو في الحالات التي يسمح بها النظام على أنه في أحوال أخرى ينتفي عن فعل الإفشاء صفة الجريمة، كما في حالة إذا كان إفشاء جهات المصادقة الرقمية لتلك المعلومات بناء على إذن كتابي أو إلكتروني من صاحب الشهادة، أو عند توافر إحدى الحالات التي يسمح فيها النظام بإفشاء معلومات صاحب الشهادة، كأن يتم الإفشاء بناء على ترخيص من إحدى الهيئات القضائية السعودية العلة من تجريم هذا الفعل إلى أن الإفشاء قد يلحق الضرر بصاحب الشهادة الرقمية، إذ يمكن للغير استغلالها بطريقة غير مشروعة ضد صاحب الشهادة كتهديده أو ابتزازه (حجازي،2005،ص: 507).

2-الركن المعنوي:

لما كانت هذه الجريمة من الجرائم العملية فإنه يتطلب توافر الركن المعنوي الذي يتخذ صورة القصد الجنائي العام بعنصريه العلم والإرادة.

وترتيباً على ذلك يجب أن يعلم الجاني (جهة المصادقة الرقمية أو أحد العاملين التابعين لها) بإفشاء المعلومات المتعلقة بصاحب شهادة التصديق بدون إذن كتابي أو إلكتروني منه، أو في الحالات التي يسمح له بذلك نظاماً.

رابعاً-تقديم جهات المصادقة الرقمية لبيانات كاذبة أو معلومات مضللة:

ألزم المنظم السعودي جهات المصادقة الرقمية بأن تقدم بيانات ومعلومات صحيحة لهيئة الاتصالات وتقنية المعلومات سواء عند الحصول على ترخيص مزاولة نشاطها أو حتى عند توقف نشاطها، ولابد أن تكون المعلومات والوثائق المسلمة للهيئة صحيحة، وأن مجرد تقديم جهات المصادقة الرقمية لبيانات كاذبة، أو معلومات مضللة للهيئة، أو إساءة استخدامها يشكل جريمة يعاقب عليها نظام التعاملات الإلكترونية الذي نص في الفقرة الرابعة من المادة (٢٣) منه على أنه «يعد مخالفة لأحكام هذا النظام... (4) قيام مقدم خدمات التصديق بتقديم بيانات كاذبة أو معلومات مضللة للهيئة أو أي سوء استخدام لخدمات التصديق».

وتعد هذه الجريمة كسابقتها من جرائم الخطر، حيث يتطلب قيامها توافر الركنين المادي والمعنوي.

1-الركن المادي:

يقوم الركن المادي لهذه الجريمة بمجرد قيام جهة المصادقة الرقمية بتقديم معلومات كاذبة أو معلومات مضللة لهيئة الاتصالات وتقنية المعلومات السعودية سواء عند الحصول على ترخيص مزاولة نشاطها، أو حتى عند توقف نشاطها، أو أي إساءة من جانب جهة المصادقة لاستخدام خدمات التصديق.

ولا تشترط هذه الجريمة حدوث ضرر معين أو نتيجة إجرامية، بل يكفي إقبال جهة المصادقة على تقديم معلومات كاذبة أو معلومات مضللة لهيئة الاتصالات وتقنية المعلومات أو أي إساءة لاستخدام خدمات التصديق، ويرجع تجريم ذلك الفعل لما فيه من مخالفة للشروط الواجب توافرها في هذه الجهة لمزاولة نشاطها، كما أن هذا الفعل يزعزع الثقة الواجب توافرها في التعاملات الإلكترونية (حجازي،2005، ص: 503).

2-الركن المعنوي:

إن جريمة تقديم معلومات كاذبة أو معلومات مضللة لهيئة الاتصالات وتقنية المعلومات السعودية، أو أي إساءة لاستخدام خدمات التصديق تعد من الجرائم العمدية التي يتمثل الركن المعنوي فيها في القصد الجنائي العام بركنيه العلم والإرادة، ولا يشترط توافر قصد جنائي خاص، وذلك لكونها من جرائم الخطر التي يعاقب المنظم السعودي فيها على مجرد ارتكاب جهة المصادقة الرقمية للفعل المجرم،

وعلى ذلك يعاقب المنظم بعقوبة الجريمة التامة بمجرد تحقق الركن المادي مع توافر القصد الجنائي دون اشتراط تحقق النتيجة المستهدفة من ارتكاب الجريمة.

خامساً-إنشاء أو نشر شهادة رقمية أو توقيع إلكتروني لغرض احتيالي:

إن إنشاء أو نشر شهادة تصديق رقمية أو توقيع إلكتروني لغرض احتيالي أو لأي غرض غير مشروع يعد سلوكاً إجرامياً يعاقب عليه النظام حتى وإن كان من قام بنشرها أو استخدامها غير منشئ لها، ويشترط أن يكون الهدف المرجو من هذا الفعل أن يستعمل لغرض احتيالي، أو لأي غرض غير مشروع استخدام شهادة التصديق الرقمي، أو التوقيع الإلكتروني لإبرام صفقات وهمية، أو مشبوهة عبر وسائل الاتصال الإلكترونية، ولهذا فقد نصت الفقرة الخامسة من المادة (٢٣) من نظام التعاملات الإلكترونية السعودي على أنه «يعد مخالفة لأحكام هذا النظام... (5) إنشاء شهادة رقمية، أو توقيع إلكتروني، أو نشرهما، أو استعمالهما لغرض احتيالي، أو لأي غرض غير مشروع».

