وزارة التعليم العالي والبحث العلمي

جامعة غرداية

كلية الحقوق والعلوم السياسية

قسم الحقوق

كتاب بيداغوجي في:

قانون المعاملات الإلكترونية

مؤلف بيداغوجي موجه لطلبة السنة الثانية ماستر

تخصص قانون خاص

من إعداد الدكتورة:

حيفري نسيمة أمال

السنة الجامعية: 2024 - 2025م

مـــقـــــــدمـــــــــة

في عصر يشهد تطورًا تكنولوجيًا هائلًا، أصبحت المعاملات الإلكترونية جزءًا لا يتجزأ من الحياة اليومية للأفراد والمؤسسات على حد سواء. سواء كنا نتحدث عن التعاقدات التجارية التي تتم عبر الإنترنت، أو العمليات المصرفية الإلكترونية، أو حتى التفاعل مع الهيئات الحكومية عبر المنصات الرقمية، فإن هذه التحولات السريعة والمستمرة في البيئة الرقمية قد أفرزت حاجة ماسة إلى وجود إطار قانوني ينظم هذه المعاملات ويضمن حقوق الأطراف المتعاقدة ويحميهم من المخاطر التي قد تنشأ عنها. من هنا، برز قانون المعاملات الإلكترونية كأحد الفروع القانونية الحديثة التي تستجيب لهذا الواقع الجديد، واضعًا الأسس والقواعد التي تحكم هذه التعاملات في إطار قانوني سليم.

تتجلى أهمية قانون المعاملات الإلكترونية في عدة جوانب، أبرزها توفير بيئة آمنة وموثوقة لإبرام العقود وتنفيذ العمليات التجارية عبر الإنترنت. فالتعاملات التي تتم في الفضاء الإلكتروني تختلف بطبيعتها عن تلك التي تحدث في العالم المادي، سواء من حيث الوسائل المستخدمة أو التحديات القانونية التي قد تنشأ عنها. على سبيل المثال، يمثل التوقيع الإلكتروني أحد الابتكارات القانونية التي ساعدت في إضفاء الطابع الرسمي والقانوني على العقود الإلكترونية، مما يضمن تنفيذها وفقًا للقوانين المعمول بها ويحفظ حقوق الأطراف المتعاقدة. كما أن حماية البيانات الشخصية، التي تعتبر من أبرز اهتمامات الأفراد في العصر الرقمي، تحتل مكانة محورية ضمن أحكام هذا القانون، حيث يهدف إلى توفير ضمانات قانونية لحماية هذه البيانات من الاستغلال أو التلاعب.

بالإضافة إلى ذلك، يوفر قانون المعاملات الإلكترونية أدوات قانونية حديثة تتناسب مع طبيعة المعاملات الرقمية، مثل الأدلة الإلكترونية والتوثيق الرقمي، مما يسهل عمليات الإثبات في النزاعات القانونية المتعلقة بالمعاملات الإلكترونية. وهذا يسهم في تعزيز الثقة في المعاملات الإلكترونية، سواء على المستوى المحلي أو الدولي، حيث أصبح بإمكان الأفراد والمؤسسات إبرام عقود والقيام بمعاملات مع أطراف في دول أخرى بثقة واطمئنان.

ولعل أحد الأسباب الرئيسية لنشوء قانون المعاملات الإلكترونية هو التوسع الهائل في التجارة الإلكترونية، التي شهدت نموًا غير مسبوق في العقود الأخيرة، فمع ظهور منصات التجارة الإلكترونية

العالمية وتزايد الاعتماد على الإنترنت كوسيلة رئيسية للتسوق والتعاقد، أصبح من الضروري وجود إطار قانوني يحكم هذه العمليات ويوفر الحماية للطرفين، سواء البائع أو المشتري، كما أدى التطور في الخدمات المالية الإلكترونية إلى ظهور مجموعة من التحديات القانونية الجديدة، مثل حماية المعلومات المالية وتنظيم الدفع الإلكتروني، وهو ما استدعى وضع تشريعات وقوانين تواكب هذه التحولات.

ومن الجدير بالذكر أن تطور قانون المعاملات الإلكترونية لم يكن بمعزل عن السياق التاريخي للتطور القانوني العام، ففي بدايات ظهور الإنترنت، كانت المعاملات الإلكترونية تجري في بيئة غير منظمة قانونيًا، مما أدى إلى ظهور العديد من المشاكل والنزاعات التي لم يكن هناك إطار قانوني محدد لحلها، ومع مرور الوقت، أدركت الدول والمنظمات الدولية الحاجة إلى وضع قوانين تنظم هذه المعاملات وتحمي حقوق الأطراف المعنية، وبالفعل، تم تطوير مجموعة من القوانين الوطنية والدولية التي وضعت الأسس والمعايير للتعاملات الإلكترونية، بما في ذلك توقيع العقود، حماية البيانات، وضمان أمن المعاملات.

الهدف من إعداد كتاب بيداغوجي في مقياس قانون المعاملات الإلكترونية يتجلى في تزويد الطلبة بأساس نظري وتطبيقي شامل لفهم هذا الفرع القانوني الحديث، يمكن تلخيص الأهداف الرئيسية لهذا الكتاب على النحو التالي:

- ✓ **توفير مادة علمية منظمة وشاملة:** وذلك من خلال تقديم محتوى علمي متكامل يغطي جميع جوانب قانون المعاملات الإلكترونية، بما في ذلك القواعد والمبادئ الأساسية، القوانين والتشريعات ذات الصلة، وأحدث التطورات في هذا المجال.
- ✓ **تعزيز الفهم التطبيقي:** بحيث سيتم تقديم أمثلة عملية وحالات دراسية تساعد الطالب على تطبيق المفاهيم القانونية في سياقات واقعية، مما يتيح لهم استيعاب كيفية تطبيق القوانين على المعاملات الإلكترونية المختلفة ويعزز قدرتهم على التعامل مع التحديات القانونية التي قد يواجهونها في المستقبل.
- ✓ **تسهيل العملية التعليمية:** من خلال تنظيم المحتوى بطريقة منهجية وواضحة، مما يساعد على تسهيل عملية التعليم والتعلم بالنسبة للطلبة والأساتذة على حد سواء. يشمل ذلك تقديم شرح

مبسط وسلس للمفاهيم القانونية المعقدة، بالإضافة إلى توفير تمارين وأسئلة تقويمية تساعد في تقييم مدى استيعاب الطالب للمادة العلمية.

- ✓ **تحسين المهارات البحثية والتحليلية:** من خلال تشجيعهم على دراسة المواد القانونية المتعلقة بالمعاملات الإلكترونية وتحليلها بشكل نقدي.
- ✓ **مواكبة التطورات التكنولوجية والقانونية:** بحيث سيسمح هذا الكتاب بتحديث المعرفة القانونية للطالب بما يتماشى مع التطورات السريعة في مجال التكنولوجيا والاقتصاد الرقمي، وذلك من خلال تسليط الضوء على التغيرات التشريعية المستمرة والتحديات الجديدة.
- ✓ **تعزيز الوعي القانوني للطالب:** وذلك بأهمية قانون المعاملات الإلكترونية في حماية الحقوق وضمان العدالة في العالم الرقمي، يشمل ذلك فهم أهمية الأمان القانوني في المعاملات الإلكترونية وحماية البيانات الشخصية والخصوصية في البيئة الرقمية.

باختصار يكمن الهدف من إعداد هذا الكتاب البيداغوجي في مقياس قانون المعاملات الإلكترونية في توفير أداة تعليمية فعالة تسهم في بناء قاعدة معرفية قوية لدى الطلبة، وتعزيز مهاراتهم التطبيقية والتحليلية، وتجهيزهم للتعامل مع التحديات القانونية في عصر التكنولوجيا الرقمية.

وباعتبار أن مقياس قانون المعاملات الإلكترونية يمثل استجابة حيوية وضرورية للتغيرات التي فرضتها الثورة الرقمية على المجتمعات الحديثة، ومع استمرار التطور التكنولوجي والاعتماد المتزايد على الإنترنت في مختلف جوانب الحياة، تظل الحاجة ماسة إلى تطوير هذا القانون وتحديثه باستمرار ليواكب التحديات الجديدة ويضمن حماية الحقوق وتحقيق العدالة في البيئة الرقمية، لذلك كان من الضروري افتتاح مضمون هذا الكتاب البيداغوجي بتقديم لمحة تمهيدية حول إلى الإطار القانوني للمعاملات الالكترونية، الذي سنتعرض من خلاله إلى ماهية نظم المعلومات والمبادلات الالكترونية ومفهوم المعاملات الالكترونية لنتعرض من خلال ذلك إلى تعريف هذا النوع من المعاملات تعريفا لغويا وقانونيا، وبيان أنواعها وآثارها القانونية، لننتقل بعد ذلك إلى تحديد مفهوم العقد الالكتروني في ظل القانون 05/18، مع تحديد التنظيم القانوني للتعاقد عن بعد من الناحية الموضوعية.

وباعتبار أن العقود الالكترونية تتطلب الاهتمام بالآليات القانونية التي تهدف إلى حماية المستهلك الالكتروني كونه يمثل الطرف الضعيف في العقد الالكتروني خلال مختلف مراحل إبرام العقد، كان لا بد من تسليط الضوء على الحماية القضائية للعقود المبرمة عن بعد، ومن ثم التطرق

إلى الحماية المستحدثة للمستهلك الالكتروني مع استعراض مختلف وسائل الإثبات القانونية لتجسيد تلك الحماية.

ولعل أهم مرحلة من مراحل العقد الالكتروني هي مرحلة التنفيذ، لذلك وجب علينا عرض التزامات المورد الإلكتروني وتحديد مسؤوليته القانونية، وجزاء الإخلال بها، بالإضافة إلى عرض طرق الوفاء الالكتروني خاصة في ظل القانون 05/18.

نتيجة لذلك سوف نعتمد في دراسة مقياس قانون المعاملات الإلكترونية على تقسيم الموضوع إلى المحاور التالية:

المحور الأول: مفهوم المعاملات الالكترونية، وأنواعها، وآثارها القانونية

المحور الثاني: طرق الاثبات في المعاملات الالكترونية

المحور الثالث: مسؤولية مزودي خدمة التصديق الالكتروني

المحور الرابع: التحديات المستقبلية وتطور المعاملات الالكترونية

المحور الأول:

مفهوم المعاملات الالكترونية

أنواعها - آثارها القانونية

قانون المعاملات الإلكترونية هو الإطار القانوني الذي ينظم الأنشطة والمعاملات التي تتم عبر الإنترنت ووسائل التكنولوجيا الحديثة، فهو يهدف إلى توفير الحماية القانونية للأطراف المتعاملة إلكترونيًا، من خلال تحديد حقوق وواجبات المستخدمين، وتوضيح كيفية إبرام العقود الإلكترونية، وحماية البيانات الشخصية، وضمان سلامة وسرية المعلومات المتبادلة. كما يساهم في تعزيز الثقة في المعاملات التجارية الإلكترونية، سواء للأفراد أو الشركات، ويشكل دعامة أساسية لتطوير التجارة الإلكترونية والتبادل الرقمي.

لذلك سنتناول ضمن هذا المحور مفهوم قانون المعاملات الإلكترونية وذلك من خلال التعرض إلى تعريف المعاملات الالكترونية، بعد التطرق إلى ظروف نشأتها، وأسباب ظهورها وتحديد ما الذي يميزها عن غيرها من المعاملات التقليدية (المبحث الأول)، ثم نتعرض إلى أنواع تلك المعاملات القائمة على الدعائم الالكترونية وتحديد أهم الآثار المترتبة نتيجة اعتمادها (المبحث الثاني).

المبحث الأول: الإطار النظري للمعاملات الالكترونية (النشأة – التعريف – الخصائص)

تُعدّ المعاملات الإلكترونية جزءًا مهمًا من التطور الرقمي الذي شهده العالم في العقود الأخيرة. نشأت هذه المعاملات نتيجة للتقدم التكنولوجي في مجال الاتصالات والشبكات، ولا سيما الإنترنت، حيث بدأ استخدامه كوسيلة رئيسية للتبادل التجاري والخدماتي. مع تزايد الاعتماد على التكنولوجيا الرقمية، أصبحت المعاملات الإلكترونية وسيلة فعالة وسريعة لتسهيل الأنشطة الاقتصادية بين الأفراد والشركات وحتى الحكومات، لذلك سنتعرض في البداية إلى نشأة المعاملات الالكترونية وأسباب ظهورها (المطلب الأول)، ثم نوضح أهم صور لتلك المعاملات في الواقع العملي مع تحديد أهم الآثار القانونية المترتبة عن المعاملات الالكترونية (المطلب الثاني).

المطلب الأول: نشأة المعاملات الالكترونية

نشأت المعاملات الإلكترونية في نهاية القرن العشرين نتيجة للتطور السريع في تكنولوجيا المعلومات والاتصالات، وخاصة مع انتشار الإنترنت خلال سنوات التسعينيات، وقد كانت البداية مع ظهور التجارة الإلكترونية كوسيلة جديدة للتبادل التجاري، مما أدى إلى تغييرات جذرية في أساليب الأعمال التقليدية.

الفرع الأول: أسباب ظهور المعاملات الالكترونية

ظهور المعاملات الإلكترونية كان نتيجة لتفاعل عدة عوامل تقنية واقتصادية بدأت بالظهور منذ منتصف القرن العشرين. أحد أبرز هذه العوامل كان التطور السريع في تكنولوجيا المعلومات والاتصالات، وخاصة الإنترنت، الذي أصبح وسيلة رئيسية لإجراء الأنشطة التجارية في التسعينيات.

أسباب ظهور المعاملات الإلكترونية:

في البداية، كان التقدم في نظم تبادل البيانات الإلكترونية (EDI) في الستينيات والسبعينيات خطوة أساسية نحو ما أصبح لاحقًا المعاملات الإلكترونية، تمثل ذلك في القدرة على إرسال الفواتير وأوامر الشراء إلكترونيًا بين الشركات، مما ساهم في تسهيل الأعمال التجارية عبر الإنترنت[1].

[1] Bea tanese, The History of Ecommerce: From the 1960s to the 2020s, 06/10/2021, https://www.shipmonk.com/blog/the-history-of-ecommerce-from-the-1960s-to-the-2020s, visité le : 21/09/2024.

ومع إطلاق شبكة الإنترنت العالمية (World Wide Web) في عام 1991، ومع تطوير متصفح الويب الأول، أصبحت الإنترنت متاحة بشكل أكبر للجمهور التجار، وقد أتاح هذا النظام الجديد للأفراد والشركات إجراء المعاملات بسهولة عبر الإنترنت، مما مهد الطريق لظهور التجارة الإلكترونية[1].

الانترنت هو مصطلح مكون من كلمتين، الكلمة الأولى عالمية " International " والكلمة الثانية تعني شبكة " Network " وعند دمج الكلمتين نتحصل على مصطلح انترنت " Internet " وبالتالي تم أخذ الجزء " inter " من الكلمة الأولى والجزء " Net " من الكلمة الثانية ليتشكل لنا " internet" بمعنى الربط بين الشبكات.

وفي ظل ثورة المعلومات التي شهدها العالم أواخر القرن العشرين ظهرت عدة مظاهر للاختراعات والتطورات في مجال أجهزة الحاسوب وإنتاج المعلومات والمعارف والاتصال، مما نتج عنه احتلال الشبكة العالمية للمعلومات (الانترنت) ذروتها في أحدث التقنيات المعلوماتية في السنوات الأخيرة، وأصبح للأنترنت الأثر الكبير في كل القطاعات والمجالات[2].

مع تطوير بروتوكولات الأمان مثل SSL (Secure Socket Layers) في عام 1994، أصبح من الممكن إجراء معاملات آمنة عبر الإنترنت، مما زاد من ثقة المستخدمين في استخدام الشبكة للتجارة، بحيث في نفس السنة، تمت أول عملية بيع عبر الإنترنت، وكانت لشخص اشترى ألبومًا موسيقيًا باستخدام هذه التقنية[3].

بالإضافة إلى التطور التكنولوجي، كان هناك حاجة من الشركات والأفراد لتبسيط العمليات التجارية وتقليل التكاليف التشغيلية، فالتجارة الإلكترونية وفرت وسيلة مريحة وسريعة للوصول إلى الأسواق العالمية، مما ساهم في ازدهارها وانتشارها.

---

[1] Vladimir Zwass, E-commerce History, Britannica, 28/08/2024, https://www.britannica.com/money/e-commerce, visité le : 08/09/2024.

[2] يوسف حسن يوسف، الاقتصاد الالكتروني، المركز القومي للإصدارات القانونية، القاهرة، مصر، الطبعة الأولى، 2012، ص 25.

[3] History And Evolution of Ecommerce - How It Began?, SpiralClick, 05/08/2019, https://spiralclick.com/blog/history-and-evolution-of-ecommerce, visité le : 11/01/2024.

الفرع الثاني: أهمية المعاملات الالكترونية

في عصر التكنولوجيا الرقمية المتسارع، أصبحت المعاملات الإلكترونية ضرورة حتمية في عالم الأعمال والتجارة. فقد أحدثت نقلة نوعية في كيفية تنفيذ العمليات التجارية، حيث أصبح بإمكان الشركات والأفراد على حد سواء إتمام صفقاتهم بسرعة ودقة عالية عبر الإنترنت، دون الحاجة إلى التعامل مع المستندات الورقية أو الوسائل التقليدية. هذا التحول إلى البيئة الرقمية لا يسهم فقط في توفير الوقت والجهد، بل أيضًا في تحسين الكفاءة التشغيلية وتقليل التكاليف، مما يعزز من تنافسية الشركات في الأسواق العالمية.

تساهم المعاملات الالكترونية في تعزيز الكفاءة والسرعة في العمليات التجارية، بحيث أصبحت المعاملات الإلكترونية عنصراً مهماً في تحسين الكفاءة والسرعة في العمليات التجارية، حيث يمكن للشركات اليوم تنفيذ الصفقات عبر الإنترنت بدلاً من الطرق التقليدية مثل البريد أو الفاكس، مما يقلل من الوقت المستغرق في تبادل المستندات ويسمح بإتمام المعاملات بشكل أسرع وأكثر دقة، هذا التحول يقلل من التكاليف التشغيلية ويساهم في زيادة الإنتاجية[1].

كما تسهم المعاملات الإلكترونية في تعزيز الشفافية والمصداقية في العلاقات التجارية من خلال توفير توثيق إلكتروني لجميع الخطوات التي تتم أثناء إبرام الصفقات، بحيث توفر الأنظمة الإلكترونية سجلات مفصلة وقابلة للمراجعة، مما يساعد في تقليل فرص التزوير والاحتيال ويزيد من الثقة بين الأطراف المتعاملة[2].

تعمل المعاملات الإلكترونية أيضا على تمكين الشركات من الوصول إلى أسواق جديدة على مستوى العالم، فبدلاً من الاعتماد فقط على السوق المحلي، يمكن للشركات تقديم منتجاتها وخدماتها للعملاء في مختلف أنحاء العالم من خلال شبكة الإنترنت، مما يتيح لها توسيع نطاق أعمالها وزيادة إيراداتها.

[1] علي أبو حيدر، أثر التكنولوجيا الرقمية في العمليات التجارية، دار الفكر العربي، مصر، 2019، ص 45.

[2] ماجد القرني، التجارة الإلكترونية وتطور نظم الشفافية، المكتبة الدولية، السعودية، 2021، ص 78.

أحد الفوائد الرئيسية للمعاملات الإلكترونية هو تقليل التكاليف التشغيلية، فبفضل استخدام الأنظمة الإلكترونية، يمكن للشركات الاستغناء عن الكثير من الموارد البشرية وتقليل التكاليف المرتبطة بإدارة الأعمال التجارية التقليدية مثل الطباعة والشحن، هذه التكلفة المخفضة تساعد في زيادة هامش الربح وتحسين القدرة التنافسية[1].

المعاملات الإلكترونية تجعل الوصول إلى العملاء أكثر سهولة وفعالية، ذلك أنه بفضل الأدوات الرقمية، يمكن للشركات التواصل مع العملاء في أي وقت ومن أي مكان، مما يسهم في تحسين خدمة العملاء وزيادة ولائهم، كما تساعد أدوات التسويق الإلكتروني على استهداف العملاء بدقة أكبر، مما يعزز من فاعلية الحملات التسويقية.

تعمل المعاملات الإلكترونية على توفير التكاليف مقارنةً بالمعاملات التقليدية مما يعتبر أحد العوامل الأساسية التي دفعت نحو التحول الرقمي في العديد من المجالات.

ففي المعاملات التقليدية، يتطلب الأمر استخدام كميات كبيرة من الورق لطباعة المستندات والمعاملات، أما في المعاملات الإلكترونية، فإنها تتم بالكامل بشكل رقمي، مما يلغي الحاجة إلى الورق ويساهم في توفير تكاليف الطباعة والتخزين، كما أن في المعاملات التقليدية، إرسال المستندات يتطلب البريد التقليدي، وهو ما يستغرق وقتاً ويكلف مالاً، أما في المعاملات الإلكترونية، يتم إرسال المستندات عبر الإنترنت فورياً وبدون أي تكلفة إضافية للبريد.

إن إتمام المعاملات يدوياً غالباً ما يتطلب وقتاً أطول للمعالجة والموافقة، بينما تتم المعاملات الإلكترونية بسرعة أكبر، مما يقلل من التأخيرات الزمنية وتكاليف العمل الإضافي.

تجدر الإشارة إلى أن تعزيز الاقتصاد الرقمي من خلال المعاملات الإلكترونية هو موضوع مهم في الاقتصاد الحديث، حيث أسهمت المعاملات الإلكترونية في دفع عجلة الاقتصاد الرقمي وتشجيع الابتكار في مجالات مثل التجارة الإلكترونية والخدمات المالية الرقمية، هذا التحول إلى المعاملات الرقمية يساعد على خلق بيئة اقتصادية أكثر كفاءة وابتكارًا.