كما نص المشرع الإماراتي على هذه الجريمة في المادة (٢٩) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي رقم ٢ لسنة 2002م التي جاء فيها «يعاقب كل من أنشأ أو نشر عن معرفة أو وفر أية شهادة أو بيانات غير صحيحة لأي غرض احتيالي أو أي غرض غير مشروع، بالحبس وبغرامة لا تجاوز 250,000 درهم أو بإحدى هاتين العقوبتين».

ويتضح من النصوص السابقة أن كلا من فعل الإنشاء والنشر والاستعمال تمثل عناصر النشاط الإجرامي في الركن المادي للجريمة، وتعد هذه الصورة من الجرائم العمدية وصورة الركن المعنوي فيها هو القصد الجنائي بنوعيه العام والخاص.

1-الركن المادي:

يتمثل الركن المادي لهذه الجريمة في الأفعال المادية التي يتكون منها السلوك الإجرامي، وهذه الأفعال تتمثل في إنشاء أو نشر شهادة تصديق رقمية أو توقيع إلكتروني لغرض احتيالي أو لأي غرض غير مشروع والعلة من تجريم ذلك الفعل هو المحافظة على الثقة في شهادة التصديق الرقمي والتوقيعات الإلكترونية وحمايتها (حجازي،2005، ص: 506).

2-الركن المعنوي:

باعتبار أن هذه الجريمة من الجرائم العمدية فإنه يستلزم توافر القصد الجنائي بنوعيه أي القصد العام والقصد الخاص، فأما بالنسبة للقصد الجنائي العام الذي يقوم على عنصري العلم والإرادة فإنه ينبغي أن يعلم الجاني بأنه يقوم بإنشاء أو نشر شهادة تصديق رقمية أو توقيع بقصد الإضرار المادي بالغير، وأما بالنسبة

للقصد الجنائي الخاص فإنه يجب أن تتجه نية الجاني إلى تحقيق غرض احتيالي، أو أي غرض غير مشروع.

سادساً-تزوير سجل إلكتروني أو توقيع إلكتروني أو شهادة التصديق الرقمي أو استعمالهم:

جرم المنظم السعودي أي تزوير في سجل إلكتروني أو توقيع إلكتروني أو شهادة التصديق الرقمي أو استعمالهم مع العلم بالتزوير حسبما نصت على ذلك الفقرة السادسة من المادة (٢٣) من نظام التعاملات الإلكترونية السعودي، من أنه « يعد مخالفة لأحكام هذا النظام... (6) تزوير سجل إلكتروني، أو توقيع إلكتروني، أو شهادة تصديق رقمي، أو استعمال أي من ذلك مع العلم بتزويره».

وهذا النوع من التزوير يطلق عليه مسمى (التزوير المعلوماتي) (العبيدي،2009،ص: 177)، ويعتمد على تغيير الحقيقة في بيانات السجل الإلكتروني، أو التوقيع الإلكتروني، أو شهادة تصديق رقمي عن طريق الاصطناع والتعديل لتغيير مضمونه بطريقة كلية أو جزئية، ويحصل هذا التزوير بأي وسيلة كانت كاستخدام برامج حاسوبية أو أنظمة معلوماتية مختصة في هذا المجال، وهو مما يترتب عليه بالتبعية اختلاف مضمون التعاملات النظامية القائمة على صحة هذه البيانات محل التزوير والغش (إبراهيم،2010،ص: 279)، ولكي يعتبر هذا السلوك مجرماً لابد من توافر الركنين المادي والمعنوي:

1-الركن المادي:

يتمثل الركن المادي لهذه الجريمة في سلوك الجاني المتمثل في تغيير الحقيقة التي تكون محل السجل الإلكتروني أو التوقيع الإلكتروني أو شهادة التصديق الرقمي أو استعمالهم، وقد يقع هذا التزوير من صاحب السجل أو التوقيع أو شهادة التصديق بقصد الإضرار بالغير أو يقع التزوير بواسطة جهات المصادقة الرقمية أو بفعل أحد موظفيها مستغلاً بذلك وظيفته .A) Penneau ,2002, p.2060).

وتصنف هذه الجريمة ضمن جرائم الخطر التي يعاقب عليها النظام السعودي، حيث يتم تجريم السلوك دون توقف ذلك على تحقق نتيجة معينة، فهذه الجريمة لا تعد من جرائم الضرر التي يرتبط العقاب فيها بإلحاق الضرر بالمجني عليه.

2-الركن المعنوي:

لا تكتمل جريمة تزوير السجل الإلكتروني أو التوقيع الإلكتروني أو شهادة التصديق الرقمي أو استعمالهم إلا بتوافر الركن المعنوي إلى جانب الركن المادي على غرار غيرها من الجرائم، وتعد هذه الجريمة من الجرائم العمدية، وصورة الركن المعنوي فيها هي القصد الجنائي بنوعيه، أي: القصد الجنائي العام والمتمثل في علم

الجاني بأنه يغير الحقيقة في السجل الإلكتروني أو التوقيع الإلكتروني أو شهادة التصديق الرقمي أو استعمالهم، وأن من شأن سلوكه الإجرامي إحداث الضرر، وعلمه بأن هذا السلوك محظور ويعاقب عليه النظام، ومع ذلك يقدم على إتيانه، وتتجه إراداته إلى هذا السلوك (تغيير الحقيقة) والأثر المترتب عليه وهو أن يشتمل السجل الإلكتروني، أو التوقيع الإلكتروني، أو شهادة التصديق الرقمي على بيانات تخالف الحقيقة، وأما القصد الجنائي الخاص فيتمثل في اتجاه نية الجاني إلى تحقيق غاية معينة وهي استعمال السجل الإلكتروني، أو التوقيع الإلكتروني، أو شهادة التصديق الرقمي فيما زور من أجله.

سابعاً-نشر شهادة تصديق رقمي مزورة أو ملغاة أو موقوفة:

إن قيام جهات المصادقة الرقمية أو صاحب شهادة المصادقة الرقمية أو شخص آخر بنشر شهادة تصديق رقمي مزورة أو ملغاة أو موقوفة وهم يعلمون بحالها وجعل الغير يُعول عليها في التعامل يعد سلوكاً إجرامياً يعاقب عليه النظام، وفي ذلك نصت الفقرة (10) من المادة (23) من نظام التعاملات الإلكترونية السعودي على أنه «يعد مخالفة لأحكام هذا النظام... (10) نشر شهادة مصادقة رقمية مزورة، أو غير صحيحة، أو ملغاة، أو موقوف العمل بها، أو وضعها في متناول شخص آخر، مع العلم بحالها. ويستثنى من ذلك حق مقدم خدمات التصديق الوارد في الفقرة (4) من المادة الثامنة عشرة)».

كما تطرق المشرع الإماراتي لهذه الجريمة في الفقرة (ج) من المادة (28) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي رقم ٢ لسنة 2002م، وجاء فيها «لا يجوز لأي شخص أن ينشر شهادة تشير إلى مزود خدمات تصديق مدرج اسمه في الشهادة، إذا كان الشخص يعرف أن:(ج) الشهادة قد ألغيت أو أوقفت، إلا إذا كان ذلك النشر بغرض التحقق من توقيع إلكتروني أو رقمي تم استعماله قبل الإيقاف أو الإلغاء».

وانطلاقاً من النصوص السابقة فإن قيام هذه الجريمة يتطلب توافر الركن المادي والمعنوي.

1-الركن المادي:

يتمثل السلوك الإجرامي لهذا الفعل في أن الجاني ينشر شهادة مزورة أو ملغاة أو موقوفة أو يضعها في متناول شخص آخر، وينصب هذا السلوك على محل معين هو شهادة التصديق الرقمي، وهذه الجريمة تعد من جرائم السلوك المجرد، حيث يتكامل قيام الركن المادي فيها بمجرد إتيان الجاني هذا السلوك الإجرامي بدون تطلب حدوث ضرر بجهة معينة أو شخص ما. ويرجع تجريم ذلك السلوك لما يترتب عليه في إلحاق الضرر بحقوق صاحب الشهادة الذي استخدمها أو الغير الذي اعتمد على صحة البيانات التي تتضمنها الشهادة عند التعاقد

الإلكتروني (أحمد،2011، ص: 133)، ويستثنى من ذلك حق جهات المصادقة الرقمية في إنشاء قاعدة بيانات لشهادات الموقوفة والملغاة التي سبق وأن أصدرتها مع الحق في حفظها ونشرها أو الاطلاع عليها إلكترونياً للتأكد من بيانات الشهادة ومن وجود توقيع إلكتروني تم استعماله قبل إصدار قرار الوقف أو الإلغاء.

2 -الركن المعنوي:

هذه الجريمة من الجرائم العمدية، إذ لابد فيها من توافر القصد الجنائي العام بعنصريه العلم والإرادة، وذلك بأن يعلم الجاني بأنه يقوم بنشر شهادة مزورة أو ملغاة أو موقوفة أو وضعها في متناول شخص آخر، وأن تتجه إرادته إلى إحداث هذا السلوك الإجرامي ويقبل النتائج المترتبة عليه، ويلاحظ أن هذه الجريمة لا تقع عن طريق الخطأ وهو ما يستشف من صياغة الفقرة من (10) من المادة (23) من نظام التعاملات الإلكترونية السعودي التي جرمت هذا السلوك، فقد بدأت بعبارة «نشر شهادة مصادقة رقمية»، أو كما هو مبين من صياغة الفقرة (ج) من المادة (28) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي التي ورد بها عبارة «الشخص يعرف أن :(ج) الشهادة قد ألغيت أو أوقفت» وهو ما يفيد العمد أو انصراف إرادة الجاني إلى ارتكاب هذا السلوك الإجرامي.