[1] Johnson, William, E-Commerce and Cost Reduction Strategies, McGraw-Hill, United Kingdom, 2018, P 58.

فالمعاملات الإلكترونية أصبحت العمود الفقري للتجارة الإلكترونية، حيث سهلت هذه المعاملات عمليات البيع والشراء بين الشركات والمستهلكين عبر الإنترنت. هذا التحول إلى التجارة الرقمية أدى إلى خفض التكاليف التشغيلية وتسريع العمليات اللوجستية، مما عزز من قدرة الشركات على النمو السريع[1].

إن الخدمات المالية الرقمية تعد واحدة من المجالات التي شهدت نمواً كبيراً بفضل التحول نحو المعاملات الإلكترونية، من خلال الابتكارات في أنظمة الدفع الرقمي، والمحافظ الإلكترونية، والعملات الرقمية المشفرة مثل "البيتكوين"، فقد أسهمت في توسيع نطاق الشمول المالي وزيادة الوصول إلى الخدمات المالية.

المطلب الثاني: تعريف المعاملات الالكترونية وخصائصها

في ظل التطور التكنولوجي السريع والتحول الرقمي الذي يشهده العالم اليوم، أصبحت المعاملات الإلكترونية جزءاً أساسياً من الحياة اليومية للأفراد والشركات، إذ يعتمد هذا النوع من المعاملات على استخدام الوسائط الإلكترونية، مثل الإنترنت والشبكات الرقمية، لإجراء مختلف العمليات التجارية والخدمية، مما يوفر السرعة والمرونة ويخفض التكلفة مقارنة بالطرق التقليدية، كما تنطوي المعاملات الإلكترونية على العديد من الخصائص التي تميزها، مثل قابلية التوسع على نطاق عالمي وسهولة الوصول، ولكنها في الوقت نفسه تطرح تحديات قانونية تتعلق بالأمان، وحماية البيانات، وحقوق الأطراف المتعاقدة، مما جعل التشريعات الحديثة، بما في ذلك التشريع الفرنسي، تولي اهتماماً كبيراً لتنظيم هذا المجال وضمان حقوق المستخدمين.

الفرع الأول: تعريف المعاملات الالكترونية

تتعدد التعاريف الخاصة بالمعاملات الإلكترونية تبعًا للسياق القانوني والتقني الذي تُطرح فيه، فبينما يُنظر إليها في الجانب القانوني كعقود تتم عبر الوسائط الإلكترونية وتتطلب اعترافًا رسميًا بصحتها، يراها الخبراء التقنيون كسلسلة من التبادلات الرقمية التي تعتمد على تكنولوجيا المعلومات والاتصالات.

[1] يوسف الخليفي، الاقتصاد الرقمي: الفرص والتحديات، دار الفكر العربي، مصر، 2019، ص 215-218.

أولا: تعريف المعاملات الالكترونية في التشريع الفرنسي

يعرف التشريع الفرنسي هذه المعاملات من خلال قوانين عديدة، أبرزها القانون رقم: 2004/575 الصادر في 21 يونيو 2004 والمعروف باسم "قانون الثقة في الاقتصاد الرقمي (Loi pour la confiance dans l'économie numérique)[1]، هذا القانون يتضمن إطاراً عاماً لتنظيم المعاملات الإلكترونية ويحدد مسؤوليات الأطراف المتعاملة.

التشريع الفرنسي يستمد الكثير من عناصره القانونية من التشريعات الأوروبية، خصوصاً تلك المتعلقة بالتجارة الإلكترونية. من أبرز التشريعات الأوروبية المؤثرة في هذا المجال، توجيه الاتحاد الأوروبي EC 31/2000/الصادر في 8 يونيو 2000، والذي تم تضمينه في القانون الفرنسي لضمان تنسيق السياسات الأوروبية في مجال التجارة الإلكترونية[2].

وبذلك فقد عرف المشرع الفرنسي المعاملات الإلكترونية بموجب القانون 2004/575 بأنها جميع العمليات التي تتم عبر الوسائط الإلكترونية مثل الإنترنت والشبكات الرقمية، وتشمل إبرام العقود التجارية، تقديم الخدمات، البيع والشراء، وتحويل الأموال، يتضمن هذا المفهوم تبادل البيانات والمعلومات بشكل إلكتروني بين الأطراف المعنية، سواء كانت أفرادًا أو شركات أو هيئات حكومية، وتتم هذه العمليات غالبًا دون الحاجة إلى وجود مادي للأطراف المتعاملة.

ثانيا: تعريف المعاملات الإلكترونية في التشريع الأمريكي

المعاملات الإلكترونية في التشريع الأمريكي تتمحور حول القوانين والتشريعات التي تنظم العمليات التجارية والمالية التي تتم عبر الإنترنت. هذه المعاملات تشمل شراء السلع والخدمات،

---

[1] القانون رقم: 2004/575 الصادر في 21 يونيو 2004، والمعروف باسم "قانون الثقة في الاقتصاد الرقمي (Loi pour la confiance dans l'économie numérique)"، هو قانون فرنسي يهدف إلى تنظيم الأنشطة الإلكترونية والاقتصادية الرقمية. جاء هذا القانون استجابة للنمو المتسارع في استخدام الإنترنت والوسائل الرقمية في الحياة اليومية، ويهدف إلى تعزيز الثقة والأمان في استخدام التقنيات الرقمية. يركز القانون على تنظيم التجارة الإلكترونية، حماية البيانات الشخصية، وضمان الأمن في المعاملات الرقمية:
Loi n° 2004-575 du 21 juin 2004, Loi pour la confiance dans l'économie numérique, Journal Officiel de la République Française, France, 2004.

[2] Thomas Roche, L'impact des directives européennes sur le droit français des transactions électroniques, Éditions LGDJ, France, 2003, P 92.

التحويلات المالية، العقود الإلكترونية، وحماية البيانات والمعلومات الشخصية. يعتمد التشريع الأمريكي على عدة قوانين لتنظيم هذه المعاملات، مع التأكيد على حماية المستهلك وضمان أمن المعاملات.

يعد القانون الموحد للمعاملات الإلكترونية (UETA) واحدًا من أهم التشريعات التي أُقرت لتنظيم المعاملات الإلكترونية في الولايات المتحدة، يهدف هذا القانون إلى ضمان أن العقود المبرمة إلكترونيًا تمتلك نفس الصلاحية القانونية كالعقود التقليدية المكتوبة على الورق[1].

أما قانون التوقيع الإلكتروني في التجارة العالمية والمحلية(E-SIGN Act) الصادر سنة 2000، فهو يعتبر من القوانين الأساسية التي تمنح العقود الإلكترونية والتوقيعات الإلكترونية نفس الحماية القانونية التي تتمتع بها العقود الورقية، الهدف من هذا القانون هو تعزيز الثقة في المعاملات الإلكترونية وتوفير إطار قانوني يتعامل مع التحديات المترتبة على التجارة عبر الإنترنت[2].

ثالثا: تعريف المعاملات الإلكترونية في التشريع المصري

في التشريع المصري، عُرفت المعاملات الإلكترونية كجزء من الجهود التشريعية لتنظيم الاقتصاد الرقمي وحماية الأطراف المتعاملة عبر الإنترنت، فقد كان هذا ضروريًا نظرًا للتوسع الكبير في استخدام التكنولوجيا والتعاملات التجارية الإلكترونية، نجد أن التعريف والتنظيم جاء بشكل أساسي عبر عدد من القوانين التي وُضعت لضمان سلامة التعاملات الإلكترونية ومصداقيتها.

تُعرَّف المعاملات الإلكترونية في التشريع المصري بأنها "أي عملية تبادل أو تفاعل أو تعامل تتم باستخدام الوسائل الإلكترونية بين الأطراف المختلفة، وتشمل العقود والاتفاقات والتوقيعات والخدمات والمشتريات التي تتم عبر الإنترنت أو من خلال وسائل الاتصال الإلكترونية"، تركز التشريعات المصرية على تنظيم هذه التعاملات لضمان الحماية القانونية لمستخدمي الوسائل الإلكترونية، سواء أكانوا أفرادًا أو شركات.

[1] National Conference of Commissioners on Uniform State Laws. Uniform Electronic Transactions Act (UETA). 1999. Available online at : https://www.lawschool.cornell.edu/.

[2] U.S. Congress. Electronic Signatures in Global and National Commerce Act (E-SIGN Act). Washington, DC: U.S. Library of Congress, 2000.

أحد الركائز الأساسية لتنظيم المعاملات الإلكترونية في مصر هو قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات رقم 15 لسنة 2004، حيث يُعرِّف التوقيع الإلكتروني ويحدد الشروط القانونية اللازمة لاعتماده كوسيلة لإثبات العقود والمعاملات التي تتم عبر الإنترنت[1].

رابعا: تعريف المعاملات الإلكترونية في التشريع الإماراتي

المعاملات الإلكترونية في القانون الإماراتي تُعرف على أنها كل ما يتعلق بالتواصل وتبادل المعلومات إلكترونيًا، بما في ذلك العقود والوثائق والمستندات التي تتم من خلال وسائل الاتصال الإلكترونية. هذا التعريف يشمل العقود التجارية، والتوقيعات الإلكترونية، والوثائق الرقمية، والمدفوعات عبر الإنترنت[2].

المشرع الإماراتي قام بتعريف المعاملات الإلكترونية في القانون الاتحادي رقم (1) لسنة 2006 بشأن المعاملات والتجارة الإلكترونية، هذا القانون يُعتبر الإطار القانوني الرئيسي لتنظيم المعاملات الإلكترونية في دولة الإمارات العربية المتحدة[3].

وفقًا لهذا القانون، تعرف المعاملات الإلكترونية بأنها كل تعامل أو عقد يتم إبرامه أو تنفيذه كلياً أو جزئياً عبر وسيلة إلكترونية، بما في ذلك تبادل البيانات الإلكترونية والتوقيعات الإلكترونية واستخدام الوثائق الإلكترونية في سياق المعاملات التجارية.

خامسا: تعريف المعاملات الإلكترونية في التشريع الجزائري

المعاملات الإلكترونية تُعتبر أحد الموضوعات الرئيسية في القانون الجزائري ضمن إطار التطور التكنولوجي الذي يشهده العالم اليوم. تتعلق المعاملات الإلكترونية بكل العمليات التجارية والخدماتية

---

[1] قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، القانون رقم 15 لسنة 2004، مطبعة الهيئة المصرية العامة للكتاب، مصر ، 2004، المادة 1.

[2] محمد علي القيسي، قانون المعاملات والتجارة الإلكترونية في دولة الإمارات العربية المتحدة، دار النهضة العربية، الإمارات العربية المتحدة، 2015، ص 45-50.

[3] القانون الاتحادي رقم (1) لسنة 2006 بشأن المعاملات والتجارة الإلكترونية، الصادر بتاريخ: 2006/01/30، الجريدة الرسمية لدولة الإمارات العربية المتحدة.

التي تتم عبر الإنترنت أو الوسائل الرقمية الأخرى، وقد اهتم المشرع الجزائري بوضع تنظيم قانوني لهذه المعاملات لضمان سلامتها وحماية الأطراف المتعاقدة فيها.

في الجزائر، تم تطوير مجموعة من القوانين التي تُعنى بتنظيم المعاملات الإلكترونية، وعلى رأسها القانون رقم 05/18 الصادر في 2018[1]، والذي يعتبر الأساس القانوني لتنظيم التجارة الإلكترونية وحماية البيانات والمستهلكين. وفقاً لهذا القانون، تُعرَّف المعاملات الإلكترونية على أنها أي تبادل للبيانات أو الخدمات يتم باستخدام الوسائل الإلكترونية[2].

المشرع الجزائري وضع تعريفاً واضحاً للمعاملات الإلكترونية في المادة 3 القانون رقم 05/18 الصادر بتاريخ 10 مايو 2018 والمتعلق بالتجارة الإلكترونية، والذي يهدف إلى تنظيم المعاملات الإلكترونية وحماية الأطراف المتعاقدة في البيئة الرقمية، سواء كانوا مستهلكين أو مزودين للخدمات، بحيث عرفت المادة المعاملات الالكترونية بأنها كل نشاط تجاري يتم عن طريق استخدام وسائل الاتصال الإلكترونية، بما في ذلك العقود المبرمة إلكترونيًا، الخدمات المقدمة عبر الإنترنت، وعروض البيع أو التبادل التي تتم باستخدام الوسائل الإلكترونية.

وقد عالج هذا القانون مجموعة من الجوانب التي تخص المعاملات الإلكترونية، منها:

1. الترخيص لممارسة التجارة الإلكترونية.
2. حماية البيانات الشخصية.
3. ضمان حقوق المستهلك الإلكتروني.
4. الإجراءات المتعلقة بالعقود الإلكترونية وتأكيد صلاحيتها.
5. الالتزامات المفروضة على الموردين في البيئة الرقمية.

[1] قانون رقم 05/18 مؤرخ في: 25 شعبان 1439هـ الموافق ل 10 مايو 2018، يتعلق بالتجارة الالكترونية، ج.ر عدد 28، مؤرخة في: 30 شعبان 1439هـ الموافق ل 16 مايو 2018.

[2] محمد بن علي، تحليل قانون 18-05: التجارة الإلكترونية في الجزائر، مجلة القانون والمجتمع، جامعة وهران2، الجزائر، 2019، ص 23-24.

الفرع الثاني: خصائص المعاملات الالكترونية

تتميز المعاملات الإلكترونية بعدة خصائص رئيسية تجعلها متفوقة على المعاملات التقليدية، منها: **السرعة والكفاءة**، حيث يمكن إتمام المعاملات بسرعة كبيرة عبر الإنترنت؛ **التكلفة المنخفضة** بفضل تقليل الحاجة إلى الأوراق والوسطاء؛ **الأمان**، من خلال استخدام التوقيع الإلكتروني وتقنيات التشفير؛ **الوصول العالمي**، حيث يمكن تنفيذ المعاملات من أي مكان في العالم؛ و**المرونة وسهولة الاستخدام**، مما يسمح بإتمام العمليات من أي جهاز متصل بالإنترنت في أي وقت.

أولا: السرعة في إنجاز المعاملات

تعتبر السرعة واحدة من أبرز خصائص المعاملات الإلكترونية، حيث يمكن إتمام العمليات التجارية والدفع الإلكتروني في غضون ثوانٍ قليلة. هذا يختلف عن المعاملات التقليدية التي قد تتطلب وقتًا أطول بسبب البنية التحتية المادية، كما تعزز سرعة المعاملات الكفاءة وتسمح بتنفيذ عدد أكبر من المعاملات في وقت أقل.

إن المعاملات الإلكترونية أصبحت أسرع وأكثر فعالية مقارنة بالمعاملات الالكترونية، هذه الأخيرة قد تستغرق فيها المعاملات أيامًا أو حتى أسابيع لإتمامها نظرًا لضرورة نقل المستندات أو الأموال فعليًا، ومن ناحية أخرى، يمكن إتمام المعاملات الإلكترونية في غضون بضع دقائق أو حتى ثوانٍ، وذلك لأن البنية الأساسية الإلكترونية تتيح نقل البيانات والدفع الفوري.

ثانيا: الوصول العالمي

من خلال الإنترنت، يمكن لأي شخص أو مؤسسة القيام بمعاملات تجارية مع طرف آخر في أي مكان في العالم، هذه الميزة توفر فرصًا للشركات للوصول إلى أسواق جديدة دون الحاجة إلى وجود مادي في تلك الأسواق[1].

إن المعاملات الإلكترونية تمكن الأفراد والشركات من الوصول بسهولة إلى الأسواق العالمية، وهذا يختلف كثيراً عن المعاملات التقليدية التي غالباً ما تكون محدودة بالقيود الجغرافية، وهذا يعني

[1] أمين الغزالي، التجارة الإلكترونية والعولمة: دراسة تحليلية، دار الجسور، الجزائر، 2020، ص 46.

أن الشركة التي تتعامل إلكترونياً تستطيع الوصول إلى العملاء والشركاء التجاريين من أي جزء من العالم دون الحاجة إلى التواجد فعلياً.

ثالثا: التكلفة المنخفضة

تتميز المعاملات الإلكترونية بتكاليف أقل مقارنة بالمعاملات التقليدية. فعلى سبيل المثال، تكاليف البريد والطباعة والنقل غير موجودة في التعاملات الإلكترونية. بالإضافة إلى ذلك، تقليل الاعتماد على الوسطاء في العمليات الإلكترونية يؤدي إلى تقليص التكاليف[1].

إن المعاملات الإلكترونية أوفر عمومًا من المعاملات التقليدية لأنها لا تتطلب الكثير من الأعمال الورقية أو اللوجستيات المعقدة، مما يؤدي بالتالي إلى خفض كبير في تكاليف المعاملات. وعلاوة على ذلك، فإن خفض متطلبات الوكلاء أو الوسطاء يقلل من الرسوم الإضافية التي يتم فرضها عادةً في المعاملات التقليدية.

رابعا: الأمان والتوقيع الإلكتروني

واحدة من أهم خصائص المعاملات الإلكترونية هي الأمان الذي توفره. يتم استخدام تقنيات التشفير المتقدمة لحماية البيانات والمعلومات الشخصية للمستخدمين. بالإضافة إلى ذلك، يتم الاعتماد على التوقيع الإلكتروني لضمان صحة وسلامة المعاملات[2].

في المعاملات الإلكترونية، يمكن الحصول على الاعتماد على التوثيق الرقمي والتوقيع الإلكتروني لضمان صحة المعاملات، وهذا يؤدي في الواقع إلى مستوى أعلى من الأمان مقارنة بالمعاملات التقليدية التي قد تكون صالحة فقط من خلال التوقيع اليدوي على الورق؛ حيث يمكن تزوير الوثيقة الورقية أو فقدها.

يسمح التوثيق الرقمي والتوقيعات الإلكترونية من توفير مزايا عديدة منها: التحقق من الهوية، سلامة البيانات، الأمان، وقابلية التتبع بحيث يمكن تتبع تفاصيل المعاملة، بما في ذلك الوقت والتاريخ والجهة الموقعة.

[1] Philip Kotler, Marketing in the Digital Age, Pearson, USA, 2020, P 34.

[2] سامي بن زيد، أمن المعلومات في التجارة الإلكترونية، دار الحافظ، الجزائر، 2020، ص 78.

خامسا: المرونة وسهولة الاستخدام

المعاملات الإلكترونية تتميز بسهولة الاستخدام والمرونة في الوصول، سواء كان ذلك من خلال تطبيقات الهواتف المحمولة أو عبر متصفحات الإنترنت، هذا يسهل على الأفراد والشركات إتمام المعاملات في أي وقت ومن أي مكان[1].

يمكن للمستخدمين إتمام المعاملات ببضع نقرات على أجهزة الحاسوب أو الهواتف الذكية، مما يوفر الوقت والجهد مقارنة بالطرق التقليدية، كما أنه بفضل الإنترنت، يمكن للمستخدمين الوصول إلى الخدمات الإلكترونية في أي وقت ومن أي مكان، دون الحاجة إلى الحضور الشخصي أو التقيد بساعات العمل.

سادسا: قابلية التتبع والشفافية

من خصائص المعاملات الإلكترونية أنها توفر سجلاً رقمياً لكل خطوة في العملية، هذا يمكن الشركات والأفراد من تتبع معاملاتهم بسهولة، ويضمن مستوى عالٍ من الشفافية في العمليات.

هذه الخاصية تتيح للشركات والأفراد إمكانية تتبع معاملاتهم بكل سهولة ودقة، هذا السجل الرقمي يضمن تسجيل جميع العمليات بدءاً من التحويلات المالية وصولاً إلى تأكيد الاستلام أو التسليم، مما يسهم في تسهيل مراجعة البيانات عند الحاجة، بفضل هذا السجل الرقمي، يمكن للشركات مراقبة حركة التدفقات المالية أو اللوجستية بشكل مستمر، كما يمكن للأفراد متابعة سير معاملاتهم الشخصية عبر منصات إلكترونية مخصصة.

بالإضافة إلى ذلك، هذا النوع من التوثيق الرقمي يعزز من مستوى الشفافية في العمليات، وجود سجل رقمي لكل خطوة من شأنه أن يقلل من الغموض أو الشكوك حول العملية، على سبيل المثال، في حال وقوع نزاع بين طرفين، يمكن الرجوع إلى هذه السجلات لتحديد المسؤولية أو تصحيح أي أخطاء محتملة، كما أن الشفافية التي يضمنها هذا النظام الرقمي تسهم في بناء الثقة بين المستخدمين والمؤسسات، ما يؤدي إلى تحسين التجربة الإجمالية للمستخدم وتعزيز الثقة في النظم الإلكترونية.

[1] Amy Webb, The Signals Are Talking: Why Today's Fringe is Tomorrow's Mainstream, PublicAffairs, USA, 2018, P 112.

المبحث الثاني: الإطار العملي للمعاملات الالكترونية (الأنواع – الآثار)

يعدّ الإطار العملي للمعاملات الإلكترونية محورًا أساسيًا في فهم تطبيقاتها المتنوعة وآثارها على مختلف المجالات. تعتمد المعاملات الإلكترونية على عدة أنواع رئيسية (المطلب الأول)، كما تحدث المعاملات الإلكترونية تأثيرات اقتصادية كبيرة مثل تحسين الكفاءة وتقليل التكاليف التشغيلية للشركات، وزيادة القدرة على الوصول إلى الأسواق العالمية (المطلب الثاني).