الفرع الثاني

أثر تحقق المسؤولية الجزائية لجهات المصادقة الرقمية

بعد التعرف على نطاق المسؤولية الجزائية الجهات المصادقة الرقمية من خلال تحديد الأفعال التي تشكل جرائم والتي يمكن أن ترتكبها هذه الجهات أثناء مزاولة نشاطها، لابد من تحديد الأثر المتحقق على ارتكاب هذه الجرائم، والذي يتمثل في العقوبات التي فرضها النظام لكل جريمة من هذه الجرائم، والتي تنقسم إلى نوعين على النحو التالي:

أولا-العقوبات الأصلية:

وهي العقوبات المقررة أصلاً للجريمة، ولقد نصت المادة (24) من نظام التعاملات الإلكترونية السعودي على أنه «مع عدم الإخلال بأي عقوبة أشد ينص عليها في نظام آخر، يعاقب كل من يرتكب أيا من الأعمال المنصوص عليها في المادة (٢٣) من هذا النظام بغرامة لا تزيد عن على خمسة ملايين ريال، أو بالسجن مدة لا تزيد على خمس سنوات، أو بهما معاً».

من خلال هذا النص يتبين أنه إذا توافرت أركان وشروط إحدى هذه الجرائم المنصوص عليها في المادة (٢٣) من نظام التعاملات الإلكترونية السعودي، يعاقب صاحب جهة المصادقة الرقمية أو أحد العاملين بها المسؤولين عن

ارتكاب الجريمة بالحبس والغرامة، وبالرغم من أن المنظم السعودي لم يضع حد أدنى لكل منهما، إلا أنه وضع حد أقصى لعقوبة الحبس وهي خمس سنوات، والحد الأقصى لعقوبة الغرامة وهي خمسة ملايين ريال، كما يجوز للقاضي ناظر الدعوى الحكم بالعقوبتين معاً أو بأحدهما حسب ظروف كل دعوى.

وفي هذا الصدد نص أيضًا قانون المعاملات والتجارة الإلكترونية لإمارة دبي رقم ٢ لسنة ٢٠٠٢ على عقوبتي الحبس والغرامة التي تتراوح ما بين مائتان وخمسون ألف، ومائة ألف درهم إماراتي في المواد (٢٩ و٣٠ و٣١ و٣٢) منه، وتفرض هذه العقوبات على جهة المصادقة الرقمية أو أي شخص تابع لها سواء أكان عضو مجلس إدارة أو مدير أو موظف في حالة ثبوت إدانتهم بأي مخالفة لأحكام هذا القانون أو اللوائح الصادرة بموجبه.

ثانياً-العقوبات التكميلية:

هي العقوبات التي قد تفرض على جهات المصادقة الرقمية بناء على الحكم عليها بالعقوبة الأصلية لجريمتها، ومن هذه العقوبات عقوبة المصادرة، وعقوبة الحجز، وعقوبة إلغاء الترخيص:

1-عقوبة المصادرة:

تعتبر عقوبة المصادرة من العقوبات المالية والتي تتمثل في نزع ملكية الأجهزة والمنظومات الإلكترونية، والبرامج المستخدمة في ارتكاب الجريمة من ملك جهة المصادقة الرقمية المخالفة وإضافتها إلى ملك الدولة دون مقابل.

وقد نصت على هذه العقوبة المادة (24) من نظام التعاملات الإلكترونية السعودي، وجاء فيها «.... ويجوز الحكم بمصادرة الأجهزة والمنظومات والبرامج المستخدمة في ارتكاب المخالفة». وما يؤخذ على المنظم السعودي في هذا الصدد أنه جعل الحكم بعقوبة المصادرة جوازيًا للقاضي وهو أمر لا يستقيم مع خطورة وجسامة المخالفة، لذا يقترح الباحث أن يكون الحكم بعقوبة المصادرة وجوبية حتى لا يتيح لجهات المصادقة المخالفة فرصة الاستفادة من الأجهزة والمنظومات والبرامج المستخدمة في الجريمة مرة أخرى على اعتبار أن هذا هو الهدف الأساسي والمستهدف من فرض عقوبة المصادرة.

كما فرض قانون المعاملات والتجارة الإلكترونية لإمارة دبي رقم 2 لسنة2002م في المادة (33) منه، وجاء فيها «... تحكم المحكمة في حالة الإدانة بموجب أحكام هذا القانون عقوبة المصادرة بمصادرة الأدوات التي استعملت في ارتكاب الجريمة».

2-عقوبة الحجز:

عقوبة الحجز تعتبر إجراء فاعل للمحافظة على

دليل ارتكاب الجريمة، أو استخدام بعض ما تحصل عليه من بيع الأدوات والأجهزة والبرامج الإلكترونية المحجوز عليها لتعويض المضرور إذا ما ثبت للمحكمة وقوع الجريمة التي نجم عنها الضرر، وتوقع عقوبة الحجز على جهة المصادقة الرقمية(حجازي،2005،ص: 534) في حال إدانتها بأحد الجرائم المنصوص عليها في نظام التعاملات الإلكترونية السعودي، إذ أنه وفقًا للمادة (25) من هذا النظام «تتولى الهيئة بالاستعانة والتنسيق مع الجهات السعودي المعنية مهمة الضبط والتفتيش على ما يقع من المخالفات المنصوص عليها في المادة (23) من النظام، وتعد محضراً بذلك، وللهيئة الحق في حجز الأجهزة والمنظومات والبرامج المستخدمة في ارتكاب المخالفة إلى حين البت فيها. ويحدد المحافظ بقرار منه أسماء الموظفين المختصين بهذه المهمة، وكيفية إجراء الضبط والتفتيش». ويتبين من النص السابق أن هيئة الاتصالات وتقنية المعلومات هي المنوط بها حجز الأدوات التي استعملتها جهة المصادقة الرقمية في ارتكاب الجريمة إلى حين صدور حكم بات فيها، ويعتبر هذا إجراء تحفظيًّا يزول في حالة ثبوت عدم ارتكاب هذه الجريمة، وهذا ما أكدته الفقرة الثانية من المادة (17) من اللائحة التنفيذية من نظام التعاملات الإلكترونية السعودي بنصها على أنه يجوز للهيئة حجز الموارد الفنية وقواعد البيانات، وغير ذلك من التدابير المناسبة التي تقتضيها حماية حقوق المتعاملين».

3-إلغاء الترخيص:

تتمثل عقوبة إلغاء الترخيص في شطب اسم جهة المصادقة الرقمية من سجل المرخص لهم بمزاولة نشاط خدمات التصديق الرقمي نتيجة ارتكابها أحد الجرائم المنصوص عليها، وهو ما يعد إخلالاً جسيماً بالتزاماتها التي فرضها النظام، ولقد منح المنظم السعودي لهيئة الاتصالات وتقنية المعلومات سلطة إلغاء ترخيص أي من جهات المصادقة الرقمية المخالفة لأحكام النظام استناداً في ذلك إلى الفقرة (2) من المادة (15) من نظام التعاملات الإلكترونية التي تنص على أنه «تتولى الهيئة تطبيق هذا النظام، ولها في سبيل تحقيق ذلك، الاختصاصات الآتية: (أ) إصدار التراخيص لمزاولة نشاط «مقدم خدمات التصديق»، وتجديدها، وإيقاف العمل بها، وإلغاؤها ويتضح من خلال استعراض أثر تحقق المسؤولية الجزائية لجهات المصادقة الرقمية، أن التشريعات السابقة قد أقرت حماية جزائية للتوقيع والتصديق الرقمي من خلال تعددها لمختلف الجرائم الواقعة عليهما، والملاحظ من استقراء نصوص المواد التي تضمنت هذه الجرائم خلو نظام التعاملات الإلكترونية السعودي وقانون

المعاملات والتجارة الإلكترونية لإمارة دبي، من اعتماد تصنيف لهذه الجرائم على غرار التشريعات الأخرى.

كما يلاحظ أنه على الرغم من أن النظام السعودي قد فرض عقوبات أصلية وتكميلية، إلا أنه لم يشدد العقوبة في حالة تكرار ارتكاب إحدى هذه الجرائم أو المخالفات المنصوص عليها في نظام التعاملات الإلكترونية، أي: لم يعالج حالة عودة جهات المصادقة الرقمية أو العاملين بها إلى اقتراف ذات الجريمة، أو المخالفة، أو ارتكاب عدة جرائم، أو مخالفات مماثلة بعد معاقبتها من أجل الجريمة، أو المخالفة السابقة. حيث إن العودة إلى ارتكاب الجريمة مرة أخرى يعد دلالة على وجود الإرادة المصرة لدى الجاني (جهة المصادقة الرقمية أو العاملين بها) على الإضرار بالغير ومخالفة أحكام النظام.

خاتمة

بإيجاز، يمكن للباحث تركيز أهم نتائج هذا البحث فيما يلي:

1. لا يوجد تعريف فقهي متفق عليه لجهات المصادقة الرقمية، كما أنه لا توجد تسمية موحدة لهذه الجهات في تشريعات الدول المختلفة التي نظمت عملها ومسؤوليتها.
2. تقوم جهات المصادقة الرقمية بدور الوسيط المؤتمن بين أطراف التعامل الإلكتروني، والشهادات التي تصدرها في هذا الشأن هي التي ترسخ الثقة في المعاملات الإلكترونية.
3. تحديد طبيعة التزامات جهات المصادقة الرقمية من حيث كونها التزامات ببذل عناية أو التزامات بتحقيق نتيجة يتطلب في واقع الحال، الرجوع إلى مضمون العقد الذي يربط جهات التصديق بصاحب الشهادة وأيضاً المصلحة التي يبتغي طرفي العقد تحقيقها من خلاله.
4. مسؤولية جهات المصادقة الرقمية في تعويض الضرر الناتج عن إخلالها بالتزاماتها تخضع لأحكام القواعد العامة للمسؤولية المدنية متى توافرت أركانها، فبموجب علاقتها بالعميل صاحب الشهادة تخضع لأحكام المسؤولية العقدية نظرا لوجود عقد بينهما، أما في إطار علاقتها بالغير الذي عول على الشهادة الصادرة عنها فإنها تخضع لأحكام المسؤولية التقصيرية نظراً لعدم وجود علاقة عقدية تربطهما معاً.
5. حظيت المسؤولية المدنية لجهات المصادقة الرقمية حظيت بتنظيم خاص من التشريعات الناظمة لعملها حيث أفردت هذه التشريعات نصوصاً خاصة لمسؤولية جهات المصادقة عن تعويض الأضرار الناتجة عن إخلالها بالتزاماتها، ومن هذه التشريعات التوجيه

الأوروبي، والنظام السعودي، والقانون الإماراتي.