المطلب الأول: أنواع المعاملات الالكترونية

لقد تنوعت المعاملات الإلكترونية لتحقيق أهداف متنوعة تلبي احتياجات المتعاملين بطرق سريعة وفعالة، وذلك اعتماداً على وسائل قانونية وتقنية متطورة تضمن سلامة هذه المعاملات وسهولة إتمامها. من بين الأنواع المختلفة للمعاملات الإلكترونية، نذكر على سبيل المثال: الشيك الالكتروني والمقاصة الالكترونية، والبطاقات البنكية والأوراق التجارية الالكترونية.

الفرع الأول: الشيك الالكتروني والمقاصة الالكترونية

يمثل الشيك الإلكتروني المقاصة الإلكترونية تطوراً حديثاً في التعاملات المالية الرقمية، لذلك سنتعرض خلال هذا الفرع إلى مفهوم وخصائص كل منهما.

أولا: الشيك الالكتروني

الشيك الإلكتروني هو نسخة رقمية من الشيك التقليدي يُستخدم لإجراء المدفوعات عبر الإنترنت بسهولة وأمان دون الحاجة إلى أوراق فعلية، فهو بمثابة المكافئ الرقمي للشيكات الورقية التقليدية، ويُستخدم كوسيلة دفع حديثة في العديد من المجالات مثل التجارة الإلكترونية.

1/- تعريف الشيك الالكتروني

الشيك الإلكتروني هو رسالة إلكترونية يتم إرسالها بشكل آمن وموثق من قبل جهة إصدار الشيك إلى متلقي الشيك للموافقة عليها وإرسالها عبر الإنترنت إلى البنك لتقديمها. يقوم البنك بإيداع قيمة الشيك في حساب المتلقي، ثم يلغي الشيك ويعيده إلكترونيًا إلى المتلقي كدليل على الدفع.

أصبح المشرع الجزائري يضمن إمكانية استعمال الشيكات الإلكترونية في المعاملات بين الأفراد (سواء كانت معاملات تجارية أو اجتماعية)، فهو في الواقع مؤشر إيجابي على القفزة النوعية فيما يتعلق بالنظام الذي يحكم استخدام مثل هذه التقنيات الحديثة من خلال الشبكات المفتوحة[1]. ذلك أن المشرع الجزائري لم يأت بتعريف واضح للشيك الإلكتروني، على خلاف ما حدث في عدد من التشريعات الأخرى، مثل التشريعات الأردنية واليمنية والسودانية التي عرفته على سبيل المثال بأنه "ورقة مالية أو تجارية قابلة للتداول إلكترونياً". والواقع أن هناك تشريعات قليلة أخرى أخذت على عاتقها تحديد التعريف الأضيق للشيكات الورقية، مثل القانون الفرنسي الصادر في 14 يونيو 1865، والقانون الاتحادي رقم 18 لسنة 1993 لدولة الإمارات العربية المتحدة بشأن المعاملات التجارية في المادة 483، والقانون الأردني رقم 12 الصادر في 14 يونيو 1966 بشأن المادة 123.

تعتمد الأطر القانونية للشيك الإلكتروني على القوانين التي تُنظم المعاملات الإلكترونية، مثل قوانين التوقيعات الإلكترونية والتجارة الإلكترونية. في معظم البلدان، يُعتبر الشيك الإلكتروني قانونياً بشرط أن يتم توقيعه إلكترونياً باستخدام تقنيات التوقيع الرقمي أو غيرها من وسائل التحقق الإلكترونية[2]. فالتوقيع الإلكتروني يُعد مكوناً أساسياً لإضفاء الشرعية على المعاملات الإلكترونية بما في ذلك الشيكات.

2/- خصائص الشيكات الالكترونية

من المزايا الرئيسية للشيك الإلكتروني تقليل الوقت اللازم لمعالجة الشيكات التقليدية الورقية، بالإضافة إلى تقليل تكلفة المعاملات الورقية[3]. فاستخدام الشيك الإلكتروني يوفر على البنوك تكاليف ضخمة تتعلق بطباعة وتوزيع الشيكات الورقية ويقلل من خطر التزوير.

[1] خرباش جميلة، الشيك الإلكتروني أداة وفاء عن بعد في التجارة الإلكترونية، مجلة البيبان للدراسات القانونية والسياسية، المجلد3 العدد1، 2018، ص 183.

[2] Jean Smith, E-commerce Law : Digital Transactions, Cambridge University Press, U.K, 2019, P 120.

[3] Sarah Wilson. "The Benefits of E-Checks in Modern Banking." *Journal of Financial Innovation*, vol. 15, no. 3, 2022, p. 204.

لكن على الرغم من المزايا الكبيرة، إلا أن هناك تحديات تتعلق بالأمان والثقة، على سبيل المثال، قد يواجه المستخدمون مخاطر تتعلق بسرقة الهوية أو اختراق البيانات[1]، بحيث أن استخدام الشيكات الإلكترونية يتطلب استثماراً كبيراً في البنية التحتية الأمنية لحماية المعلومات المالية الحساسة.

ثانيا: المقاصة الالكترونية

تعد المقاصة الإلكترونية واحدة من الوسائل الحديثة لتسوية المعاملات المالية بين البنوك والمؤسسات المالية، تهدف إلى تسريع المعاملات المالية وتقليل التكاليف المرتبطة بها، حيث تمثل بديلاً عن الأنظمة التقليدية للمقاصة الورقية، وقد أصبحت المقاصة الإلكترونية ضرورة في العالم الرقمي الحالي الذي يعتمد على التكنولوجيا المتطورة لتحسين كفاءة النظام المالي.

1/- تعريف المقاصة الالكترونية

المقاصة الإلكترونية تسهل تسوية الشيكات والمعاملات المالية بين البنوك بشكل سريع وفعال، حيث يتم تبادل البيانات المالية إلكترونياً بدلاً من الأوراق، مما يسرع عملية التحصيل ويزيد من دقة وكفاءة النظام المصرفي.

المقاصة الإلكترونية هي عملية تبادل التعليمات المالية بين البنوك أو المؤسسات المالية باستخدام أنظمة إلكترونية تقوم بتسوية المدفوعات والمطالبات بينها. تعتمد هذه العملية على استخدام تقنيات متطورة للحفاظ على الأمان والسرعة في تسوية المعاملات المالية، تعد من أهم الابتكارات في التعاملات المالية الحديثة، حيث تعمل على تقليل الوقت والتكلفة وزيادة الكفاءة. وتتم هذه العملية من خلال أنظمة إلكترونية متقدمة تضمن الأمان وسرعة التنفيذ.

هناك العديد من الأنظمة المستخدمة في المقاصة الإلكترونية، من بينها:

أ/- أنظمة المقاصة الآنية :(RTGS) حيث يتم تسوية المعاملات في الوقت الفعلي، ما يقلل من مخاطر التأخير.

[1] Linda Davis. "Cybersecurity Challenges in E-Check Systems." Cybersecurity Journal, vol. 8, no. 4, 2020, p. 312.

ب/- أنظمة المقاصة الصافية :(Net Settlement Systems) تعتمد على تجميع المعاملات وتسويتها في نهاية اليوم[1].

إن الأنظمة الآنية تسهم بشكل كبير في تحسين السيولة المالية داخل الأسواق، حيث يتم تسوية المدفوعات على الفور، مما يعزز الثقة بين المؤسسات المالية.

تجدر الإشارة إلى أن المقاصة الإلكترونية تسهم في تعزيز الاقتصاد من خلال تسهيل حركة الأموال بشكل أسرع وأكثر أمانًا، إن المقاصة الإلكترونية تقلل من التكاليف التشغيلية وتساعد في تحسين السيولة النقدية بين البنوك، مما يزيد من كفاءة النظام المالي.

2/- التحديات والمخاطر المرتبطة بالمقاصة الإلكترونية

على الرغم من فوائد المقاصة الإلكترونية، إلا أن هناك تحديات كبيرة تواجه المؤسسات المالية، بما في ذلك مخاطر الأمن السيبراني والاحتيال، فتزايد الهجمات الإلكترونية في السنوات الأخيرة جعل البنوك والمؤسسات المالية بحاجة إلى اتخاذ تدابير وقائية إضافية لحماية أنظمتها من الاختراق.

أحد أبرز المخاطر التي تواجه أنظمة المقاصة الإلكترونية هو الأمن السيبراني، مع الاعتماد المتزايد على التكنولوجيا، تتزايد أيضًا الهجمات السيبرانية التي تستهدف اختراق الأنظمة المالية وسرقة البيانات فقد ارتفعت الهجمات الإلكترونية على البنوك والمؤسسات المالية بشكل ملحوظ في السنوات الأخيرة، مما جعل الحاجة إلى تقوية أنظمة الأمن السيبراني أمرًا بالغ الأهمية.

نظرًا لاختلاف التشريعات والقوانين بين الدول، تواجه أنظمة المقاصة الإلكترونية تحديات في التوافق مع هذه القوانين، خاصة فيما يتعلق بمعايير مكافحة غسل الأموال وتمويل الإرهاب. فالمؤسسات المالية تحتاج إلى الالتزام بالتشريعات الوطنية والدولية لضمان أن عمليات المقاصة تتوافق مع المتطلبات القانونية والتنظيمية[2].

---

[1] سالم عبد العزيز، "تحليل كفاءة أنظمة الدفع الإلكترونية"، المجلة العربية للدراسات المالية، المجلد 8، العدد 3، القاهرة، مصر، 2020، ص. 98.

[2] خالد أحمد، "التحديات القانونية لأنظمة المقاصة الإلكترونية"، المجلة الدولية للقانون المالي، المجلد 5، العدد 2، دار النشر القانونية، عمان، الأردن، 2020، ص. 112.

الاعتماد الكلي على التكنولوجيا قد يؤدي إلى مشاكل تشغيلية في حال حدوث أعطال تقنية أو فشل في الأنظمة، فقد تتعرض أنظمة المقاصة الإلكترونية لأعطال فنية تؤدي إلى تأخير أو توقف المعاملات، مما يسبب خسائر مالية أو تأثير سلبي على سمعة المؤسسات المالية بحيث يؤدي هذا الاعتماد الكبير على التكنولوجيا إلى زيادة حساسية النظام أمام المخاطر التشغيلية.

التحدي الآخر هو الحفاظ على مستوى عالٍ من الشفافية والثقة بين الأطراف المتعاملة، عدم الشفافية في بعض الأحيان، سواء في العمليات أو التكاليف، قد يؤدي إلى تآكل الثقة بين البنوك والمؤسسات المالية[1]. إن البنوك تحتاج إلى تحسين الشفافية في أنظمة المقاصة الإلكترونية لضمان كفاءة العمليات وزيادة الثقة بين المشاركين في السوق.

المقاصة الإلكترونية تعتمد بشكل كبير على توفير السيولة الفورية لتسوية المعاملات. عدم توفر السيولة الكافية في أي وقت قد يؤدي إلى تعطل عملية المقاصة، مما يؤثر سلبًا على الأنظمة المالية. قد تؤدي التقلبات في السيولة إلى زيادة الضغط على المؤسسات المالية، وبالتالي يتعين عليها تبني استراتيجيات فعالة لإدارة السيولة.

تعتبر المقاصة الإلكترونية من الابتكارات الهامة التي أسهمت في تحسين كفاءة النظام المالي وتقليل التكاليف وزيادة سرعة المعاملات. ومع ذلك، يتعين على المؤسسات المالية اتخاذ التدابير اللازمة لحماية هذه الأنظمة من المخاطر المتزايدة المتعلقة بالأمن السيبراني.

الفرع الثاني: البطاقات البنكية والأوراق التجارية الالكترونية

مع التقدم السريع في التكنولوجيا وتزايد الاعتماد على الحلول الرقمية في المعاملات المالية، أصبحت البطاقات البنكية والأوراق التجارية الإلكترونية جزءًا لا يتجزأ من النظام المالي الحديث. تقدم البطاقات البنكية، مثل بطاقات الائتمان والخصم، وسيلة مريحة وآمنة لإجراء المدفوعات اليومية، سواء عبر الإنترنت أو في نقاط البيع الفعلية. من ناحية أخرى، تُسهم الأوراق التجارية الإلكترونية، مثل الشيكات الإلكترونية والحوالات، في تبسيط وتسريع عمليات الدفع والتسوية بين المؤسسات المالية، مما

[1] هشام عبد الحليم، "الثقة والشفافية في أنظمة المقاصة الإلكترونية"، مجلة الدراسات المصرفية، المجلد 6، العدد 1، المعهد العربي للدراسات المالية والمصرفية، القاهرة، مصر، 2020، ص. 45.

يعزز الكفاءة والشفافية في الاقتصاد الرقمي. هذا التطور في وسائل الدفع يساهم بشكل كبير في تقليل استخدام النقد وتحسين التدفقات المالية بشكل أكثر أمانًا وسرعة.

أولا: البطاقات البنكية

البطاقات البنكية هي وسيلة دفع إلكترونية تسمح لحاملها بإجراء معاملات مالية دون الحاجة إلى استخدام النقود الورقية. تطورت هذه البطاقات منذ اختراعها لتشمل أنواعًا متعددة مثل بطاقات الخصم، بطاقات الائتمان، والبطاقات المدفوعة مسبقًا. يعتمد عمل البطاقات البنكية على شبكة معقدة من الأنظمة البنكية الإلكترونية التي تضمن سلامة المعاملات.

1/- مفهوم البطاقات البنكية

تُعرف البطاقة البنكية بأنها بطاقة بلاستيكية تحتوي على شريط مغناطيسي أو رقاقة إلكترونية تخزن معلومات حساب حامل البطاقة في البنك. يستخدم حامل البطاقة هذه المعلومات لإجراء عمليات دفع إلكترونية أو سحب نقدي من أجهزة الصراف الآلي.

وتنقسم البطاقات البنكية إلى عدة أنواع وفقًا لنوع الحساب المصرفي والغرض من الاستخدام، أبرز أنواعها تشمل:

أ/- بطاقة الخصم :يتم خصم قيمة المشتريات مباشرة من حساب حامل البطاقة.

بطاقة الخصم هي واحدة من الأدوات البنكية الإلكترونية الشائعة التي تتيح للمستخدمين الوصول إلى أموالهم المخزنة في حساباتهم البنكية بطريقة مباشرة، سواء لسحب النقود من الصرافات الآلية أو لإجراء عمليات شراء إلكترونية. تعمل بطاقة الخصم كوسيلة دفع مريحة حيث يتم خصم المبلغ مباشرة من رصيد الحساب الجاري للحامل.

حامل بطاقة الخصم هو الشخص الذي يمتلك الحساب المصرفي المرتبط بالبطاقة ويكون له الحق في استخدامها لإجراء عمليات السحب أو الشراء. يتم إصدار البطاقة بناءً على طلب حامل الحساب وتكون مرتبطة بحسابه البنكي. يُعتبر حامل البطاقة مسؤولًا عن جميع العمليات المالية التي تتم باستخدام البطاقة، سواء كانت معاملات سحب نقدي أو شراء من المتاجر أو الدفع عبر الإنترنت.

حامل البطاقة له دور أساسي في إدارة الحساب المصرفي، حيث يمكنه الوصول إلى الرصيد في أي وقت وسحب الأموال أو الدفع إلكترونياً. كما أنه مسؤول عن الحفاظ على أمان البطاقة وبياناتها، بما في ذلك الرقم السري .(PIN) يُعد حامل البطاقة هو الشخص الوحيد المخول باستخدام البطاقة، وفي حال فقدان البطاقة، يجب عليه الإبلاغ الفوري للبنك لتعليق الحساب والحد من أي استخدام غير مصرح به[1].

تتيح بطاقة الخصم لحاملها مجموعة من المزايا، منها القدرة على إجراء عمليات دفع وسحب في أي وقت ومن أي مكان، دون الحاجة إلى حمل النقود. كما توفر حماية مالية حيث يتم رفض المعاملات إذا كان الرصيد غير كافٍ، مما يحمي حامل البطاقة من تكبد ديون غير مرغوبة[2].

من الناحية القانونية، حامل بطاقة الخصم مسؤول عن جميع المعاملات التي تتم باستخدام بطاقته، كما يجب على حامل البطاقة الالتزام بشروط البنك الخاصة باستخدام البطاقة والحفاظ على أمانها، في حال إساءة الاستخدام أو الفقدان، يُطلب من حامل البطاقة الإبلاغ فورًا لتجنب التبعات المالية.

لحماية البطاقة، يجب على حاملها اتباع عدة إجراءات أمنية مثل عدم مشاركة الرقم السري مع أي شخص، وعدم كتابة الرقم السري على البطاقة أو في مكان يسهل الوصول إليه، والامتناع عن إجراء المعاملات من خلال أجهزة غير موثوقة. كما يجب تجنب فتح روابط غير معروفة عند استخدام البطاقة في الشراء الإلكتروني[3].

بطاقة الخصم هي وسيلة مالية مهمة وفعالة لحاملها، حيث تتيح له الوصول المباشر إلى رصيده وإجراء معاملاته اليومية بطريقة مريحة وآمنة. ومع ذلك، فإن المسؤولية الكبرى تقع على عاتق حامل البطاقة في الحفاظ على أمان البطاقة ومتابعة حساباته بانتظام.

---

[1] Brown, P. "Legal Obligations of Debit Cardholders." International Journal of Electronic Transactions Law, Vol. 28, 2018, pp. 112-130.

[2] Doe, A. "Advantages of Debit Cards in Modern Banking." Banking Review Quarterly, Issue 12, 2020, pp. 34-45.

[3] Miller, K. "Security Measures for Debit Cardholders." Electronic Banking Security Journal, Vol. 17, 2021, pp. 55-70.

ب/- بطاقة الائتمان :تتيح لحاملها إجراء مشتريات على أن يتم سداد المبلغ في وقت لاحق، يكون عادةً بفائدة.

بطاقة الائتمان هي أداة دفع إلكترونية تصدرها المؤسسات المالية تتيح لحاملها شراء السلع والخدمات والدفع لاحقًا. وفقًا لـ"مؤسسة النقد العربي السعودي" (ساما)، تُعتبر بطاقة الائتمان عقدًا بين مصدر البطاقة وحاملها، حيث يلتزم المصدر بتقديم حد ائتماني يُستخدم في الشراء، ويلتزم حامل البطاقة بسداد المبلغ المستحق في وقت لاحق[1].

دور ومسؤوليات حامل البطاقة

حامل البطاقة هو الفرد الذي تُصدر له بطاقة الائتمان ويكون مسؤولًا عن استخدامها وسداد المستحقات. من أبرز مسؤولياته:

1. **الالتزام بشروط العقد** :يجب على حامل البطاقة قراءة وفهم شروط وأحكام عقد بطاقة الائتمان لضمان الامتثال للالتزامات المالية.
2. **الحفاظ على سرية المعلومات** :يجب حماية معلومات البطاقة من الوصول غير المصرح به، بما في ذلك رقم البطاقة، تاريخ الانتهاء، ورمز الأمان.
3. **سداد المستحقات في الوقت المحدد** :لتجنب الرسوم الإضافية والفوائد، يجب على حامل البطاقة سداد المبالغ المستحقة في مواعيدها.

تتكون بطاقة الائتمان من العناصر التالية:

- رقم البطاقة :الرقم الفريد المكون من 16 رقمًا يُستخدم لتحديد حساب حامل البطاقة.
- اسم حامل البطاقة :يظهر على البطاقة، وهو الشخص المصرح له باستخدامها.
- تاريخ الانتهاء :يشير إلى مدة صلاحية البطاقة.
- الرمز السري :(CVV) رمز أمان مكون من ثلاثة أرقام مطبوع على ظهر البطاقة[2].

[1] مؤسسة النقد العربي السعودي .(2021) بطاقات الائتمان.

[2] Smith, Julia. "Components of Credit Cards and Their Security Features." Financial Instruments Journal, vol. 58, no. 1, 2019, pp. 112-128.

يمكن أن يستفيد حامل البطاقة من عدة مزايا، مثل استرداد النقد، جمع النقاط والمكافآت على المشتريات، والحصول على خصومات خاصة. بالإضافة إلى ذلك، يمكن أن توفر بطاقات الائتمان مزايا تأمينية على المشتريات أو عند السفر.

ج/- البطاقات المدفوعة مسبقًا :تحتاج إلى إيداع مبالغ مالية مسبقة الاستخدام[1].

البطاقات المدفوعة مسبقًا تعد نوعًا من البطاقات البنكية الإلكترونية التي يمكن لحاملها استخدامها لإجراء معاملات مالية دون الحاجة إلى حساب بنكي مباشر. تتميز بأنها تحتوي على رصيد معين مسبقًا، يتم تعبئته قبل الاستخدام، مما يجعلها خيارًا مثاليًا لأولئك الذين يرغبون في التحكم في نفقاتهم أو لا يرغبون في استخدام بطاقات الائتمان التقليدية.

فهي بطاقات مصرفية تصدرها البنوك أو المؤسسات المالية، ويتم شحنها بمبلغ معين يمكن استخدامه لإجراء عمليات شراء إلكترونية أو سحب نقدي من أجهزة الصراف الآلي. تكون البطاقة منفصلة عن حساب بنكي مباشر، ولكنها مرتبطة به عند الشحن. تستخدم في الغالب لتسهيل التعاملات المالية الإلكترونية والتحكم في النفقات.

تعمل البطاقات المدفوعة مسبقًا من خلال تحميلها بمبلغ نقدي محدد مسبقًا، ثم استخدام هذا الرصيد لإجراء المعاملات. تتم عملية الشحن من خلال عدة طرق مثل التحويل المصرفي، أو الإيداع النقدي، أو التحويل الإلكتروني عبر تطبيقات الهواتف الذكية. بمجرد انتهاء الرصيد، يجب إعادة شحن البطاقة للاستمرار في استخدامها[2].

البطاقات المدفوعة مسبقًا أصبحت أداة شائعة في التجارة الإلكترونية. فهي تتيح للمستخدمين إجراء معاملات إلكترونية بدون الحاجة إلى الإفصاح عن معلومات حساسة مثل أرقام الحسابات البنكية. كما تسهم في حماية الأفراد من الاحتيال في التسوق عبر الإنترنت.

---

[1] يوسف محمد، أنواع البطاقات البنكية واستخداماتها في المعاملات الإلكترونية، دار الندوة، القاهرة، مصر، 2019، ص 78.

[2] "What Is a Prepaid Debit Card and How Does It Work?", The Balance, https://www.thebalancemoney.com/, Accessed September 2023.

تعتبر البطاقات البنكية أداة حيوية في تسهيل المعاملات المالية للأفراد والشركات. فهي تساعد في:

- تقليل الاعتماد على النقود الورقية، مما يقلل من مخاطر السرقة.
- تسهيل عمليات الشراء الإلكترونية عبر الإنترنت.
- توفير الوقت والجهد لحامل البطاقة من خلال عمليات سحب الأموال أو الدفع السريع[1].

2/- التحديات والمخاطر المرتبطة باستخدام البطاقات البنكية

رغم الفوائد العديدة، توجد مخاطر ترتبط باستخدام البطاقات البنكية، مثل:

- **الاحتيال الإلكتروني** :حيث يتم استخدام المعلومات المسروقة من البطاقة للقيام بمعاملات غير شرعية.
- **السرقة الإلكترونية** :يتمكن المتسللون من سرقة المعلومات من الشريط المغناطيسي أو الرقاقة الإلكترونية[2].

مع ازدياد الاعتماد على التجارة الإلكترونية، أصبحت البطاقات البنكية جزءًا لا يتجزأ من هذه العمليات. توفر وسائل دفع آمنة وسهلة للمستهلكين لإجراء عمليات الشراء عبر الإنترنت. يزداد الاعتماد على البطاقات البنكية يومًا بعد يوم، مع التطور المستمر في تقنيات الدفع الرقمي.

البطاقات البنكية تمثل أداة مالية قوية في عالم المعاملات الرقمية. رغم المخاطر المرتبطة باستخدامها، إلا أن فوائدها في تسهيل المعاملات، وتقليل الاعتماد على النقود الورقية، ودعم التجارة الإلكترونية تجعلها أساسية في الاقتصاد الحديث.

[1] خالد السعدي، أهمية البطاقات البنكية في الاقتصاد الرقمي .دار الجيل، بيروت، لبنان، 2020، ص 103.

[2] محمود علي، المخاطر والتحديات المرتبطة باستخدام البطاقات البنكية، مجلة الاقتصاد الرقمي، د.ب.ن، العدد 12، 2021، ص 32.

ثانيا: الأوراق التجارية الالكترونية

تعتبر الأوراق التجارية الإلكترونية من بين التطورات القانونية التي ظهرت نتيجة الثورة الرقمية والتكنولوجيا الحديثة، والتي تهدف إلى تبسيط التعاملات التجارية عبر استخدام التكنولوجيا بدلاً من الوسائل الورقية التقليدية.

1/- تعريف الأوراق التجارية الإلكترونية وخصائصها

تتميز الأوراق التجارية الإلكترونية بخصائص تجعلها موازية للأوراق التقليدية، مثل القوة التنفيذية والإثباتية. فهي تعتمد على توقيعات إلكترونية وأنظمة تشفيرية لحماية المعلومات[1]. الأوراق التجارية الإلكترونية تلعب دورًا حيويًا في تحسين سرعة المعاملات التجارية وتقليل التكلفة الإدارية المتعلقة بالأوراق التقليدية، مما يسهم في تحقيق الاستدامة الاقتصادية للشركات[2].

تُعرف الأوراق التجارية الإلكترونية بأنها وثائق رقمية صادرة عن المؤسسات المالية أو التجارية، تحمل نفس الخصائص القانونية للأوراق التجارية الورقية التقليدية، مثل الكمبيالات والشيكات. تعتمد هذه الأوراق على البنية التحتية الرقمية التي تسمح بتبادلها إلكترونيًا مع التوقيع الإلكتروني كبديل للتوقيع اليدوي.

كما يشير جيمس ماكنزي إلى أن الأوراق التجارية الإلكترونية تتمتع بنفس القوة التنفيذية للأوراق التقليدية، وذلك بفضل الاعتراف القانوني بالتوقيع الإلكتروني والمعاملات الرقمية في العديد من التشريعات العالمية[3].

1 محمد عبد الغني، التجارة الإلكترونية: القانون والواقع، مكتبة القانون العربي، بيروت، لبنان، 2021، ص. 42.

2 علي صادق، التكنولوجيا المالية والمعاملات الإلكترونية، دار الكتاب العربي، دبي، الإمارات العربية المتحدة، 2018، ص. 121.

3 جيمس ماكنزي، القانون الرقمي والتجارة الإلكترونية، مطبعة جامعة أوكسفورد، المملكة المتحدة، 2018، ص. 57.

تعتبر الرقمنة أهم خصائص الأوراق التجارية الإلكترونية، حيث تُسهم في تسهيل عملية التعاملات المالية عبر الإنترنت وتقليل الحاجة إلى الطباعة والنقل الفعلي، الأوراق التجارية الإلكترونية تعتمد على التشفير وأنظمة الأمان الإلكتروني التي تضمن عدم التزوير أو التلاعب بالمعلومات.

تتميز الأوراق التجارية الإلكترونية بأنها تحمل نفس القوة القانونية للأوراق الورقية التقليدية في معظم الدول بسبب اعتماد القوانين على مفهوم التوقيع الإلكتروني كأداة قانونية مقبولة لإثبات التعاملات.

من أبرز خصائص الأوراق التجارية الإلكترونية المرونة وسرعة التنفيذ؛ حيث يُمكن التعامل بها بسرعة كبيرة مقارنة بالأوراق التقليدية التي تحتاج إلى وقت أطول لإتمام المعاملات الورقية، مثل التوقيع اليدوي وإرسال المستندات عبر البريد[1].

2/- التحديات القانونية للأوراق التجارية الإلكترونية

مع التطور التكنولوجي السريع، انتقلت العديد من المعاملات التجارية من الشكل التقليدي إلى الشكل الإلكتروني، فأصبحت الأوراق التجارية الإلكترونية جزءًا أساسيًا من العمليات التجارية الحديثة، لكنها تواجه العديد من التحديات القانونية التي تحتاج إلى معالجة .ورغم الفوائد العديدة، تواجه الأوراق التجارية الإلكترونية العديد من التحديات القانونية، مثل عدم توافق الأنظمة القانونية بين الدول وعدم وجود إطار قانوني دولي موحد.

تواجه العديد من الدول العربية تحديات في تطبيق الأوراق التجارية الإلكترونية بسبب النقص في البنية التحتية القانونية والتكنولوجية، ولكن بعض الدول، مثل الإمارات العربية المتحدة، قامت بخطوات كبيرة في هذا المجال.

على الرغم من التطور التقني، لا تزال بعض الدول تفتقر إلى التشريعات التي تعترف بالأوراق التجارية الإلكترونية بنفس القوة القانونية للأوراق التقليدية. هذا يؤدي إلى عدم اليقين القانوني ويعيق التداول الدولي لهذه الأوراق[2].

---

[1] Sara Peterson, International Trade and Internet Laws, Blackwell Publishing, New York, USA, 2017, p. 83.

[2] ليلى محمد العطار، التحديات القانونية للتجارة الإلكترونية في الوطن العربي، مجلة الحقوق، جامعة الكويت، العدد 4، 2020، ص 27.

تتعرض الأوراق التجارية الإلكترونية لمخاطر الاختراق والاحتيال الإلكتروني، مما يتطلب وجود أنظمة أمان متقدمة وتشريعات تحمي الأطراف المتعاملة.

كما هو التحدي في إثبات صحة التوقيع الإلكتروني وهوية الموقع عليه، فإنه تختلف المعايير التقنية والقانونية للتوقيعات الإلكترونية بين الدول، مما يعيق الاعتراف المتبادل.

المطلب الثاني: العقد الالكتروني في قانون 05/18

العقد الإلكتروني في إطار القانون 05/18 هو عقد يتم إبرامه عبر وسائل إلكترونية، مثل الإنترنت، دون الحاجة إلى حضور مادي للأطراف المتعاقدة، وهذا ما يجعل العقد الإلكتروني يتميز بالعديد من الخصائص، أهمها السرعة في إبرام العقود، المرونة في التعامل، والقدرة على تجاوز الحدود الجغرافية.

غير أنه تجدر الإشارة إلى أنه لا يختلف العقد الالكتروني عن العقد التقليدي إلا في طريقة الانعقاد أو وسيلته التي تتم باستخدام أجهزة الاتصال الحديثة ذات التقنية العالية ومنها شبكة الانترنت، وفي خاصية الانعقاد –عبر تلك الوسائل– عن بعد من حيث المكان مع وجود نوع من المعاصرة من حيث الزمان.

لذلك سنتعرض في البداية إلى تعريف العقد الالكتروني بالنظر إلى طريقة انعقاده ثم نحدد أهم الخصائص التي تميزه عن باقي العقود التقليدية.

الفرع الأول: تعريف العقد الالكتروني

العقد الإلكتروني هو اتفاق يتم إبرامه وتوثيقه عبر وسائل إلكترونية (الإنترنت أو غيرها من الوسائل الالكترونية)، ويتضمن شروطًا ملزمة للطرفين دون الحاجة إلى تواجد مادي لهما، كما يختلف تعريف العقد الإلكتروني من تشريع إلى آخر، سواء في البلدان العربية أو الأجنبية، سنستعرض هنا تعريفات هذا المفهوم في مختلف التشريعات.

أولا: التشريع المصري

في مصر، العقد الإلكتروني يُنظم من خلال قانون التوقيع الإلكتروني رقم 15 لسنة 2004[1]، الذي ينص بموجب المادة 1 منه على أن العقد الإلكتروني يتمتع بنفس القوة القانونية التي يتمتع بها العقد المكتوب أو العقد التقليدي، غير أنه يشترط أن تتوفر فيه الأركان التقليدية للعقد، مثل الرضا والأهلية.

ثانيا: التشريع العراقي

عرفت المادة 8 من قانون الاتصالات السلكية العراقي 109 لسنة 1980 الاتصال عن بعد بأنه إرسال واستلام الأمواج اللاسلكية بكافة أنواعها واتصالاتها، سواء كانت بواسطة إشارة أو علامة أو كتابة أو صورة أو صوت أو أية معلومات خرى، مهما كان نوعها، ولأي غرض كانت[2].

ثالثا: التشريع الأمريكي

في الولايات المتحدة، العقد الإلكتروني يُنظم بموجب قانون التجارة الإلكترونية الفيدرالي لعام 2000 (Electronic Signatures in Global and National Commerce Act – ESIGN Act). يمنح هذا القانون الاعتراف القانوني للعقود الإلكترونية في المعاملات التجارية، بشرط أن تتضمن موافقة إلكترونية واضحة من الأطراف[3].

رابعا: التشريع الأوروبي

الاتحاد الأوروبي يعتمد على التوجيه الأوروبي رقم EC 31/2000/بشأن التجارة الإلكترونية، الذي ينظم تفاصيل العقود الإلكترونية على مستوى الدول الأعضاء. يشدد التوجيه على ضرورة وجود إجراءات واضحة تتيح للمستهلكين معرفة كافة تفاصيل العقد قبل إتمامه[4].

خامسا: التشريع الفرنسي

---

[1] قانون التوقيع الالكتروني المصري لسنة 2004، مرجع سابق.

[2] قانون التوقيع الإلكتروني العراقي رقم 15 لسنة 2004، الصادر بتاريخ: 24 ديسمبر 1980، نشر في الجريدة الرسمية العراقية "الوقائع العراقية" في العدد رقم 2760 في سنة 1980.

[3] U.S. Congress U.S. Congress, Electronic Signatures in Global and National Commerce Act (ESIGN), Library of Congress, United States of America, 2000, Section 101, ESIGN Act.

[4] European Union, Directive 2000/31/EC on electronic commerce, Belgium, 2000, Office of the European Union, Article 11

في فرنسا، يُنظم العقد الإلكتروني بموجب القانون رقم: 2004/575 المؤرخ في 21 يونيو 2004، والذي يشمل الإجراءات المتعلقة بثقة الاقتصاد الرقمي (La loi pour la confiance dans l'économie numérique)[1] يوضح القانون أن العقد الإلكتروني يجب أن يتم بشفافية ويجب أن يكون لطرفي العقد فرصة التأكيد النهائي قبل إتمامه.

وقد نص قانون الاتصالات الفرنسي الصادر بتاريخ: 1986/12/30 التي عرفت الاتصال عن بعد بأنه كل انتقال أو إرسال أو استقبال لرموز أو إشارات أو كتابة أو صور أو أصوات أو معلومات، أيا كانت طبيعتها، بواسطة ألياف بصرية أو كهرباء لاسلكية أو أية أنظمة إلكترومغناطيسية أخرى[2].

يلاحظ من النص الفرنسي أن التعريف يشمل الاتصالات عبر الانترنت لمختلف الأغراض، ومن بينها إبرام العقود، بوصف الشبكة الدولية (الإنترنت) وسيلة حديثة للاتصال عن بعد، وإنها وسيلة مفتوحة لكل مشترك، وهي وسيلة سمعية بصرية في آن واحد[3].

سادسا: التشريع الجزائري

في القانون الجزائري، ينظم العقد الإلكتروني من خلال القانون رقم 18-05 المؤرخ في 10 مايو 2018، الذي يتعلق بالتجارة الإلكترونية.

يعرّف هذا القانون العقد الإلكتروني بموجب المادة 6 فقرة 2 بأنه اتفاق مبرم بين طرفين أو أكثر عن بعد، دون الحضور الفعلي والمتزامن لأطرافه باللجوء حصريا لتقنية الاتصال الإلكتروني.

تتطلب العقود الإلكترونية في الجزائر توفر عدد من الشروط ليتم اعتبارها صحيحة وقانونية. يشترط أن يكون هناك:

1. رضا حقيقي بين الأطراف.

---

[1] French National Assembly, Loi n° 2004-575 pour la confiance dans l'économie numérique, French Official Gazette, France, 2004, Article 1369-1.

[2] L'article: **"On entend par télécommunication toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images ou de sons, de renseignements de toute nature par fil, radioélectricité, optique ou autres systèmes électromagnétiques."** Loi n° 86-1067 du 30 décembre 1986, Code des postes et des communications électroniques, Journal Officiel de la République Française, L32.

[3] عبد الباسط جاسم محمد، إبرام العقد عبر الانترنت، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، لبنان، 2010، ص 40.

2. تحديد موضوع العقد بدقة.

3. اعتماد وسائل التوثيق الإلكتروني، مثل التوقيع الإلكتروني.

يعتبر الإثبات في العقود الإلكترونية أحد أهم الجوانب التي تطرقت لها القوانين الجزائرية. وفقاً للقانون رقم 15-04 المتعلق بالتجارة الإلكترونية، فإن البيانات الإلكترونية والمراسلات الإلكترونية بين الطرفين تعتبر وسيلة إثبات قانونية[1].

العقود الإلكترونية ترتب نفس الآثار القانونية المترتبة على العقود التقليدية، حيث تلتزم الأطراف بتنفيذ العقد بحسب ما تم الاتفاق عليه إلكترونياً. في حالة النزاع، يمكن الاحتكام إلى القضاء الجزائري بناءً على أحكام القانون رقم 18-05[2].

التشريع الجزائري يسير بخطى ثابتة نحو تكييف النصوص القانونية مع التطورات التكنولوجية الحديثة، وهو ما يعكس الاهتمام المتزايد بالعقود الإلكترونية.

وبذلك يمكن القول أن العقود الالكترونية هي العقود التي تتم عبر هذه الوسائل ونحوها من الآلات التي تعمل عن طريق الالكترون، وهذا من حيث الأصل، إلا أنه بعد ظهور الحاسب الآلي وانتشار المراسلة والتعاقد بواسطته، خصص هذا المصطلح للعقود التي تتم عن طريقه، أما التعاقد عبر الراديو أو الهاتف أو غيرها من وسائل الاتصال فلا يشملها عرفا هذا المصطلح في السنوات الأخيرة، وأصبح مصطلح العقود الالكترونية ينصرف مباشرة إلى العقود التي تتم عبر شبكة الانترنت[3].

الفرع الثاني: خصائص العقد الالكتروني

تميز العقد الإلكتروني بعدة خصائص تجعله مختلفًا عن العقود التقليدية، كما تجعل العقود الإلكترونية مرنة وسريعة في إبرامها.

من أبرز هذه الخصائص:

---

[1] يوسف عبد القادر، وسائل الإثبات في التجارة الإلكترونية، مجلة القانون والاقتصاد، العدد 7، 2021.

[2] عبد العزيز عبد الله، الآثار القانونية للعقود الإلكترونية، دار النهضة العربية، الجزائر، 2018، ص. 114.

[3] يوسف حسن يوسف، العقود التجارية الالكترونية الدولية، المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة، مصر، 2012، ص 11.

أولا: خصوصية الانعقاد عن بعد

إن طبيعة العقود الالكترونية المتأتية من طريقة انعقادها عن بعد، جعل لها بالضرورة أحكاما تختلف عن أحكام العقود المبرمة بين حاضرين، والتي يكون الحضور المادي للأطراف فيها مساعدا على تذليل كثير من الصعوبات التي تتمثل في تحقق كل منهم من شخصية الآخر القانونية، والتثبت من تلقيه التعبير الإرادي الصادر عن المتعاقد الآخر، وضبط تاريخ العقد ومكانه، وسلامة المستندات المتعلقة به، فضلا عن كثير من المسائل القانونية التي يضمنها الحضور المادي للأطراف في التعاقد بين حاضرين عموما، والسبب الأول الذي يستدعي وضع قواعد خاصة بالعقود المبرمة عن بعد هو حماية المستهلكين في هذا النوع من العقود[1].

الانعقاد عن بُعد في العقود الإلكترونية يتطلب أن يكون هناك تفاعل بين الأطراف عبر وسيلة إلكترونية تحدد هوية الطرفين وتضمن سلامة البيانات المتبادلة. عادةً ما يعتمد هذا النوع من العقود على تقنيات الأمان مثل التوقيع الإلكتروني الذي يعتبر بمثابة توقيع شخصي على العقد.

ثانيا: العقد الالكتروني عقد مرتبط بحق العدول

يقصد بحق العدول ذلك الحق المخول لأحد أطراف العلاقة التعاقدية في إلغاء العقد أو العدول عنه خلال فترة زمنية محددة بعد الإبرام، هذا الحق يعد عنصرًا أساسيًا لحماية المستهلكين في العقود الإلكترونية.

أبرز ما يترتب على التعاقد عن بعد، سواء الإنترنت أو عبر غيره من الوسائل الحديثة، هو عدم تمكن المستهلك أو المشتري من الحكم الدقيق على المنتوج أو السلعة بشكل جازم، مهما بلغ الوصف الذي يصفه به المهني أو البائع من الدقة عبر موقعه على الانترنت[2]، وهذا الأمر نجده يتجسد من خلال المشرع الفرنسي من خلال نص المادة الأولى من القانون الصادر بتاريخ: 06 يناير 1988 التي نصت على أن لمشتري المنتجات الحق في إعادة المبيع إلى البائع واسترداد ما دفعه أو استبدال المبيع خلال مدة 7 أيام من تاريخ تقديم المبيع.

[1] عبد الباسط جاسم محمد، مرجع سابق، 46.

[2] أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الانترنت، دار النهضة العربية، القاهرة، مصر، 2003، ص 42.

إن منح هذا الحق في العدول لأحد الأطراف يستلزم إيجاد ما يعرف ب: "الإستمارة الضامنة" والتي يقصد بها استمارة ترافق العقد تقوم بوظيفة إعلام الطرفين بوجود الخيار أو الرخصة، ووظيفة بدء حساب مدة الأيام السبعة، وهي تشبه إلى حد ما استمارة الضمان التي يمنحها بعض التجار إلى العملاء في السلع التي يعلن بائعها عند التعاقد إنها مضمونة لمدة يحددها سلفا[1].

رغم أهمية حق العدول في العقد الالكتروني إلا أن هناك تحديات قانونية مثل تحديد مدة حق العدول وإجراءات الإلغاء، مما يتطلب تعديلات قانونية واضحة لحماية الأطراف المعنية.

ثالثا: العقد الإلكتروني يبرم دون حضور مادي لأطرافه

السمة الأساسية للعقد الإلكتروني هي أنه يربط بين طرفين متعاقدين لا يجمعهما مجلس عقد حقيقي لأن العقد يبرم عن بعد بوسائل تكنولوجية حديثة لتبادل الموافقات. ويتم تبادل الموافقات إلكترونيًا عبر الإنترنت من خلال مجلس عقد تحكيم افتراضي[2]، وعلاوة على ذلك، قد يكون فوريًا ولكنه معاصر بالتأكيد حتى عند تنفيذه عن بعد وفي نقاط زمنية مختلفة. وتنتج هذه المعاصرة عن وجود تصرفات للأطراف تهدف إلى الالتزام النهائي بتبادل تفاعلي.

رابعا: العقد الالكتروني يتسم غالبا بالطابع الدولي

العقد الإلكتروني يتمتع بخصائص تجعله ذو طابع دولي، حيث يمكن للأطراف من دول مختلفة إبرامه بسهولة عبر الإنترنت. هذا التوسع في نطاق العقود الإلكترونية يعكس طبيعة التجارة العالمية. توجد عدة اتفاقيات دولية تنظم العقود الإلكترونية، مثل اتفاقية الأمم المتحدة بشأن عقود البيع الدولي للبضائع (CISG) التي تهدف إلى تسهيل التجارة الدولية.