6. يواجه المضرور صعوبة في إقامة الدليل على مسؤولية جهات المصادقة الرقمية في حال وقوع خطأ من جانبها، ويعود ذلك إلى ما تتمتع به تلك الجهات من إمكانيات مالية وموارد بشرية تشكل دعامات، وتجعل من إثبات خطأ جهات المصادقة أمراً متعذراً.
7. جعل نظام التعاملات الإلكترونية السعودي الحكم بعقوبة مصادرة الأجهزة والمنظومات والبرامج المستخدمة في ارتكاب أحد الجرائم المخالفة لأحكامه جوازيًا للقاضي.
8. لم يعالج نظام التعاملات الإلكترونية السعودي حالة عودة الجاني (سواء جهة المصادقة الرقمية أو العاملين بها إلى اقتراف ذات الجريمة أو جريمة أخرى مماثلة بعد معاقبته من أجل الجريمة السابقة.

وبناء على ما تقدم، فإن الباحث يوصي بما يلي:

1. زيادة الوعي لدى المتعاملين بالمعاملات بأهمية التصديق الرقمي وإجراءاته، وذلك بعقد الندوات والدورات المتخصصة والمؤتمرات، التي تعالج هذا الموضوع الهام.
2. أن مجرد توافر معلومات غير صحيحة في شهادة التصديق الرقمي يكفي لقيام مسؤولية جهة المصادقة في حال تعذر إثبات إخلال الأخيرة ببذل العناية المعقولة بسبب تعقد الإجراءات الفنية والتقنية مع عدم الاعتداد بأي مبرر لإعفائها إلا في حالة إثبات عائدية الخطأ إلى سبب أجنبي وليس إثبات عدم إهمالها أو تقصيرها، إذ إن عدم الإهمال أو التقصير هو من ضمن واجباتها وليس مبرراً لإعفائها من المسؤولية.
3. قيام المنظم السعودي بإلزام جهات المصادقة الرقمية بأن تحدد بشكل دقيق طبيعة التزاماتها من خلال بنود العقود التي تبرمها مع عملائها.
4. أن يتشدد القضاء السعودي في إمكانية قبول نفي الخطأ من جانب جهات المصادقة الرقمية بغرض التملص من المسؤولية المدنية.
5. إعفاء غير المضرور من عبء إثبات خطأ جهة المصادقة الرقمية مع اعتبار أن مسؤولية الأخيرة قائمة على الخطأ المفترض. وذلك اتساقاً مع القواعد العامة في المسؤولية المفترضة، إذ يكفي وقوع الضرر بسبب تهاون جهة المصادقة أو قصورها المهني لتترتب مسؤوليتها التقصيرية، وبغض النظر عن نوع التزامها تجاه الغير، وعلى جهة المصادقة نفي مسؤوليتها الكاملة عن الخطأ الذي نتج عنه الضرر.
6. فرض تأمين إجباري عن المسؤولية الناجمة عن أعمال جهات المصادقة الرقمية؛ إذ من شأن هذا التأمين أن يحدد طبيعة هذه المسؤولية وحالات الإعفاء منها.

7. أن ينص المنظم السعودي على أن الحكم بعقوبة مصادرة الأجهزة والمنظومات والبرامج المستخدمة في ارتكاب أحد الجرائم المخالفة لأحكام نظام التعاملات الإلكترونية يكون وجوبياً منعاً من استفادة الجاني منها مرة أخرى، وبذلك يتحقق الهدف الأساسي من هذه العقوبة.
8. مراعاة المنظم السعودي للجانب العقابي، ووضع عقوبة أشد في حالة عودة الجاني إلى اقتراف ذات الجريمة أو جريمة أخرى مماثلة بعد معاقبته من أجل الجريمة السابقة، تفادياً لتكرار الجريمة مرة أخرى، ولإضفاء الحماية الكاملة على التعاملات الإلكترونية المصادق عليها.
9. إنشاء محاكم متخصصة لنظر المنازعات الناشئة عن تقديم خدمات المصادقة الرقمية للتوقيع الإلكتروني لضمان سرعة الفصل بغرض تحقيق العدالة الناجزة.

قائمة المراجع:

أولاً -باللغة العربية:

أبو الليل، إبراهيم الدسوقي. (2002م). الجوانب القانونية للتعاملات الإلكترونية. الكويت: مجلس النشر العلمي.

أبو الليل، إبراهيم الدسوقي. (2003م). توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق تجاه الغير المتضرر. مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون. كلية الشريعة والقانون. جامعة الإمارات العربية المتحدة. الفترة من 10-12مايو2003م.المجلد5. دبي. الإمارات: منشورات جامعة الإمارات العربية المتحدة.

شرف الدين، أحمد. (2000م). عقود التجارة الإلكترونية. القاهرة: دار النهضة العربية.

البياتي، نادية ياس. (2014م). التوقيع الإلكتروني عبر الإنترنت ومدى حجيته في الإثبات. ط1. الأردن: دار البداية ناشرون وموزعون.

-الشنراقي، حسام محمد نبيل. (2013م). الجرائم الإلكترونية: دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني. مصر. الإمارات: دار الكتب القانونية، دار شتات للنشر والإلكترونيات.

العبيدي، أسامة بن غانم. (2012م). حجية التوقيع الإلكتروني في الإثبات. المجلة العربية للدراسات الأمنية والتدريب بجامعة نايف للعلوم الأمنية. السعودية، ٢٨(56)، 141-198.