تتيح العقود الإلكترونية ذات الطابع الدولي مرونة كبيرة في إبرام الصفقات التجارية، ولكنها أيضًا تواجه تحديات مثل اختلاف القوانين بين الدول والمخاطر القانونية، كما تعتبر قضايا الأمان والثقة من العوامل المهمة في العقود الإلكترونية، حيث يجب على الأطراف ضمان سلامة المعاملات لحماية حقوقهم.

---

[1] عبد الباسط جاسم محمد، مرجع سابق، ص 50.

[2] محمد سعد خليفة، مشكلات البيع عبر الانترنت، دار النهضة العربية، القاهرة، مصر، 2002، ص 30.

يعتبر العقد الالكتروني عقدا دوليا لعدم إمكانية تطبيق المعايير التقليدية في القانون الدولي الخاص بوصفه عقدا داخليا أو وطنيا.

خامسا: العقد الالكتروني بين التفاوض والإذعان

عقود الإذعان هي عقود يسلم فيها القابل بشروط يضعها الموجب سلفا ولا يقبل مناقشة فيها وتتعلق بمرفق ضروري أو سلعة ضرورية محل احتكار قانوني أو فعلي كعقد اشتراك الماء والكهرباء والتأمين.

إن لاعتبار العقد الالكتروني من ضمن قبيل عقود الإذعان أو التفاوض جعل الفقه ينقسم إلى قسمين:

الرأي الأول: يعتبر أن العقود الالكترونية هي عقود إذعان بالمعنى الدقيق لأن المهني يفرض شروطه ولا يملك المستهلك إلا أن يقبل هذه الشروط أو يرفضها دون تفاوض[1].

الرأي الثاني: يرى هذا الجانب من الفقه أن العقود الالكترونية ليست عقود إذعان، لأن التاجر وإن كان يفرض شروطه ولا يقبل بصددها مفاوضة، إلا أن من شروط الإذعان أن يتعلق باحتكار مرفق أو سلعة ضرورية من جانب التاجر، وليس كل عقد الكتروني ينطوي على احتكار أو على ضرورة أو يتعلق بمرفق ضروري.

ويرى بعض الفقهاء اختيار معيار إمكانية التفاوض، لأنه باعتبار أن العقد الالكتروني أذا سمح بالتفاوض والمراجعة وتعديل بعض بنوده فهو عقد تفاوض ويخرج من نطاق الإذعان، وعدم سماحه بذلك يجعل منه عقد إذعان وبالتالي فإن تحديد طبيعة العقد الالكتروني بكونه عقد إذعان أو عقد تفاوض يكون بالنظر إلى من وجه إليه الإيجاب أو انعدامه في مراجعة الموجب ومفاوضته بشأن بنود العقد وشروطه.

هذا الأمر من شأنه أن يخلق عدم استقرار المراكز القانونية وترديدا للعقد الالكتروني نفسه، بين الإذعان والتفاوض حسب مصلحة الطرف القوي فيه، لذلك نجد أن العقود الالكترونية هي عقود إذعان

---

[1] عبد المجيد الحكيم، عبد الباقي البكري، محمد طه البشير، الوجيز في نظرية الالتزام في القانون المدني العراقي، مصادر الالتزام، مطبعة جامعة بغداد، 1986، ص 44.

بالمعنى الحرفي من حيث تفسيرها لمصلحة المستهلك، بوصفه طرفا مذعنا في العلاقة العقدية، وبغض النظر عما إذا كان العقد الالكتروني يرد على سلعة ضرورية من عدمه أو إذا كان هناك احتكار لهذه السلعة أم لا[1].

سادسا: العقد الالكتروني بين الطابع المدني والتجاري

اختلفت الآراء الفقهية في اعتبار العقود الالكترونية عقود ذات طابع مدني أو تجاري فهناك ما يعتبر من العقود مدنيا وهناك ما يعتبر تجاريا.

العقود المدنية تركز على المعاملات الشخصية والخاصة، بينما العقود التجارية تتعلق بالمعاملات التي تهدف إلى تحقيق ربح وتدخل في إطار الأعمال التجارية.

قد يكون العقد الإلكتروني مدنيا إذا تم من خلال اتفاق بين طرفين يتم عبر الوسائط الإلكترونية ويهدف إلى تحقيق مصالح شخصية أو خاصة، وليس لأغراض تجارية، مثل شخص يقوم بشراء هدية عيد ميلاد لصديق عبر موقع تسوق إلكتروني، في هذه الحالة، العقد بين الشخص وموقع التسوق يعتبر عقدًا مدنيًا لأنه يتعامل مع احتياجات شخصية.

وقد يكون العقد الإلكتروني تجاريا إذا تم من خلال اتفاق يتم عبر الإنترنت بين طرفين لأغراض تجارية، ويدخل في نطاق الأنشطة التجارية.، مثل شركة تبيع منتجاتها عبر موقع إلكتروني وتقوم بإبرام عقود مع زبائنها، في هذه الحالة العقد يعتبر عقدًا تجاريًا لأنه يتعلق بمبيعات تجارية ويهدف إلى تحقيق الربح.

[1] عبد الباسط جاسم محمد، مرجع سابق، ص 52.

المحور الثاني:

طـرق الإثبـات في المعــامـــلات الالكتـــرونية

تعتبر طرق الإثبات في المعاملات الإلكترونية من العناصر الأساسية لضمان صحة وسلامة هذه المعاملات. تشمل طرق الإثبات المستخدمة في هذا السياق المستندات الإلكترونية، والتوقيعات الرقمية، والسجلات الإلكترونية، والتي تهدف إلى تأكيد هوية الأطراف المعنية، وضمان عدم التلاعب بالمعلومات. يُعتبر التوقيع الرقمي مثلاً وسيلة فعالة لإثبات صحة الوثائق الإلكترونية، حيث يتم استخدام تشفير متقدم لضمان سلامة البيانات.

علاوة على ذلك، تسهم التقنيات الحديثة في تعزيز موثوقية الإثبات في المعاملات الإلكترونية، حيث توفر سجلات غير قابلة للتغيير لكل معاملة، كما تعمل هذه الوسائل على التعزيز من الشفافية والثقة بين الأطراف، مما يسهل من إجراء المعاملات الإلكترونية بشكل آمن وفعال. وبذلك، تعتبر طرق الإثبات عنصرًا محوريًا لضمان استمرارية نمو التجارة الإلكترونية وتطورها في العالم الرقمي.

لذلك وبغرض تحديد مدى إمكانية الإثبات في المعاملات الالكترونية يتطلب منا الأمر بيان الموقف القانوني من الكتابة الالكترونية في ظل النصوص القانونية النافذة (المبحث الأول)، وكذلك بيان مدى إقرار الإثبات بالتوقيع الالكتروني (المبحث الثاني).

المبحث الأول: إقرار الإثبات بالكتابة الإلكترونية

في عصر التكنولوجيا الرقمية، أصبحت الكتابة الإلكترونية والتوقيع الإلكتروني جزءًا أساسيًا من الحياة اليومية والعمليات التجارية. تسهم هذه الأدوات في تسريع وتسهيل التفاعلات القانونية والتجارية، مما يقلل من الحاجة للأوراق التقليدية والإجراءات المعقدة. الكتابة الإلكترونية توفر وسيلة فعّالة للتواصل وتبادل المعلومات، بينما يعزز التوقيع الإلكتروني من مصداقية المعاملات ويؤمن حقوق الأطراف المعنية. تتطلب هذه الظواهر فهمًا عميقًا للتقنيات والآليات القانونية المرتبطة بها، مما يفتح آفاقًا جديدة لتطوير الأعمال وتحسين الكفاءة. مع تزايد الاعتماد على الحلول الرقمية، يبرز أهمية التعرف على الأسس القانونية والفنية التي تحكم هذه العمليات.

لذلك سنتعرض خلال هذا المبحث إلى مفهوم الكتابة الإلكترونية لتحديد تعريفها وخصائصها (المطلب الأول)، ثم نتعرض إلى صور الكتابة الإلكترونية وحجيتها في الإثبات (المطلب الثاني).

المطلب الأول: مفهوم الكتابة الإلكترونية

لتحديد مفهوم الكتابة الإلكترونية يتعين علينا في البداية تعريفها ثم تحديد خصائصها التي تميزها عن الكتابة التقليدية وشروط قبولها في الإثبات.

الفرع الأول: تعريف الكتابة الإلكترونية وخصائصها

أولا: تعريف الكتابة الإلكترونية

الملاحظ في الحياة العملية أنه كثيرا ما يُخلط بين التصرف القانوني وأداة إثباته، فيقال مثلاً، عقد بيع رسمي، أو عقد بيع عرفي، ويقصد بذلك الورقة الرسمية أو الورقة العرفية المثبتة للتصرف القانوني وعقد البيع، غير أنه يجب التحرز من مثل هذا الخلط، ذلك أن كلمة "عقد" هي كلمة تطلق على التصرف القانوني الذي يتم بتوافق إرادتين، أما الورقة فهي الدعامة التي يفرغ فيها هذا التصرف فتكون أداة إثبات عليه، ولهذا التفريق أهمية بالغة، إذ أنه من المحتمل أن يكون التصرف القانوني باطلاً رغم استيفاء المحرر المثبت له شروط صحته المتطلبة قانوناً، كما أنه من الممكن أن يكون

التصرف صحيحاً رغم عدم استيفاء المحرر للشروط القانونية المتطلبة، فيبقى هذا التصرف قابلاً للإثبات بوسائل أخرى كالإقرار أو اليمين مثلا[1] .

الكتابة لغة: مشتقة من الفعل الثلاثي كتب بمعنى خط، فيقال: كتب الشيء أي خطه، والكتاب ما كُتب فيه، والكتابة: هي ما يخطه الإنسان، كما تعني: ضم شيء إلى شيء، وقد استعير هذا المعنى للتعبير عن تصوير الكلام بحروف الهجاء وذلك لأن هذا التصوير إنما يتم بضم الحروف بعضها إلى بعض.

كما تعرف الكتابة اصطلاحا بأنها رموز تعبر عن الفكر والقول بصرف النظر عن الوسيط الذي تستند عليه أو الدعامة التي تستند إليها، وما إذا كانت الكتابة على الورق أو على دعامة إلكترونية، طالما أن هذا الوسيط أو الدعامة قادر على نقل رموز الكتابة فهو صالح للاعتداد به[2].

أما مصطلح الالكترونية فهو نسبة إلى الإلكترون المعروف في علم الفيزياء وهو عنصر أول ثابت ذو شِحنة كهربائية سلبية، يمثل أساس الآليات الإلكترونية، وهو أحد المكونات في ذرة المادة[3].

تعريف الكتابة الإلكترونية في التشريعات المقارنة

1/- في التشريع اللبناني

عرف مشروع تعديل قانون أصول المحاكمات المدنية اللبناني الكتابة الالكترونية بأنها الكتابة التي تقوم على تسلسل حروف أو أية رموز أو إشارات تشكل معنى قابلا للقراءة، وذلك أيا كانت الوسائل المستخدمة كسند لها[4].

---

[1] صقر ن، مكاري ن، الوسيط في القواعد الإجرائية والموضوعية للإثبات في المواد المدنية، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2009، ص 76.

[2] وسيم شفيق الحجار، الإثبات الالكتروني، منشورات صادر الحقوقية، بيروت، لبنان، 2001، ص 18.

[3] The Physics Classroom. (n.d.). *The Electron*. Retrieved September 17, 2024, from https://www.physicsclassroom.com/class/modern/Lesson-1/The-Electron

[4] المادة 142 مكرر 1 من مشروع تعديل قانون أصول المحاكمات المدنية اللبناني (ق.أ.م.م.ل).

في لبنان، تم وضع إطار قانوني لتنظيم الكتابة الإلكترونية، والذي يعكس أهمية استخدامها في مختلف المجالات، وذلك من خلال القانون رقم 2018/81 (قانون المعاملات الإلكترونية)[1].

يعتبر هذا القانون الإطار القانوني الرئيسي الذي ينظم الكتابة الإلكترونية في لبنان، حيث يعترف بالكتابة الإلكترونية كوسيلة قانونية للتوثيق والعقود، ينص القانون بموجب المادة 1 منه على أن الكتابة الإلكترونية هي أي معلومات تُنتج أو تُخزن أو تُرسل بوسائل إلكترونية، بما في ذلك الرسائل النصية والبريد الإلكتروني.

2/- في التشريع المصري

قانون المعاملات الإلكترونية (رقم 15 لسنة 2004)، يعتبر هذا القانون هو الإطار القانوني الأساسي الذي ينظم الكتابة الإلكترونية في مصر. ينص على أن الكتابة الإلكترونية تُعتبر دليلاً قانونيًا في المحاكم إذا توافرت فيها الشروط المنصوص عليها.

أنشأت مصر هيئات متخصصة، مثل الهيئة القومية للبريد، لتطوير وتقديم خدمات الكتابة الإلكترونية والتوقيع الإلكتروني، مما يعكس أهمية هذه الأدوات في المعاملات الحكومية.

3/- في التشريع الإماراتي

قانون المعاملات الإلكترونية (رقم 1 لسنة 2006)، يعتبر هذا القانون الإطار القانوني الأساسي الذي ينظم الكتابة الإلكترونية في الإمارات. ينص على أن الكتابة الإلكترونية تُعتبر دليلاً قانونيًا معترفًا به في المحاكم إذا توافرت فيها الشروط المحددة.

تتناول التشريعات الإماراتية أهمية تأمين المعلومات والبيانات المتبادلة إلكترونيًا، مما يعزز من حماية الكتابة الإلكترونية ضد التلاعب أو الاختراق، كما أنشأت الإمارات هيئات متخصصة مثل الهيئة العامة لتنظيم الاتصالات والحكومة الرقمية، لتطوير وتقديم خدمات الكتابة الإلكترونية والتوقيع الإلكتروني، مما يعكس أهمية هذه الأدوات في المعاملات الحكومية.

---

[1] قانون المعاملات الإلكترونية- https://www.coe.int/en/web/digital-nation/legislation .Retrieved from 2018.

4/- الكتابة الإلكترونية في الاتفاقيات الدولية

تعتبر الكتابة الإلكترونية معترفًا بها دوليًا، حيث تم تضمينها في عدة اتفاقيات:

- **اتفاقية الأمم المتحدة بشأن استخدام وسائل الاتصالات الإلكترونية في العقود الدولية:** تعترف هذه الاتفاقية بأن الكتابة الإلكترونية تُعتبر معادلة للكتابة التقليدية، مما يسهل إجراء المعاملات التجارية الدولية[1].
- **مبادئ الأمم المتحدة للتجارة الإلكترونية:** تنص المبادئ على أهمية اعتراف الدول بالكتابة الإلكترونية وتوفير إطار قانوني يحمي حقوق الأطراف[2].

5/- الكتابة الإلكترونية في التوجيه الأوروبي

يحدد التوجيه الشروط القانونية لاستخدام التوقيع الإلكتروني ويعتبره معادلًا للتوقيع التقليدي، كما تساهم في حماية البيانات الشخصية عند استخدام الكتابة الإلكترونية، مما يعزز الثقة في المعاملات الإلكترونية.

6/- الكتابة الإلكترونية في التشريع الأمريكي

تُعتبر الكتابة الإلكترونية جزءًا أساسيًا من التشريعات الأمريكية، بحيث نجد قانون التوقيع الإلكتروني في التجارة العالمية ((ESIGN Act)، يعترف هذا القانون بالكتابة الإلكترونية ويعتبرها قانونية، مما يسهل المعاملات التجارية[3].

قانون حماية الخصوصية:(Privacy Act) ينظم هذا القانون كيفية استخدام البيانات الشخصية في الكتابة الإلكترونية، مما يعزز حماية المعلومات. كما تشرف هيئات مثل وزارة التجارة ومكتب إدارة الأعمال الصغيرة على تنظيم وتطوير خدمات الكتابة الإلكترونية والتوقيع الإلكتروني، مما يعكس أهمية هذه الأدوات في المعاملات الحكومية والتجارية.

---

[1] United Nations. (2017). United Nations Convention on the Use of Electronic Communications in International Contracts. Retrieved from https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications_international_contracts

[2] United Nations. (1996). Mali Declaration on Electronic Commerce. Retrieved from https://unctad.org/webflyer/mali-declaration-electronic-commerce

[3] U.S. Congress. (2000). Electronic Signatures in Global and National Commerce Act. Retrieved from https://www.congress.gov/bill/106th-congress/house-bill/1714/text

7/- الكتابة الإلكترونية في التشريع الجزائري

لجأ المشرع الجزائري إلى عملية تطويع قواعد القانون المدني المتعلقة بالإثبات لتستوعب الرسائل والدعامات غير الورقية، فتعرض إلى الكتابة الإلكترونية في المادة 323 مكرر، وكذا المادة 323 مكرر 1 من القانون 10/05 المعدل للقانون المدني الجزائري. حيث نصت المادة 323 مكرر "ينتج الإثبات بالكتابة من تسلسل حرو ف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها."

لقد التزم المشرع الجزائري بالمفهوم الموسع للكتابة ولم يحصرها في وسيلة التعبير المحددة حتى يترك المجال لوسائل أخرى قد يطرأ عليها جملة من التطورات، وهذا يشمل الكتابة التقليدية والطباعة الآلية والبريد الإلكتروني، كما لم يحصر وسيلة الإرسال التي قد تكون مادية بتسليم الأوراق، أو مغناطيسية كالفاكس والتلكس، أو إلكترونية بواسطة الحاسوب والإنترنت، كما يتبين من المادة 543 مكرر والتي تذكرنا بالمادة 1/1316 من القانون الفرنسي باعتبار أنها تضمنت نفس المفاهيم.

كما تجدر الإشارة إلى أنه لا يوجد في القانون أي شرط للاعتقاد بأن الكتابة يجب أن تكون على الورق، مع الإشارة إلى أن المشرع الفرنسي لم يحدد الوسيط الذي تتم عليه الكتابة، وإلى جانب ذلك، تبنت العديد من الاتفاقيات الدولية هذا المفهوم، ومنها اتفاقية الأمم المتحدة بشأن النقل الدولي للبضائع. ومن الواضح، أنه لا ينبغي أن تؤخذ الكتابة في ضوء ارتباطها بالوسيط أو الوسيط المستخدم في التسجيل، بل في ضوء وظيفتها في إعداد الأدلة على وجود الفعل القانوني وتحديد مضمونه بطريقة تسمح للأطراف بالرجوع إليها في حالة النزاع. الوسيلة ليست الرسالة: النص هو الكتابة، عندما تتم الكتابة.

من خلال المادة 323 مكرر نلاحظ أن المشرع الجزائري وسع مفهوم الكتابة ليشمل الكتابة على ورق برسم رمزي والكتابة في شكل إلكتروني، فرغم أننا نعتبر الكتابة عادة على نوع الورق العادي إلا أن الكتابة الآن تنشأ من تحضيرات معينة بأشكال وأحجام مختلفة، وبالتالي فهي غير مقيدة بمفهوم الورق حيث قد تنشأ صناعة ورق أخرى غير معترف بها في الوقت الحاضر، فنقول إن مفهوم الكتابة قد اتسع ليشمل كل الوثائق الإلكترونية المستخرجة من وسائل الاتصال الحديثة أيا كانت مادتها أو

شكلها أو وسيلة نقلها حتى ولو لم تظهر على وسيط مادي ملموس أو غير ملموس ليقرأه الإنسان ودون استعمال أي وسيلة أخرى[1].

ثانيا: خصائص الكتابة الالكترونية

تمتاز الكتابة الإلكترونية بغزارتها، وإمكانية الحصول عليها ونقلها بسرعة هائلة، كونها مسجلة على دعائم مغناطيسية، لا يمكن قراءتها أو الاطلاع عليها إلا من خلال عرضها على شاشة الحاسوب الآلي، وطباعتها على ورق بواسطة الطابعة الملحقة بهذا الحاسوب.

وبالتالي يتضح لنا أن الكتابة الإلكترونية تتميز بعدة خصائص تميزها عن الكتابة التقليدية، تتمثل في ما يلي:

1/- سرعة الكتابة الالكترونية وضمان الأمن القانوني لها

إن صياغة شرط القابلية للقراءة متماثلة سواء كانت الكتابة بخط اليد أو إلكترونية، ففي الحالتين يجب أن تكون الكتابة مقروءة. وشرط القابلية للقراءة الذي يمكن تحديده بسهولة في الكتابة بخط اليد لأنها تُقرأ فورًا، يصعب تحديده في الكتابة المطبوعة بحكم الفقه لأنها مسجلة على وسيط غير ورقي (أي إلكتروني)، وقد أصبح التسجيل على وسيط إلكتروني له قواعد تقنية والوصول إليه أسرع، بل إن هذا النوع من الكتابة قد يكون مشفرًا؛ وسوف يتعين فك هذا التشفير بحيث يكون في شكل بيانات واضحة وقابلة للإدراك المباشر[2].

تُعد الكتابة الإلكترونية من الوسائل الحديثة التي ساهمت في تسريع العمليات الإدارية والقانونية. مع التطور التكنولوجي السريع، أصبح بإمكان الأفراد والمؤسسات التعامل مع الوثائق والمستندات بسهولة وسرعة فائقة دون الحاجة إلى استخدام الورق. ومع ذلك، فإن التحدي الأبرز الذي يواجه الكتابة الإلكترونية هو ضمان الأمن القانوني لها، بحيث تكون هذه الوثائق معترف بها قانونياً ومحمية من التزوير أو التلاعب.