كيسي، زهيرة. (2012م). النظام القانوني لجهات التوثيق الإلكتروني. مجلة دفاتر السياسة والقانون. الجزائر، (7)، 213-227.

كميل، طارق. (2008). مقدمو خدمات المصادقة الإلكترونية، مجلة جامعة الشارقة للعلوم الشرعية والقانونية. الإمارات، 5(3)، 237-279.

عبد الفتاح، عابد فايد. (2006م). الكتابة الإلكترونية في القانون المدني: الفكرة والوظائف. القاهرة: دار النهضة العربية.

التهامي، سامح عبد الواحد. (2006م). التعاقد عبر الإنترنت. القاهرة: دار الكتب القانونية.

البكباشي، سحر. (2009م). التوقيع الإلكتروني. الإسكندرية: منشأة المعارف.

الحفني، عبد الحميد عثمان. (1992م). المسؤولية المدنية للموثق: دراسة مقارنة بين القانون المصري والفرنسي. مجلة البحوث القانونية والاقتصادية بجامعة المنصورة. مصر، (12)، 1-252.

حجازي، عبد الفتاح بيومي(2009م). التجارة

الإلكترونية العربية. الكتاب الثاني: النظام القانوني للتجارة الإلكترونية في دولة الإمارات العربية المتحدة. ج ٢. مصر: دار الكتب القانونية.

حجازي، عبد الفتاح بيومي. (2008م). حماية المستهلك عبر شبكة الإنترنت: دار الكتب القانونية.

حجازي، عبد الفتاح بيومي. (2005م). التوقيع الإلكتروني في النظم القانونية المقارنة. ط1. الإسكندرية: دار الفكر الجامعي.

حجازي، عبد الفتاح بيومي. (2002م). النظام القانوني لحماية التجارة الإلكترونية. الكتاب الأول: نظام التجارة الإلكترونية وحمايتها مدنياً. الإسكندرية: دار الفكر الجامعي.

عبد المجيد، ثروت. (2007م). التوقيع الإلكتروني. الإسكندرية: دار الجامعة الجديدة.

الطوال، عبير ميخائيل الصفدي. (2007م). التوقيع الإلكتروني. ط1. عمان. الأردن: دار وائل للنشر والتوزيع.

التميمي، علاء حسين. (2007م). الجهة المختصة بإصدار شهادة التصديق الإلكتروني. القاهرة: دار النهضة العربية.

التميمي، علاء حسين. (2012م). المستند الإلكتروني. ط2. القاهرة: دار النهضة العربية.

فهمي، خالد مصطفى. (2007م). النظام القانوني للتوقيع الالكتروني في ضوء الاتفاقيات الدولية والتشريعات العربية. الإسكندرية: دار الجامعة الجديدة.

أبو مندور، مصطفى. (2008م). خدمات التوثيق الإلكتروني. ندوة الجوانب القانونية للتعاملات الإلكترونية. كلية الحقوق. جامعة حلوان. مسقط. سلطنة عمان. (http://almhamihamed.blog-spot.com/2012/04/blog-post_4021.html-)

منصور، محمد حسين. (2007م). الإثبات التقليدي والإلكتروني. الإسكندرية: دار الفكر الجامعي.

يوسف، أمير فرج. (2007م). التوقيع الإلكتروني. الإسكندرية: دار المطبوعات الجامعية.

ثانياً-باللغة الإنجليزية:

Angle, J. (1999). why use digital (signature of electronic commerce). *Journal of information law and technology*.

Bruce, S., Nathan, Terence D. Watson. (2010). Electronic signatures, agreements and documents: The Recipe for Enforceability and Admissibility.

Chris, H. (2011). "A history of signatures". From cave paintings to robo-signings. For a history on the statute of frauds with regard to advances in technology: supra note 31.

George, B., Bellas, Wachowski, Patricia, B. F. (2001) "Introduction to the uniform electronic transactions act: Principles, policies and provisions": 37 IDAHOL. REV.

Harry, H. T. (2001). " Electronic contracts in the United States and the European union" Varying Approaches to the Elimmination of paper and pen: EJCL, vol.5.3.

Froomkin, M. (1996). The essential role of trusted third parties in electronic commerce.

Loeb, L. (1995). Your right in the online world: Osborn Mc / Graw – hall, New York, USA.

Burr, W., Dodson, D., Newton, E., Perlner, R. , Polk, W. , Gupta, S. and Nabbus, E. (2013), Electronic Authentication Guideline, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-63-2

ثالثاً-ترجمة المراجع العربية بالإنجليزية:

Abdel-Fattah, A. (2006). Electronic writing in civil law: Idea and functions (in Arabic). Cairo: Dar Al -Nahda Al-Arabia.

Abdel-Magied, T. (2007). Electronic signature (in Arabic). Alexandria : Dar Al -Jamiea Al-Jadida.

Abu Aleil, A. (2002). Legal aspects of electronic transactions (in Arabic). Kuwait: Scientific Publication Council.

Abu Aleil, A. (2003). Documenting electronic transactions and the responsibility of the authentication body towards the affected third party (in Arabic). *Electronic Banking Conference between Sharia and Law*. Faculty of sharia and law. United Arab Emirates University, v.5. Dubai. Emirates: Publications of United Arab Emirates University.

Abu Mandur, M. (2008). Electronic documentation services (in Arabic). Symposium on legal aspects of electronic transactions. Faculty of Law. Helwan University. Muscat, Sultanate of Oman.

Mansour, M. (2007). Traditional and electronic proof (in Arabic). Alexandria: Dar Al-Fikr Al-jamai.

Youssef, A. (2007). Electronic signature (in Arabic). Alexandria: Dar Al-matbueat Al-jamieia.

رابعاً-باللغة الفرنسية:

Anne, P. (2003).la sécurité juridique à travers le processus de normalisation, sécurité juridique et sécurité technique:indépendance ou métissage, Confiance organisée par le programme international de coopération scientifique (CRDP/ CECOJI): Monterial, 30seb,2003.

Antoine,g., Gobert ,d.(2020). Pistes de reflextion pour une de legislation relative a la signature digitale et au régime des autorité de certification, available at: http:/ www. droit. fund, net. visited;21-3-2020.

Caprioli.E.(1998). sécurité et confiance danc le commerce électronique, signature numérique et autorité de certification: JCP.

Didier, G. (2001). Cadre juridique pour les signatures électroniques et les services de certification Analyse de la loi du 9 juillet 2001, publiée in la preuve, formation permanent CUP, Vol 54: Marsp.

Didier, G.(2020).commerce électronique ;Vers un cadre juridique général pour les tiers de confiance, available at: http:/ www.droittechnolgye.org/doniers/goberttiersconfiance. donier.pdf, visited;15-2-2020.

Parisienne,s., et Trudel, J.(1996). L, identification et la certification dans le commerce électronique, QUEBEC: Ed. Yuon Blaaisint.

Penneau, A. (2002). La certification des produits et system permettant la réalisation des actes et signatures électronique ; a propos du décret n.du 18 avr. 2002 ,Rev: Dalloz .

Pierre, H. V., Jean ,M.(2006). La confiance: sa nature et son rôle dans le commerce électronique: Lex. electronica vol. 11 n. 2, fall.

Thomas, J. (2000).smedinghoff: Revue hellénique de droit international.

خامساً -المواقع الإلكترونية:

www.almhamihamed.blogspot.com/2012/04/blog-post_4021.html.

www. droittechnolgye. org/doniers/goberttiersconfiance. donier. pdf,visited;15-1-2020

www. droit. fund, net. visited;21-3-2020

www.lex-electronica, org/articles/v11-2 vallee. mackaa/htm, visited;17-2-2020

www.lex. electronhca. orglarticles/v11-2valeemackaay. pdf.. visited;17-2-2020

Albakbashi, S. (2009). Electronic signature (in Arabic). Alexandria: Monchaat Al -Maaref.

Al Bayati, N. (2014). The electronic signature on the Internet and its validity in evidence (in Arabic). Edition1, Jordan: publisher: Dar Al Bidaya.

Aleabidi, A. (2012). Authentic electronic signature in evidence (in Arabic). *Arab Journal of Security Studies and Training*, *28*(56),141-198. Naif University for Security Sciences. Saudi Arabia.

Al-Hefni, A. (1992). The civil responsibility of the notary: A comparative study between Egyptian and French law (in Arabic). *Journal of Legal and Economic Research*, 12, 1-252. Mansoura University, Egypt.

Alshiniraqiu, H. (2013). Cybercrime: A comparative applied study on electronic signature assault crimes (in Arabic). Egypt. Emirates. Dar Al-kutub Al-qanunia. Dar Shatat lilnashr wal'iilikturuniaat.

Al-tihami, S. (2006). A contract over the internet (in Arabic). Dar Al-kutub Al-qanunia.

Al-tamimi, A. (2007). The authority responsible for issuing the electronic certification certificate (in Arabic). Dar Al -Nahda Al-Arabia.

Al-tamimi, A. (2012). Electronic document (in Arabic). Edition2. Cairo: Dar Al -Nahda Al-Arabia.

Al-twal, A. (2007). Electronic signature (in Arabic). Edition1. Oman. Jordan: Dar Wayil lilnashr waltawzie.

Charaf-Eddine, A. (2000). Electronic commerce contracts (in Arabic). Cairo: Dar Al -Nahda Al-Arabia.

Fahumi, K. (2007). The legal system for electronic signature in light of international agreements and Arab legislation (in Arabic). Alexandria: Dar Al -jamiea Al-jadida.

Hijazi, A. (2002). The legal system for protecting electronic commerce. The first book: The electronic commerce system and its civil protection (in Arabic). Alexandria: Dar Al-Fikr Al-jamai.

Hijazi, A. (2005). Electronic signature in comparative legal systems (in Arabic). Edition1. Alexandria: Dar Al-Fikr Al-jamai.

Hijazi, A. (2008). Consumer protection over the Internet (in Arabic). Dar Al-kutub Al-qanunia.

Hijazi, A. (2009). Electronic commerce of Arabs (in Arabic). The second book: The legal system for electronic commerce in the United Arab Emirates. Part 2. Egypt. Dar Al-kutub Al-qanunia.

Kaysi, Z. (2012). The legal system for electronic authentication bodies (in Arabic). *The Journal of Politics and Law Notebooks*. Algeria, 7,141-198.

Kmyl, T. (2008). Electronic authentication service providers (in Arabic). *University of Sharjah Journal of Sharia and Legal Sciences*, 5(3), 237-279. United Arab Emirates.