---

[1] علي عبد العال خشاب الأسدي، حجية الرسائل الإلكترونية في الإثبات المدني، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت –لبنان، ،2013، ص 41.

[2] Yves POULLET, Mireille ANTOINE, Vers la confiance ou comment assurer le développement du commerce électronique, collection LEEPRESSE, Paris France, 2001, 452.

إن الأمن القانوني للكتابة بنوعيها يمكن أن تهدده مخاطر إلا أن هناك وسائل فنية وقانونية لمجابهة هذه المخاطر، فضلا عن إمكانية الاحتفاظ بالكتابة الإلكترونية لفترة طويلة من الزمن أكبر من إمكانية الاحتفاظ بالكتابة العادية، كونها أقصر عمرا من الكتابة الالكترونية، ولا يمكن الاعتداد بهذا النوع من الكتابة كدليل للإثبات ما لم يكن بالإمكان الاحتفاظ بها بشكلها الأصلي الذي أنشأت به[1].

على الرغم من الفوائد العديدة للكتابة الإلكترونية، إلا أن هناك بعض التحديات التي تواجه ضمان الأمن القانوني لها، مثل اختلاف التشريعات بين الدول فيما يتعلق بالاعتراف بالوثائق الإلكترونية والتوقيعات الرقمية، بالإضافة إلى المخاطر المرتبطة بالهجمات الإلكترونية والقرصنة.

2/- عدم ظهور الكتابة الالكترونية إلا بواسطة جهاز الحاسوب

تكتب الكتابة الالكترونية بلغة الآلة، ومن ثم لا يمكن أن تظهر لعين الناظر، إلا بواسطة جهاز الحاسوب، الذي يتمكن من قراءتها عن طريق معالجتها وتحويلها إلى كتاب بإحدى لغات الإنسان تعرض على شاشة الحاسوب[2]، فإن الحاسوب هو وسيلة كتابة وقراءة الوثيقة الإلكترونية، وهذا الأمر لا يضعف قيمة هذه الوثيقة في الإثبات، بقدر ما يجعلها تتميز بخاصية من خصائصها.

إن عدم ظهور الكتابة الالكترونية مباشرة لا يحول دون مساواتها بالكتابة التقليدية، لأنها وإن كانت غير ظاهرة للعيان إلا أنها قابلة للقراءة، وإن كان ذلك بواسطة جهاز الحاسوب، كما أن ذلك لا يضعف من قيمتها في الإثبات بقدر ما يمثل خاصية من خصائص هذا النوع من الكتابة.

3/- الكتابة الالكترونية أدت لظهور ما يسمى بالإثبات الالكتروني

يقصد بالإثبات الالكتروني قبول المحررات الالكترونية ضمن أدلة الإثبات بوصفها دليلا كتابيا كاملا، بحيث تشمل هذه السندات الالكترونية المستخرجة من الانترنت والتلكس والفاكس ومخرجات الحاسب وكل الوسائل الالكترونية المتاحة.

---

[1] علي عبد العالي خشاب الأسدي، مرجع سابق، ص 22-23.

[2] عبد العزيز المرسي حمود، مدى حجية المحرر الالكتروني في الإثبات في المسائل المدنية والتجارية، د.د.ن، د.م.ن، 2005، ص 15.

وبسبب ظهور الإثبات الالكتروني تزايد استخدام الكتابة الالكترونية بشكل مضطرد نتيجة لأهميتها في تحقيق الاقتصاد في التعاقد، بحيث يتم إنجاز تلك التعاملات في أقصر وقت وبأقل جهد وأدنى نفقات حتى وإن يفصل بين المتعاقدين مسافات طويلة، مما يسهم في تحقيق السرعة والدقة في إبرام المعاملات القانونية وسهولة إثباتها عن طريق مختلف وسائل الإثبات الملائمة لها.

4/- تخفيض تكاليف النقل والخزن إلى أقل حد ممكن

لقد ساهم جهاز الحاسوب الآلي والوسائل الالكترونية المختلفة مثل USB و CD Rom في حل مشكلة التخزين لما تكلفه الوسائل التقليدية بسبب الحاجة إلى مكان التخزين لحفظ الأرشيف، وصعوبة نقلها من مكان إلى آخر في ضوء نظام النقل الحالي.

فهذه الوسائل الالكترونية ساهمت في حل المشكلة لقدرتها الفائقة في خزن كميات هائلة من المحررات والوثائق على الرغم من صغر حجمها، ومن ثم ظهر ما يسمى بالأرشيف الالكتروني والسجل الالكتروني[1].

5/- تمتاز الكتابة الالكترونية بالوضوح والإتقان

إن طبيعة الكتابة الالكترونية واستنادها إلى دعامة إلكترونية، يسمح لها بتصحيح الأخطاء التي تقع أثناء الكتابة، دون أن يترك التصحيح أي أثر يذكر، الأمر الذي يجعل من المحرر الالكتروني محرر منظم وواضح وخالي من الأخطاء[2].

الفرع الثاني: الشروط القانونية للكتابة الإلكترونية

تخضع الكتابة الالكترونية إلى جملة من الشروط لتؤدي الكتابة وظيفتها القانونية في الإثبات حتى تتمتع بالثقة والأمان من جانب مختلف المتعاملين، لذا سنلقي الضوء على أهم هذه الشروط: قابلية القراءة، الكتابة الإلكترونية ثابتة ومستمرة، إمكانية الحفظ وعدم قابلية الكتابة الإلكترونية للتعديل، وهوية الشخص الذي أصدرها.

---

[1] أحمد المهدي، الإثبات في التجارة الالكترونية، دار الكتب القانونية، مصر، 2004، ص 18.

[2] نضال إسماعيل برهم، أحكام عقود التجارة الإلكترونية، دار الثقافة، عمان، الأردن، 2005، ص 18.

1/- قابلية القراءة

تعتبر قابلية الكتابة الإلكترونية للقراءة من الشروط الأساسية التي تتطلبها العديد من الأنظمة القانونية لضمان قبول المستندات والبيانات الإلكترونية كأدلة أو معاملات قانونية، فالقدرة على قراءة المستند الإلكتروني تعني أن المعلومات الموجودة فيه يجب أن تكون واضحة، ومنظمة بطريقة تسهل فهمها وتفسيرها عند الحاجة.

في السياق القانوني، تُعدّ قابلية القراءة شرطًا لضمان الشفافية والموثوقية، فأي مستند إلكتروني لا يمكن قراءته بشكل صحيح أو يعاني من صعوبات تقنية قد يُرفض كدليل قانوني، من هذا المنطلق، تعتمد الأنظمة على معايير وتقنيات لتنسيق وحفظ الملفات الإلكترونية بطريقة تحافظ على سلامة البيانات وإمكانية الوصول إليها في أي وقت.

أيضاً، لا يقتصر الأمر على قابلية القراءة فحسب، بل يجب أن تكون المستندات الإلكترونية قابلة للتوثيق ولإثبات أصالتها، بحيث يكون من الممكن التحقق من عدم التلاعب بها أو تغيير محتواها بعد إنشائها[1].

2/- الكتابة الإلكترونية ثابتة ومستمرة

تعتبر الكتابة الإلكترونية جزءًا أساسيًا من الحياة اليومية، حيث تتطلب استمرارية وثباتًا في المحتوى لضمان فعاليته وتأثيره.

الثبات يشير إلى استمرارية وجود المحتوى الإلكتروني وإمكانية الوصول إليه بمرور الزمن. يتطلب ذلك تخزين البيانات بطريقة تضمن عدم فقدانها، مما يعزز من مصداقيتها وموثوقيتها[2]، كما تعتبر الاستمرارية في الكتابة الإلكترونية ضرورية لأسباب عدة، بحيث أنها تساهم في تحسين تجربة المستخدم وذلك بتوفير استمرارية المحتوى لإمكانية الوصول الدائم للمستخدمين، كما أنها تعمل على

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910 , visité le : 28/07/2024.
[2] Smith, David. "Digital Preservation and the Future of Digital Content." Journal of Digital Information, 2005.

تعزيز التعلم والمعرفة، بحيث يساعد المحتوى المستمر في تكوين قاعدة معرفية متزايدة تساهم في التعلم الذاتي، إضافة إلى ذلك فإنها تدعم هوية العلامة التجارية وتجذب الجمهور.

3/- إمكانية الحفظ وعدم قابلية الكتابة الإلكترونية للتعديل

تعد الكتابة الإلكترونية من العناصر الأساسية في العصر الرقمي، ويُعتبر شرط إمكانية الحفظ وعدم القابلية للتعديل من الأمور الحيوية لضمان موثوقية المعلومات.

إمكانية الحفظ تشير إلى القدرة على تخزين المعلومات بشكل دائم، بحيث تكون متاحة للمستخدمين في المستقبل. يتطلب ذلك استخدام تقنيات تخزين فعالة تضمن عدم فقدان البيانات.

إن عدم القابلية للتعديل تعني أن المحتوى الإلكتروني لا يمكن تغييره بعد نشره، مما يعزز من مصداقيته، هذا الشرط مهم للأسباب التالية[1]:

- **الشفافية:** يساهم في تعزيز الثقة بين المؤلف والجمهور.
- **الحفظ التاريخي:** يحافظ على السجلات التاريخية كما هي، مما يُسهّل البحث والدراسة في المستقبل.

ولتحقيق هذين الشرطين، يجب مراعاة عدة عوامل[2]:

- **اختيار الصيغ المناسبة:** يجب استخدام صيغ ملفات تدعم الحفظ الدائم، مثلPDF/A ، والتي تحافظ على تنسيق المحتوى.
- **التقنيات المستخدمة:** ينبغي استخدام تقنيات تشفير قوية لضمان عدم التلاعب بالمحتوى.
- **سياسات الحفظ:** وضع سياسات واضحة لتحديد كيفية الحفظ والتعامل مع المعلومات.

تستخدم العديد من المؤسسات تقنيات الحفظ وعدم القابلية للتعديل في الكتابة الإلكترونية، نذكر من ذلك:

- **المكتبات الرقمية** :تستخدم المكتبات تقنيات محددة لحفظ المواد الرقمية، مثل الأرشيفات الإلكترونية.

[1] McKemmish, Sue. "What Is Records Continuum Theory?" Archival Science, 2001.
[2] Dempsey, Lorcan. "The Role of Libraries in the Digital Preservation Landscape." Library Journal, 2012.

- **الكتب الإلكترونية** :بعض الناشرين يوفرون كتبًا إلكترونية بصيغ لا يمكن تعديلها لضمان حقوق المؤلفين.

إن شرط إمكانية الحفظ وعدم القابلية للتعديل في الكتابة الإلكترونية يعتبران من الأسس الهامة لضمان موثوقية المعلومات، من خلال مراعاة العوامل المؤثرة، يمكن تحقيق مستوى عالٍ من الأمان والثقة في المحتوى الرقمي.

4/- هوية الشخص الذي أصدرها

نص المشرع الجزائري في المادة 323 مكرر 1 من خلال العبارة "... بشرط إمكانية التأكد من هوية الشخص الذي أصدرها"...، وكذا المشرع الفرنسي بنص المادة 1366 من القانون المدني الفرنسي، حيث ألزم أن تكون الكتابة تدل بوضوح على الشخص الذي أصدرها، وجاء نص المادة كالتالي:

« L'écrit électronique à la même force probante que l'écrit sur support papier, sous réserve que puisse être dument identifié la personne dont il émane, et qu'il soit établi et conservé dans des conditions de nature a en garantir l'intégrité »

كما نص قانون الأونسيترال النموذجي المتعلق بالتجارة الالكترونية[1] 1996 على هذا الشرط في المادة 10 فقرة ج، حيث أنه من بين طرق حفظ الكتابة الإلكترونية تحديد الشخص الذي أنشأ رسالة البيانات، والتدليل على الجهة المستقبلة والإقرار بالاستلام (المادة 14) وتاريخ ووقت وزمان الإرسال وكذا الاستلام (المادة 15)، وبالتالي يقتضي القانون بالاحتفاظ على المستندات أو السجلات أو معلومات بعينها، ويتحقق الوفاء بهذا المقتضى متى تم الاحتفاظ برسائل البيانات مع توفر الشروط المذكورة[2].

[1] قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(1996)، تاريخ الاعتماد: 12 حزيران/يونيه 1996، منشورات الأمم المتحدة، نيويورك، 2000.

[2] وائل أنور بندق، قانون التجارة الإلكترونية (قواعد الأونسيترال ودليلها التشريعي)، مكتبة الوفاء القانونية، الإسكندرية، مصر، الطبعة الأولى، 2009، ص 16.

المطلب الثاني: حجية الكتابة الإلكترونية وصورها

تعدُّ حجية الكتابة الإلكترونية من الموضوعات الحيوية في العصر الرقمي، حيث تساهم في تعزيز التواصل ونقل المعرفة بطريقة فعالة وسريعة، فإن فهم حجية هذه الكتابات يعدُّ أمرًا ضروريًا لتقييم مصادر المعلومات وتحديد موثوقيتها في مختلف المجالات (الفرع الأول)، هذا وتتنوع صور الكتابة الإلكترونية بشكل كبير، مما يعكس تطور وسائل التعبير في العصر الرقمي، إذ توفر الرسائل الإلكترونية والتقارير الرقمية وسيلة فعالة للتواصل المهني والشخصي بحيث تعكس هذه الصور تأثير التكنولوجيا على أساليب الكتابة والتفاعل مع الجمهور، مما يجعلها جزءًا أساسيًا من الحياة اليومية (الفرع الثاني).

الفرع الأول: حجية الكتابة الإلكترونية

الكتابة الإلكترونية أصبحت جزءًا لا يتجزأ من المعاملات اليومية، سواء كانت في السياقات الشخصية، التجارية، أو الحكومية. ومع التطور التكنولوجي، ظهرت تساؤلات حول حجية الكتابة الإلكترونية ومدى قبولها كدليل قانوني. في العديد من الأنظمة القانونية، تم الاعتراف بالكتابة الإلكترونية كوسيلة قانونية موثوقة للاتفاقيات والمعاملات، بشرط استيفائها لمعايير معينة مثل التوثيق الرقمي، التوقيع الإلكتروني، والسلامة من التزوير.

حجية الكتابة الإلكترونية تعتمد بشكل كبير على القدرة على إثبات صحة المستند الإلكتروني ومصدره، خاصة من خلال تقنيات مثل التوقيع الإلكتروني الذي يمنح الوثيقة نفس القوة القانونية التي تحظى بها المستندات الورقية الموقعة. علاوة على ذلك، العديد من القوانين الحديثة، مثل قوانين التجارة الإلكترونية وحماية البيانات، تضع إطارًا قانونيًا يعزز موثوقية وأمان المعاملات الإلكترونية، مما يعزز الثقة في استخدامها كأدلة في المحاكم والتعاملات الرسمية.

بشكل عام، الكتابة الإلكترونية معترف بها قانونيًا ما دامت تفي بالشروط التقنية والقانونية التي تضمن صحتها وسلامتها، مما يجعلها أداة فعالة وموثوقة للتوثيق في العصر الرقمي.

حجية الكتابة الإلكترونية تشير إلى الاعتراف القانوني بالإثباتات والوثائق التي تتم بشكل إلكتروني، والتي تستخدم تقنيات رقمية كبديل للكتابة التقليدية الورقية. مع تطور التكنولوجيا، أصبح من

الضروري تطوير أطر قانونية تتيح قبول الوثائق الإلكترونية في التعاملات اليومية، خاصة في مجالات مثل التجارة الإلكترونية، العقود الرقمية، والمراسلات الرسمية.

يمكن القول أن المشرع الجزائري عندما عدل القانون المدني، أخذ في الاعتبار المبادئ الواردة في القانون النموذجي للتجارة الإلكترونية، وأدرج المادة 323 مكرر 1 التي تنظر إلى الإثبات بالكتابة في شكل إلكتروني باعتباره كتابة ورقية بشرط أن يكون من الممكن التحقق من هوية الشخص الذي أصدرها وأن يتم إعدادها وحفظها في ظروف تضمن سلامتها، والواقع أن ما يمكن ملاحظته هنا هو أن المشرع الجزائري جعل الوثائق التي تصدر في شكل إلكتروني جزءًا من نظام الإثبات الكتابي التقليدي وأعطاها فعالية كاملة، وهذا حتى قبل أن يعالج الوثائق الإلكترونية فعليًا[1].

إن الوسائل التكنولوجية الحديثة التي أتاحت الكتابة الالكترونية كما هو الأمر في الفاكس والتلكس والحاسبات وغيرها، تدفع رجال القانون إلى تطوير المفهوم التقليدي للدليل الكتابي، بحيث يشمل هذا المفهوم الكتابة على دعامات غير ورقية تكون لها نفس الحجية في الإثبات، ما دام استخدام هذه الدعامات كان مصحوبا بآليات تكفل التحقق من هوية مرسل الرسالة ونسبتها إليها كاستخدام التشفير أو نظام الكود في التوقيع[2].

وفيما يخص مجال المحررات والتواقيع الإلكترونية، فإن الحجية تعتمد على الشروط السابقة الدراسة، على استخدام ضوابط وإجراءات إلكترونية، ومن خلال المادة 323 مكرر 1، فيمكن استنباط قرينة قانونية على سلامة المحرر المادية إلى غاية إثبات العكس، ويكون ذلك من خلال النص على الحجية الكاملة للمحرر الإلكتروني وهذا بشرط إعداده وحفظه في ظروف سلامته وإمكانية تحديد هوية من أصدره، فالكتابة أو المحرر الإلكتروني أصبح يتمتع بنفس الحجية التي يقررها القانون للكتابة الخطية إذا استوفى الشروط التي حددتها النصوص السابقة الذكر، فهناك من يرى بأن هذا الدليل سوف يحل محل الدليل الكتابي بعد تحول العالم إلى المجتمع الافتراضي والحكومة الإلكترونية.

---

[1] بن مبارك ماية، الإثبات الالكتروني في مجال القانون الخاص الجزائري، مجلة البحوث في العقود وقانون الأعمال، المجلد 7، العدد 2، 2022/06/10، ص 632.

[2] سلطان عبد الله محمود الجواري، عقود التجارة الالكترونية والقانون الواجب التطبيق – دراسة قانونية مقارنة، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، لبنان، 2010، ص 217.

ولكن استثناء هناك حالات لا يمكن فيها الاعتراف بالمحرر الكرتوني، وهي بدورها تنقسم إلى طائفتين اثتنين. تتمثل الطائفة الأولى في المعاملات ذات الشكلية الخاصة، وهي[1]:

- مسائل قانون الأسرة مثل الزواج والطالق والوصايا، التبني، الميراث، الوقف...إخ
- التصرفات العقارية الخاصة بنقل الملكية، إنشاء أو تسجيل أي حق من الحقوق العينية المتعلقة بالعقارات، وتقرير رهن أو امتياز عليها.
- عقود بعض الخدمات العامة لعقود المياه والكهرباء.
- الدعاوى القضائية وإعلانات الدعاوى والمرافعات وقرارات وأوامر المحاكم والإعلانات القانونية .

وأما الطائفة الثانية، فتتمثل في معاملات الأوراق المالية ومثالها السندات القابلة للتداول "الأسهم".

الفرع الثاني: صور الكتابة الإلكترونية

في عالم الكتابة الإلكترونية، تتنوع الأساليب والأنواع بحسب الأهداف والسياقات التي تُستخدم فيها، من أبرز هذه الأنواع نجد الكتابة الرسمية والكتابة العرفية، حيث تلعب كل منهما دورًا مهمًا في التواصل عبر الإنترنت.

يوجد فرق بين الكتابة والمحرر أو الوثيقة، فالكتابة عنصر مهم من عناصر المحرر، وبدونها يفقد المحرر قيمته، فالكتابة وحدها لا تكفي، بل لابد أن تتوفر فيها شروط معينة لتكون رسمية، فلابد أن تكون بالإضافة إلى الكتابة، مألوفة ومقصودة للإثبات، موقعة. والسؤال المطروح هنا هو: إلى أي مدى تفي الكتابة الإلكترونية بشروط المحرر الرسمي وكذلك المحرر المألوف حتى تكون لها حجية في الإثبات؟

أولا: الكتابة الرسمية الالكترونية

المستندات الإلكترونية هي تلك التي يتم التعبير عنها في شكل رقمي، سواء بلغة رسمية أو لغة متعارف عليها في المستندات، ومع القفزة الكبيرة في عدد العمليات الإلكترونية ووسائل الاتصال الحديثة، كان لا بد من إيجاد نصوص قانونية تضمن الاستفادة من هذه الوسائل وتكرس القوة الإثباتية

[1] بن مبارك ماية، مرجع سابق، ص 632-633.

لهذه الأخيرة، ومن هذا المنطلق تم إرساء مبدأ صحة التوقيع الإلكتروني والكتابة الإلكترونية المرتبطة به، بشرط توفر شروط معينة يجب توافرها حتى يصبح مقبولاً كدليل إثبات أمام القضاء.

لقد ساوى المشرع الجزائري بين الكتابة الخطية والكتابة الإلكترونية، إلا أنه لم يبين حدود هذه المساواة. وعليه، يفهم أنه في ظل هذه النصوص الرسمية في شكل الكتروني.

كما يفهم أنه اعتبر المحررات الإلكترونية الموقعة تتمتع بحجية المحررات العرفية فقط، من خلال نص المادة 327 من القانون المدني الجزائري، والتي اعتدت بالتوقيع الإلكتروني إذا ما حقق الشروط المنصوص عليها في كل من المادتين 323 مكرر و323 مكرر 1 ، خصوصا وأن التوقيع عنصر جوهري في المحرر العرفي الورقي، وبالتالي، فالتوقيع الإلكتروني عنصر جوهري كذلك في المحرر العرفي الإلكتروني، وقد يفهم هذا على أن استبعاد غير مباشر للمحررات الرسمية الإلكترونية، خصوصا أن تعديل القانون المدني كان في سنة 2005، والقانون الذي ينظم عمل هيئات المصادقة الالكترونية لم يصدر إلا في سنة 2005 لكن مع صدور القانون 04/15 والذي يعتبر بداية لما يسمى بالغير الموثق، والمتمثل في جهات المصادقة الإلكترونية؛ لا يستبعد وجود محررا ت إلكترونية رسمية، وفقا للشروط التي يضعها القانون[1].

إن أهم إشكالية في الإثبات بالمحررات الرسمية هي مسألة التفرقة بين أصل المحرر وصورته، إن الكتابة الإلكترونية تقتضي أن النسخة هي تكرار تام لأصلها مهما تعددت، فكل نسخة هي أصلية، وهذا ما أكده المشرع الفرنسي من خلال المادة 11/1316 من القانون المدني المعدل بالقرار رقم 2005/674 والتي تنص على أنه عندما يشترط إرسال عدة نسخ، فإن ذلك يمكن استيفاؤه من خلال الكتابة الالكترونية إذا كانت تلك الكتابة يمكن طباعتها من قبل المرسل إليه[2].

غير أنه تجدر الإشارة إلى أن المشرع الجزائري لم يتعرض إلى مسألة التفرقة بين أصل المحرر الالكتروني وصورته، رغم أنه ساوى بين المحررات الالكترونية والمحررات العرفية من حيث الحجية.

---

[1] غنية باطلي، الكتابة الالكترونية، المجلة الجزائرية لقانون الأعمال، كلية الحقوق والعلوم السياسية، المسيلة، العدد الثاني، ديسمبر 2020، ص 22.

[2] المرجع نفسه، ص 22.

إن المشرع الجزائري كرس مبدأ التعادل الوظيفي بين الكتابة على الشكل الإلكتروني والكتابة على الورق، وهو تأكيد على المساواة بين الكتابة التقليدية والكتابة الإلكترونية، أي لهما نفس الأثر والفعالية من حيث الحجية وصحة الإثبات، فللمحرر الإلكتروني حجية تضاهي حجة المحرر الرسمي إذا استجمع شروطه وأركانه المتطلبة قانوناً، ونستدل في ذلك بواقعة شراء أحد لاعبي كرة القدم لجزيرة بأكملها بواسطة عقد إلكتروني[1].

ثانيا: المحررات العرفية الالكترونية

الوثيقة العرفية هي تلك الوثيقة التي لا تحمل توقيع من أصدرها أو ختمه أو بصمة إصبعه، أو يمكن وصفها بأنها ليست وثيقة رسمية أي لا يصدرها موظف عام، كما يعرف البعض العقد العرفي بأنه أي عقد غير رسمي إلا إذا تدخل موظف بحكم وظيفته في إعداد العقد، فالوثيقة الإلكترونية العرفية هي التي يعدها شخص ليس موظفاً عاماً أو شخص مكلف بخدمة عامة تدخل في إعدادها، والوثائق الرسمية محاطة بالضمانات. وبذلك يمكن القول أن الوثائق العرفية هي تلك التي لا تنفذ أمام موظف عام أو ضابط عمومي أو موظف تحت يده؛ كما قد تكون وثائق فقدت أحد الشروط الرسمية التي تجعل منها وثيقة رسمية، فالمحرر الإلكتروني العرفي له حجية تتساوى والسند العادي في الإثبات.

تنص المادة 327 قانون المدني الجزائري على أنه يعتبر العقد العرفي صادرا ممن كتبه أو وقعه أو وضع عليه بصمة أصبعه ما لم ينكر صراحة ما هو منسوب إليه، أما ورثته أو خلفه فلا يطلب منهم الإنكار ويكفي أن يحلفوا يمينا بأنهم لا يعلمون أن الخط أو الإمضاء أو البصمة هو لمن تلقوا منه هذا الحق.

كما أن المادة 328 من القانون المدني أشارت إلى أن البيانات المدونة في المحرر العرفي تكون حجة على أطراف المحرر نفسه، بما في ذلك التاريخ الذي يؤكد صدور المحرر إلا أنه لا يكون نافذا في مواجهة الغير إلا من اليوم الذي يكون فيه التاريخ ثابتا، وذلك بهدف حماية هذا الغير من أي غش قد يرتكبه أحد الأطراف إضرارا به.

[1] أميمة لعروسي، حجية المحرر الالكتروني، موقع المكتب القانوني الالكتروني (e-legal office)، https://e-legaloffice.com/authentic-electronic-contract/، تم الاطلاع بتاريخ: 2024/08/17.

كما اشترطت المادة 328 من القانون المدني أن العقد العرفي لا يكون ثابتا إلا ابتداء من:

-من يوم تسجيله.

-من يوم ثبوت مضمونه في عقد آخر حرره موظف عام.

-من يوم التأشير عليه على يد ضابط عام مختص.

-من يوم وفاة احد الذين لهم على العقد خط و امضاء.

غير انه يجوز للقاضي تبعا للظروف، رفض تطبيق هذه الأحكام فيما يتعلق بالمخالصة.

فإذا كان العقد العرفي متوفر على هذه الشروط ما على صاحبه إلا التوجه الى أحد مكاتب التوثيق ليصب محتوى هذا العقد العرفي في عقد توثيقي ويودعه في المحافظة العقارية وبعد اشهار هذا العقد يمكن حينئذ التصرف في العقار " بيعه هبته أو رهنه.'' ...

أما صور المحررات العرفية فإنها تعرف بأنها ورقة منقولة عنها عن طريق الكتابة أو التصوير ولا تحمل توقيع من نسب إليه المحرر، وغالبا ما يكون توقيعه منقولا بطريق التصوير، وطبقا للقواعد العامة في الإثبات فإن الأصل العام أن صور المحررات العادية ليس لها حجية في الإثبات وذلك لأن الصورة هي نسخة تنقل عن المحرر الأصلي فتكون خالية من التوقيع، كما أن ليس لها صفة الرسمية كما هو الحال بالنسبة لصور المحررات الرسمية التي يقوم بتحريرها موظف عام[1].

يقصد بالنسخة الورقية من المستند الإلكتروني الورقة الناتجة عن طباعة المستند الإلكتروني على وسيط ورقي تقليدي، ولا تتمتع بأية قيمة إثباتية لأنها لا تحمل توقيعًا إلكترونيًا أو كتابيًا، وإذا تم استنساخ مستند إلكتروني إلكترونيًا، وأعطيت هذه النسخة الإلكترونية توقيعًا إلكترونيًا، ففي هذه الحالة تشكل هذه النسخة الأصل؛ عندما يتم توقيعها بهذه الطريقة ويجب أن يكون لها نفس القيمة الإثباتية للأصل.

[1] عائشة قصار الليل، حجية المحرر والتوقيع الإلكتروني في الإثبات، دراسة تحليلية مقارنة، رسالة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم الحقوق، باتنة، 2017، ص 212.

المبحث الثاني: إقرار الإثبات بالتوقيع الالكتروني

مع تطور التكنولوجيا وازدياد الاعتماد على الوسائل الرقمية في المعاملات اليومية، أصبح إقرار الإثبات بالتوقيع والتصديق الإلكترونيين أمرًا ضروريًا لضمان موثوقية وأمان الوثائق والمعاملات الإلكترونية، بحيث يعد التوقيع الإلكتروني أحد الأدوات القانونية التي تثبت هوية الموقع وتأكيد التزامه بالمحتوى (المطلب الأول)، بينما يأتي التصديق الإلكتروني ليضفي طابعًا قانونيًا ورسميًا على هذه التواقيع ليعطي حجية للتوقيع الالكتروني، مما يضمن عدم التلاعب أو التزوير، كما يهدف هذا النظام إلى تسهيل المعاملات وتبسيط الإجراءات مع المحافظة على الحماية القانونية للحقوق والمصالح (المطلب الثاني).

المطلب الأول: ماهية التوقيع الإلكتروني

في ظل التحول الرقمي المتسارع، أصبح التوقيع الإلكتروني أداة أساسية في إثبات صحة المعاملات والعقود التي تتم عبر الإنترنت، يعد التوقيع الإلكتروني وسيلة حديثة لتأكيد هوية الأطراف المتعاقدة، ويعزز الثقة في الوثائق الرقمية من خلال ضمان عدم التلاعب بمحتواها، ومع تزايد الاعتماد على الوسائل الإلكترونية في الحياة العملية، أصبح إثبات التوقيع الإلكتروني ضرورة ملحة لتأمين التعاملات الرقمية وضمان استمراريتها بما يتوافق مع الإطار القانوني الحديث، ويعد عنصرًا هامًا في تطوير الاقتصاد الرقمي.

الفرع الأول: تعريف التوقيع الإلكتروني

التوقيع الإلكتروني هو وسيلة رقمية تستخدم لإثبات هوية الموقع على وثيقة إلكترونية وتأكيد موافقته أو قبوله لمحتواها، يتميز التوقيع الإلكتروني بقدرته على توفير درجة عالية من الأمان والموثوقية، حيث يمكنه ضمان عدم التلاعب أو التزوير في البيانات الموقعة، ويعتبر بديلاً قانونيًا عن التوقيع التقليدي في العديد من الدول، حيث يحظى باعتراف قانوني ويمكن استخدامه في العقود والمعاملات الرسمية عبر الإنترنت، كما يعتمد التوقيع الإلكتروني عادة على تقنيات تشفير معقدة لضمان سرية المعلومات وصحة البيانات المتبادلة، مما يجعله أداة أساسية في التجارة الإلكترونية والخدمات الحكومية الرقمية.

أولا: تعريف التوقيع الالكتروني في القوانين المقارنة

يقصد بالتوقيع الإلكتروني، بيانات في شكل إلكتروني (بيانات فريدة مثل رموز أو مفاتيح التشفير الخاصة)، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق.

لا تعتبر الكتابة دليلا كاملا في الإثبات إلا إذا كانت مذيلة بالتوقيع والذي يعتبر العنصر الثاني من عناصر الدليل الكتابي، أو العنصر الثاني من عناصر الرسالة إلكترونية كانت أم خطية حتى يضفي عليها القانون حجية في الإثبات، وبالتوقيع يمكن نسبة الورقة إلى مصدرها حتى ولو كانت مكتوبة بخط غيره[1]، وفي هذا الشأن قضت محكمة التمييز الاتحادية في العراق أن إقرار المدعى عليه بتوقيعه على ورقة الدين المبرزة من قبل المدعي يثبت صدورها منه[2]، ذلك أن السندات العادية يكتمل بناؤها القانوني بالتوقيع، فإن خلت من التوقيع وكانت مكتوبة بخط يد مصدرها اعتبرت مبدأ ثبوت بالكتابة.

عرف القاموس الفرنسي الشهير Robert التوقيع بأنه: علامة شخصية يضعها الموقع باسمه بشكل خاص وثابت ليؤكد صحة مضمون الورقة وصدق ما كتب بها وإقراره بتحمل المسؤولية عنها[3].

وهناك من الفقه من عرف التوقيع الإلكتروني كذلك على أنه له معنيان المعنى الأول هو فعل أو عملية التوقيع ذاتها، أي واقعة وضع التوقيع على مستند يحتوي على معلومات معينة أو إشارات معينة تسمح بتمييز الشخص الموقع" أما المعنى الثاني وهو المقصود بالتوقيع في نطاق الإثبات وهو علامة خطية خاصة ومميزة يضعها الموقع بأية وسيلة على مستند لإقراره.

وقد ذهب جانب من الفقه إلى أن تعريف التوقيع الالكتروني عبارة عن مجموعة من المعلومات مدرجة بشكل الكتروني في رسالة بيانات أو مضافا عليها أو مرتبطا بها ارتباطا منطقيا، تستخدم لتحديد

---

[1] علي عبد العالي خشاب الأسدي، مرجع سابق، ص 76.

[2] قرار محكمة التمييز الاتحادية في العراق رقم 1014، استئنافية، 2005/11/12، قرار غير منشور.

[3] محمد السعيد رشدي، وسائل الاتصال الحديثة في الإثبات، مؤسسة دار الكتب للطباعة والنشر والتوزيع، الكويت، 1997، ص 40.

هوية وإثبات موافقته على فحوى الرسالة، وتؤكد سلامتها، ويشترط فيه ضرورة إتقانه وفقا لإجراءات حسابية وخوارزمية بحيث يستحيل سرقته، وتزوير مضمون السند[1].

كما نصت المادة 2 الفقرة (أ) من قانون الأونسيترال النموذجي بشأن التوقيعات الالكترونية على أن التوقيع الالكتروني يعني بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية المقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات[2].

كما تدخل المشرع الفرنسي بتعديل بعض نصوص القانون المدني لتتفق مع التوقيع على العقود والمحررات الالكترونية، فجاء في نص المادة 1316 من القانون المدني الفرنسي المعدلة بالقانون الصادر في 2000/03/13 بتعريف التوقيع بأنه التوقيع الذي يميز هوية صاحبه... وإذا ما تم التوقيع في شكل الكتروني وجب استخدام طريقة موثوق بها، لتميز هوية صاحبه[3].

وقد أصدر المجلس الأوروبي في 1999/12/13 التوجيه الأوروبي رقم 1999/93 الخاص بالتوقيعات الالكترونية، وتبنى هذا التوجيه في مادته الأولى أن الهدف منه تسهيل استعمال التوقيعات الالكترونية، والمساهمة بالاعتراف القانوني بها، وهو ينشئ إطارا قانونيا للتوقيعات الالكترونية وخدمات مصادقة معينة من أجل التوظيف الملائم للسوق الداخلي، وحدد في المادة 2 فقرة 1 التوقيع الالكتروني بأنه يعني بيانات في شكل إلكتروني، ترتبط أو تتصل قانونيا ببيانات الكترونية أخرى، وتستخدم كوسيلة للمصادقة، ونصت الفقرة 2 من المادة ذاتها على أن التوقيع الالكتروني المتقدم يعني توقيعا إلكترونيا يستوفي المتطلبات التالية:

- أن يكون مرتبطا بالموقع بشكل فريد؛
- أن يكون قادرا على تحديد هوية الموقع؛

---

[1] ضياء أمين مشيمش، التوقيع الالكتروني، دراسة مقارنة، المنشورات الحقوقية، بيروت لبنان، 2003، ص 124.

[2] عادل رمضان الأبيوكي، التوقيع الإلكتروني في التشريعات الخليجية (دراسة مقارنة)، المكتب الجامعي الحديث، الطبعة الأولى، الإسكندرية، مصر، 2009، ص 18.

[3] ممدوح محمد خيري هاشم المسلمي، مشكلات البيع الالكتروني عن طريق الانترنت في القانون المدني – دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2000، ص 161.

- أن ينشأ باستخدام وسائل يحتفظ بها الموقع تحت سيطرته هو فقط؛
- أن يكون مرتبطا بالبيانات التي تشير إليها على نحو يؤدي إلى اكتشاف أي تغيير لاحق أدخل على تلك البيانات[1].

ثانيا: تعريف التوقيع الالكتروني في التشريع الجزائري

عرّف المشرع الجزائري التوقيع الإلكتروني لأول مرة في نص المادة 327 فقرة 2 من القانون المدني الجزائري المعدلة بالقانون 10/05 التي تنص على أنه يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر1، ذلك من أجل إضفاء الحجية على المحررات الإلكترونية وأن يعتد بالتوقيع الإلكتروني بنفس الشروط التي يعتد بها السند الإلكتروني، وهذه الشروط تتمثل في التأكد من هوية الشخص الذي أصدره، ثم إعداده وحفظه بشكل يضمن سلامته وأهمل المشرع شرط التأكد من ارتضاء الموقع بما ورد في الوثيقة .

أما عن تعريف التوقيع الإلكتروني عرفه في المرسوم التنفيذي 162/07 في المادة 3 مكرر[2] منه على أن التوقيع الإلكتروني هو أسلوب عمل أو معطى يستجيب للشروط المحددة في المادتين 323 مكرر و323 مكرر 1 من الأمر 58/75 المتضمن القانوني المدني.

وعرف المشرع الجزائري التوقيع الالكتروني أيضا بموجب قانون التوقيع والتصديق الإلكتروني[3] في المادة 02 الفقرة 1 من القانون 04/15 بأنه بيانات إلكترونية في شكل إلكتروني مرفقة أو مرتبطة ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق وبالتالي نتبين أن المشرع الجزائري أقر بالتوقيع الإلكتروني كوسيلة توثيق إلا إنه لم يوضح الطريقة التي يستخدم بها، كما أنه قام بتعريفها تعريفا عاما بشكل يؤدي بالضرورة إلى اتساع نطاق مفهوم التوقيع الالكتروني.

---

[1] فادي محمد عماد الدين توكل، عقد التجارة الالكترونية، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، لبنان، 2010، ص 147/146.

[2] مرسوم تنفيذي رقم 162/07 مؤرخ في 30 ماي 2007 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، جريدة رسمية عدد 37 يعدل ويتمم للمرسوم التنفيذي رقم 123/01 المؤرخ في 09 ماي 2001.

[3] قانون رقم 04/15 مؤرخ 10 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، جريدة رسمية عدد 06 الصادرة في10 فيفري 2015.

الفرع الثاني: صور التوقيع الالكتروني

مع تزايد الاعتماد على التكنولوجيا الرقمية في مختلف المجالات، ظهرت أشكال متنوعة من التوقيع الإلكتروني التي تلبي احتياجات المستخدمين في بيئات متعددة، تتنوع هذه الأشكال من التوقيعات البسيطة التي تعتمد على التوقيع اليدوي الممسوح ضوئيًا، إلى التوقيعات الأكثر تعقيدًا التي تستخدم تقنيات التشفير والشهادات الرقمية لضمان الأمان والمصداقية.

أولا: التوقيع الرقمي أو الكودي- Digital Signature

التوقيع الرقمي أو البصمة الرقمية (Signature Numérique) يقصد به بيان أو معلومة يتصل بمنظومة بيانات أخرى أو صياغة منظومة في صورة شفرة (Code)[1]، فهو يتضمن عدة أرقام يتم تركيبها لتكون في النهاية كودا يتم التوقيع به ويستخدم في التعاملات البنكية والمراسلات الالكترونية التي تتم بين التجار أو بين الشركات وبعضها[2].

وقد أقر القضاء الفرنسي واعترف بصلاحية التوقيع الرقمي الذي يتم بواسطة شخص من خلال الرقم الخاص المستخدم في بطاقات الدفع، وهذا بالنسبة للاتفاقات المتعلقة بإثبات التصرفات[3].

ويذهب البعض إلى أن التوقيع الكودي بوصفه صورة من صور التوقيع الالكتروني يكون له ذات القوة التي هي للتوقيع التقليدي ما لم تكن قوته أفضل، وغالبا ما يرتبط التوقيع الكودي بالبطاقات البلاستيكية أو الممغنطة كبطاقة الفيزا، وماستر كارد وغيرها[4].

تعتبر هذه الصورة من صور التوقيع الالكتروني الأوسع انتشارا والأكثر أهمية وشهرة في نطاق التعامل الالكتروني، وغالبا ما يتم استخدامه بين التجار أو بين الشركات التجارية كما يستخدم في التعاملات المصرفية، وذلك بسبب طابع الأمان والموثوقية الذي يتميز به هذا التوقيع الالكتروني.

---

[1] سلطان عبد الله محمود الجواري، مرجع سابق، ص 183.

[2] فادي محمد عماد الدين توكل، مرجع سابق، ص 159.

[3] محمد أحمد محمد نور إسماعيل، مدى حجية التوقيع الإلكتروني في عقود التجارة الالكترونية، أطروحة دكتوراه، كلية الحقوق، القاهرة، مصر، 2008، ص 88.

[4] عادل رمضان الأبيوكي، مرجع سابق، ص 20.

ثانيا: التوقيع البيومتري (التوقيع باستخدام الخواص الذاتية) – Biometric Signature

هذا التوقيع يتطلب دراسة الخواص الذاتية (الشخصية) للإنسان مثل بصمة إصبعه، أو بصمة عينه (مسح شبكية العين) أو شفته أو نبرة الصوت أو طبيعة خطه من خلال اهتزازات اليد عند الكتابة أو الضغط على القلم[1]، غير أنه تجدر الإشارة إلى أن هذه الصورة من التوقيع الالكتروني قد وجهت إليها العديد من الانتقادات والتي تتمثل في[2]:

- تتعرض هذه الصورة من صور التوقيع الالكتروني للتزوير كشخص مثلا يرتدي عدسات لاصقة يتم تصميمها بالكمبيوتر بحيث تكون مطابقة لقزحية العين للشخص المراد انتحال صفته.
- يمكن نسخها أو مهاجمتها من طرف قراصنة الحاسب الآلي عن طريق فك شفرتها.
- لا يتلاءم هذ النوع من التوقيعات مع الحاسبات الآلية للأشخاص العاديين.
- يتطلب هذا النوع من التوقيع الالكتروني إلى استثمارات ضخمة لتمكين مستخدمي الشبكة الالكترونية من استخدام الخصائص الذاتية لشخص الموقع في التوقيع الالكتروني.

غير أنه رغم كل تلك الانتقادات إلا أن هذه الصورة من التوقيع تنتشر بصورة أكبر وذلك نتيجة للتطور التكنولوجي المتسارع قد يأتينا بحلول أسرع للتغلب على مشكلاتها الفنية وتكاليفها الباهظة.

وقد نجد هذا التوقيع الالكتروني غالبا في المطارات الدولية بحيث يتم استعماله للتعرف على هوية المسافر وحفظها بالبيانات المحفوظة بالكمبيوتر.

ثالثا: التوقيع بالقلم الالكتروني – PEN-OP

يقوم هنا مرسل الرسالة بكتابة توقيعه الشخصي باستخدام قلم إلكتروني (Pen-Computer Signature)، وهو خاص على شاشة الحاسب الآلي عن طريق برنامج معين، ويقوم هذا البرنامج بوظيفتين أساسيتين لهذا النوع من التوقيعات، الأولى هي خدمة التقاط التوقيع The Signature

[1] عصمت عبد المجيد بكر، أثر التقدم العلمي على العقد – تكوين العقد، إثبات العقد، دار صباح صادق جعفر، بغداد، العراق، 2007، ص 112.

[2] عادل رمضان الأبيوكي، مرجع سابق، ص 21.

Capture Service والثانية هي خدمة التحقق من صحة التوقيع The Signature Verification Service[1].

تعتمد هذه الطريقة على استخدام قلم إلكتروني خاص، حيث يقوم المتعامل بكتابة توقيعه الشخصي على شاشة الحاسب الآلي، ويتم التحقق من صحة التوقيع عن طريق برنامج خاص، وذلك بالاستناد إلى حركة القلم والأشكال التي يتخذها من دوائر وانحناءات والتواءات، ولكي يستطيع التعامل لا بد من مطابقة توقيعه للتوقيع المحفوظ بذاكرة الحاسب الآلي[2].

إن استخدام هذه الطريقة محفوف بالعديد من المشكلات التي لم تجد طريقها إلى الحل لحد الآن وهي مشكلة إثبات العلاقة بين التوقيع والرسالة الالكترونية إذ لا توجد تقنية تحدد هذه الرابطة إذ بإمكان المرسل إليه الاحتفاظ بنسخة من التوقيع التي وصلته على أحد الرسائل الالكترونية ثم يعيد وضعها على أي رسالة إلكترونية أخرى ويدعي أن واضعها هو صاحب التوقيع الفعلي وهو ما يؤدي إلى انعدام الثقة والأمان في هذه الطريقة التي تتطلب حاسوب قلمي بمواصفات خاصة علاوة على ما يتطلبه من كلفة مرتفعة[3].

رابعا: التوقيع باستخدام البطاقات الممغنطة المقترنة بالرقم السري

يتم هذا التوقيع بالموافقة على عمليات السحب النقدي أو السداد بالبطاقة، بحيث يستطيع كل شخص يمتلك جهاز كمبيوتر موصول بشبكة الانترنت أن يقوم بإدخال رقم بطاقته الصادرة من أي البنوك أو مؤسسات الائتمان في المكان المخصص لذلك عندما يطلب منه، فهي تماما كما لو كان العميل يستعملها خارج جهاز الكمبيوتر فهو إن أراد سحب مبلغ نقدي فما عليه إلا أن يدخل بطاقته

[1] عايض راشد المري، مدى حجية الرسائل التكنولوجية الحديثة في إثبات العقود التجارية، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 1998، ص 114.

[2] عادل رمضان الأبيوكي، مرجع سابق، ص 22.

[3] سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة، دار النهضة العربية، القاهرة، مصر، 2006، ص 226.

إلى المكان المخصص في جهاز الصرف الآلي ATM ويدخل الرقم السري والذي غالبا ما يكون من اختيار الشخص العميل ويتصف بالسرية[1].

غير أن ما يؤخذ على هذه الطريق في التوقيع الالكتروني هو إمكانية سرقة البطاقة أو ضياعها أو إمكانية الحصول على بياناتها مع الرقم السري لشخص ما وبالتالي استعمالها دون موافقة مالكها.

خامسا: التوقيع عن طريق تحويل الخط اليدوي إلى توقيع إلكتروني

يقصد به نقل توقيع الشخص المحرر بخط اليد عن طريق تصوير الماسح الضوئي Scanner، ثم نقل هذه الصورة إلى الملف الذي يراد إضافة التوقيع إليه عبر شبكات الاتصال الالكتروني لإعطائه الحجية اللازمة[2]، بحيث يتم نقل التوقيع المكتوب بخط اليد بهذه الطريقة بصورة رسوم بيانية يحفظ على وسائط إلكترونية في ذاكرة الحاسب الآلي، ثم نقل هذه الصورة من التوقيع إلى السند أو الملف الذي يراد إضافة هذا التوقيع لاستكماله، ويتم ذلك عن طريق شبكة الانترنت أو عن طريق شرائط ممغنطة أو أسطوانة ممغنطة تمهيدا لاستخدامه على السند المراد إضافة التوقيع إليه[3].

ورغم أن هذه الصورة تعتبر مرنة وسهلة الاستعمال كما تبدو، إلا أن استعمالها يتسبب في العديد من المشاكل أبرزها مسألة لإثبات الصلة بين التوقيع ورسالة البيانات أو المحرر، بحيث أنه يمكن للمرسل إليه الاحتفاظ بنسخة من التوقيع ووضعها على أي وثيقة محررة عبر وسيط إلكتروني ثم يدعي أن التوقيع تم وضعه من طرف صاحب التوقيع الأصلي، وبذلك فإن هذه الصورة من صور التوقيع الالكتروني لا توفر أي درجة من درجات الثقة والأمان في التوقيع الالكتروني.

سادسا: التوقيع بالضغط على مربع الموافقة OK-BOX

قد يحدث في الكثير من العقود الالكترونية أن تتم الموافقة على إبرام العقد من خلال النقر على زر الموافقة في المكان المخصص لذلك بلوحة مفاتيح الكمبيوتر، أو بالضغط على الخانة المخصصة

---

[1] فادي محمد عماد الدين توكل، مرجع سابق، ص 164.

[2] عصمت عبد المجيد، مرجع سابق، ص 102.

[3] سمير حامد عبد العزيز الجمال، مرجع سابق، ص 225.

للقبول في نموذج العقد المعروض على شاشة الكمبيوتر، هذا وقد يطلب من العميل لزيادة التأكيد على الموافقة ضرورة الضغط مرتين Double Click لضمان الجدية في التعامل[1].

غير أن هذه الطريقة لا تعتبر في حد ذاتها توقيعا، بالدرجة التي تجعل المحرر الالكتروني يكتسب كل العناصر التي تجعل منه دليلا كافيا، لذلك غالبا ما يتم اللجوء إلى إضافة جانب إضافي في نموذج التعاقد لإضافة الرقم السري بالإضافة إلى إمكانية استخدام المفتاح الخاص الذي على أساسه تمنح الشهادة الخاصة به[2].

سابعا: التوقيع عن طريق استخدام بطاقات الدفع الإلكتروني

البطاقات الممغنطة والمقترنة برقم سري والتي تسمى أيضا بطاقات الاعتماد، أو بطاقات الدفع الالكتروني والتي تصدرها مؤسسات مالية وهي بطاقة بلاستيكية مستطيلة تحمل اسم المؤسسة المصدرة لها وشعارها وتوقيع حاملها بشكل بارز على وجه البطاقة ورقمها واسم حاملها ورقم حسابه وتاريخ انتهاء صلاحيتها ويمكن لكل شخص أن يستخدم هذه البطاقات حتى لو لم يكن لديه حاسب آلي أو لم يكن متصلا بشبكة الانترنت[3].

هذا النوع من التوقيع الالكتروني يحوز قدرا كبيرا من الثقة والأمان ويبعث على الطمأنينة في تأكيد انتساب التوقيع إلى الموقع، لكن يؤخذ عليه أنه ينفصل ماديا عن الموقع مما يؤدي إلى إمكانية حصول أي شخص من الغير على البطاقة، وفي حال تعرفه على الرقم السري الذي قد يهمل صاحبه في حفظه، ومن جهة ثانية أنه يتعارض مع قاعدة اصطناع الخصم دليلا لنفسه لأن الذي يصدر البطاقة هو المصرف مصدر البطاقة في مواجهة العميل، وعند نشوء نزاع يتعلق بعملية السحب الذي يقوم بها هذا الأخير، فإن المصرف هو الذي يتمسك بالتوقيع تجاه العميل[4].

أما بالنسبة لصور التوقيع الالكتروني في التشريع الجزائري فإنه بالرجوع الى أحكام القانون رقم 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني، نجد أن المشرع الجزائري قد

---

[1] Alain Bensoussan, Le commerce électronique, aspects juridique, édition HERMES, Paris, 1998, P 34.

[2] فادي محمد عماد الدين توكل، مرجع سابق، ص 164.

[3] علي عبد العالي خشاب الأسدي، مرجع سابق، ص 92.

[4] ثروت عبد الحميد، التوقيع الالكتروني، دار النيل للطباعة والنشر، مصر، 2001، ص 57.

تعرض إلى نوع وحيد من أنواع التوقيع الإلكتروني وهو التوقيع الإلكتروني الموصوف والذي نص عليه في المادة 7 بقوله هو التوقيع الذي يتوفر على الشروط التالية:

- أن ينشأ على أساس شهادة للتصديق الإلكتروني الموصوف.
- أن يرتبط بالموقع دون سواه.
- أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.
- أن يكون مرتبط بالبيانات الخاصة به، بحيث يمكن الكشف عن التغيرات اللاحقة أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع بهذه البيانات.

وبالرجوع إلى نص المادة 8 من القانون 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني نجد المشرع الجزائري قد اعتبر التوقيع الموصوف وحده الممثل للتوقيع الإلكتروني.

الفرع الثالث: خصائص وعيوب التوقيع الالكتروني

أولا: خصائص التوقيع الالكتروني

يتميز التوقيع الالكتروني بجملة من المميزات والخصائص تميزه عن التوقيع العادي، تتمثل في ما يلي:

1/- يرد التوقيع الالكتروني على وسيط إلكتروني بوسيلة إلكترونية

فالتوقيع الإلكتروني عبارة عن مجموعة من الإجراءات تكون على شكل حروف أو أرقام أو رموز أو شفرة أو صوت.

إن برنامج الحاسب الآلي أو أي وسيلة أخرى تستعمل من أجل تنفيذ إجراء أو الاستجابة بصدد إنشاء أو إرسال التوقيع الالكتروني وذلك بوسيلة إلكترونية أيا كانت، أي من خلال الوسائل التقنية الحديثة[1].

[1] عادل رمضان الأبيوكي، مرجع سابق، ص 34.

2/- التوقيع الالكتروني يرتبط برسالة إلكترونية

أي أن التوقيع الالكتروني يتصل برسالة إلكترونية، هذه الأخيرة عبارة عن معلومات يتم إنشاؤها أو إرسالها وتخزينها عن طريق وسيلة إلكترونية مثل البريد الإلكتروني أو التلكس وغيرها.

3/- يهدف التوقيع الالكتروني إلى تحقيق أغراض ووظائف التوقيع التقليدي

إن صحة التوقيع الالكتروني ونسبته إلى موقعه والتثبت منه يجعل منه بديلا للتوقيع العادي، بحكم التطور الذي تعرفه وسائل الاتصال عن بعد وفق التقنيات الحديثة.

4/- الأمن والخصوصية

إن إمكانية تحديد هوية المرسل والمستقبل إلكترونيا والتأكد من مصداقية الأشخاص والمعلومات، بحيث يساهم في حماية المؤسسات من عمليات تزوير التوقيعات، وذلك ما يضفي على التوقيع الالكتروني درجة عالية من الأمن والخصوصية بالنسبة للمتعاملين.

5/- السرعة

يوفر التوقيع الالكتروني الكثير من الوقت والجهد باعتبار أنه ينجز العديد من المعاملات في وقت وجيز مما يساهم في ازدهار المعاملات الإلكترونية بشكل عام والتجارة الإلكترونية بشكل خاص، مثال ذلك: يعمل التوقيع الالكتروني على التيسير على المتعاملين للحصول على ما يحتاجونه من سلع وخدمات دون الحاجة لنقل النقود، كما تمكنهم من شراء ما يحتاجونه حتى ولو لم يكن بحوزتهم أموال نقدية سائلة[1].

6/- التوقيع الإلكتروني أكثر تعقيدا من التوقيع العادي

التوقيع الإلكتروني غير قابل لتحديد هوية الموقع بصورة مباشرة، كونه يحتاج إلى برامج خاصة للتأكد من صحة التوقيع وعدم تعرضه للتلاعب، إضافة إلى أن التوقيع الالكتروني لا يعتبر توقيعا

[1] عادل رمضان الأبيوكي، المرجع السابق، ص 36.

شخصيا لأن استخدامه مقيد بحسب الكتابة الالكترونية، وبالتالي لا بد من تقنيات تكنولوجية تكفل ضمان استخدام التوقيع الالكتروني حتى يقره القانون[1].

ثانيا: عيوب التوقيع الإلكتروني

على الرغم من الإيجابيات الكثيرة التي تميز التوقيع الالكتروني عن التوقيع العادي إلا أن هناك بعض الجوانب السلبية التي تشكل خطرا على سلامة وضمان التوقيع والمستند الذي يتضمنه، وتتمثل هذه العيوب في ما يلي:

1/- القيمة المكلفة للتوقيع الإلكتروني

من عيوب التوقيع الإلكتروني أن تكلفته قد تكون مرتفعة نسبيًا. هذه التكلفة تشمل الحصول على شهادة رقمية من هيئة معتمدة، والتي قد تكون مكلفة لبعض الأفراد أو الشركات الصغيرة. بالإضافة إلى ذلك، تتطلب الأنظمة المستخدمة في إدارة وتطبيق التوقيع الإلكتروني أجهزة وبرمجيات متخصصة، مما يزيد من التكلفة الإجمالية. قد تتطلب بعض الدول أو المؤسسات أيضًا دفع رسوم تجديد دورية للشهادات الرقمية، مما يضيف أعباء مالية مستمرة.

لذلك يرى بعض الفقه أن ارتفاع كلفة التوقيع الالكتروني يعد أحد العيوب التي تعتريه، الأمر الذي يحتم إيجاد حل لهذه المشكلة.

2/- إساءة استعمال التوقيع الإلكتروني أو استعماله من قبل الغير

أحد العيوب الرئيسية للتوقيع الإلكتروني هو احتمالية إساءة استعماله أو استخدامه من قبل أشخاص غير مخولين. إذا تم اختراق بيانات المستخدم أو سرقة الشهادة الرقمية الخاصة به، يمكن للطرف الآخر استخدام التوقيع الإلكتروني للقيام بتصرفات غير مشروعة باسم الشخص أو الشركة المالكة. هذا الأمر يشكل تهديدًا لأمان المعاملات الإلكترونية، وقد يؤدي إلى خسائر مالية أو قانونية كبيرة. بالإضافة إلى ذلك، صعوبة التحقق من هوية الشخص الفعلي الذي يستخدم التوقيع قد تزيد من احتمالية حدوث عمليات تزوير.

[1] ثروت عبد الحميد، مرجع سابق، ص 24.

مثال ذلك: التوقيع الكودي واستعمال البطاقة المصرفية، حيث يتم استعمال البطاقة من قبل الغير وبالتالي صرف مبالغ مالية بدون وجه حق، كحصول هذا الغير على البطاقة بطريق السرقة أو العثور عليها بعد ضياعها من صاحبها فيقوم الغير بسحب النقود أو يقوم بالوفاء بقيمة عملياته التجارية بتلك البطاقة المملوكة لغيره[1].

3/- إمكانية تزوير التوقيع الإلكتروني

رغم أن التوقيع الإلكتروني يُعتبر آمناً بشكل عام، إلا أن هناك احتمالات لتزويره. يمكن للمهاجمين سرقة المفاتيح الخاصة التي يستخدمها الأفراد أو الشركات في توقيع الوثائق، مما يؤدي إلى استخدام تلك المفاتيح لتزوير التوقيعات.

رغم التقنيات المتقدمة المستخدمة في تأمين التوقيع الإلكتروني، إلا أن هناك دائماً احتمالية لحدوث تزوير. إذا تمكن المجرمون من الوصول إلى مفاتيح التشفير الخاصة أو اختراق النظام، يمكنهم بسهولة توقيع وثائق رسمية وتحويل الأموال بشكل غير قانوني. رغم التقنيات المتقدمة المستخدمة في تأمين التوقيع الإلكتروني، إلا أن هناك دائماً احتمالية لحدوث تزوير. إذا تمكن المجرمون من الوصول إلى مفاتيح التشفير الخاصة أو اختراق النظام، يمكنهم بسهولة توقيع وثائق رسمية وتحويل الأموال بشكل غير قانوني.

4/- تشجيع عمليات غسل الأموال

مع تزايد الاعتماد على التوقيع الإلكتروني في المعاملات الرقمية، أصبحت التكنولوجيا تلعب دورًا حيويًا في تسهيل الأعمال وتبسيط الإجراءات. ومع ذلك، فإن هذا التطور السريع يأتي أيضًا مع تحديات ومخاطر، منها استخدام التوقيع الإلكتروني كأداة محتملة لتسهيل الجرائم المالية مثل غسل الأموال. غسل الأموال هو عملية تحويل الأموال المكتسبة بطريقة غير شرعية إلى أموال ذات مظهر قانوني. في هذا البحث، سنستعرض كيف يمكن للتوقيع الإلكتروني أن يساهم في تشجيع عمليات غسل الأموال، مع التركيز على العيوب الأمنية والتشريعية التي تفتح المجال أمام هذه الأنشطة غير القانونية.

[1] نجوى أبو هيبة، التوقيع الالكتروني (تعريفه– مدى حجيته في الإثبات)، دار النهضة العربية، مصر، دون سنة نشر، ص 99.

الفرع الرابع: وظائف التوقيع الالكتروني

يتم تحديد مفهوم التوقيع عموما بناء على الوظائف التي يؤديها، لذلك وجب علينا معرفة ما إذا التوقيع الالكتروني باعتباره يتم بوسائل الكترونية يقوم بذات الوظائف التي يقوم بها التوقيع العادي، ذلك سنتبين وظائف التوقيع الالكتروني: التثبت من هوية صاحب التوقيع، التعبير عن رضا صاحب التوقيع، التوقيع الالكتروني يدل على حضور صاحب التوقيع، التصديق على محتوى المحرر ومنحه صفة الأصل.

أولا: التثبت من هوية صاحب التوقيع

إن العبرة في التوقيع أن يكون مميزا لشخصية صاحبه ويعبر عن هويته، وإرادته في الالتزام بمضمون السند، ولا يهم شكل التوقيع لأن الشكل غير مقصود لذاته.

فحتى يكون العقد صحيحا لا بد من أن يصدر من جائز التصرف وبرضاه حتى تترتب عليه آثار العقد من تملك المشتري للمبيع وتسليم الثمن للبائع في عقد البيع مثلا، ولذا لا بد من تعيين طرفي العقد، فالبائع على شبكة الإنترنت يدون البيانات التي تثبت هويته كما أن المشتري يقوم بتدوين البيانات التي تثبت هويته، ويكون العقد مذيلا بتواقيع رقمية تؤكد شخصية طرفي العقد وهي طريقة إثبات هوية طرفي العقد[1].

ولقد عرف المشرع الجزائري الموقع في المادة 3 مكرر بأنه شخص طبيعي يتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله ويضع موضع التنفيذ جهاز إنشاء التوقيع الالكتروني، وبالتالي يتبين أن المشرع الجزائري حدد هوية الموقع أو شخصيته بتعبير عن الحساب الخاص للموقع أو حساب الشخص الطبيعي أو المعنوي الذي يمثله، فهو قد حدد ذاتية الشخص أو ذمته[2].

[1] عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الالكترونية (الحاسب الآلي وشبكة المعلومات "الإنترنت")، دار الوراق، دار النيربين للطباعة والنشر والتوزيع، الطبعة الثالثة، 2006، ص 146.

[2] بلقاسم حامدي، إبرام العقد الإلكتروني، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص قانون الأعمال، جامعة الحاج لخضر، باتنة، 2015، ص 216.

ثانيا: التعبير عن رضا صاحب التوقيع

التوقيع الالكتروني شأنه شأن التوقيع العادي فهو يدل على رضا صاحب التوقيع بما هو مدون في المحرر وقبوله بمحتواه، فمتى قام الموقع بوضع توقيعه إلكترونيا على محتويات المحرر فإن ذلك يعتبر قرينة على رضاه وقبوله بمحتوى ذلك المحرر.

نصت المادة 327 من القانون المدني الجزائري، أن العقد يعتبر صادر ممن وقعه ما لم ينكره، كما نصت المادة 01 من القانون 15/-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين الخاص أنه يحوز حصريا الموقع فقط ويستخدم لإنشاء التوقيع الإلكتروني، وعليه فكل من يوقع إلكترونيا على المحرر تحدد هويته وتوثق وهذا ما نصت عليه المادة 02 من القانون 04/15.

ثالثا: التوقيع الالكتروني يدل على حضور صاحب التوقيع

التوقيع الالكتروني على عكس التوقيع العادي لا يمكن توقع حضور الموقع شخصيا، لذلك اختلف الفقه حول هذه المسألة وانقسم إلى قسمين[1]:

الرأي الأول: يرى أن قيام صاحب البطاقة بسحب النقود من جهاز الصرف الآلي، بإدخال البطاقة مصحوبة بالرقم السري، فهذا يدل على حضور الشخص ذاته صاحب التوقيع الالكتروني وقت إدخال الرقم السري.

الرأي الثاني: يرى أنه لا يجوز مطلقا معادلة التوقيع الالكتروني بالتوقيع اليدوي بحيث لا يمكن مع التوقيع الالكتروني التأكد من حضور الموقع ومن وجوده فعلا وقت التوقيع.

إن التثبت من حضور الشخص حضورا حقيقيا ماديا يختلف بحسب الصورة التي تم بها التوقيع، فالتوقيع الالكتروني لا يقتصر على بطاقة الصرف الآلي فحسب، لأن له عدة صور مختلفة، وبالتالي فإن مسألة التأكد من حضور الشخص فعليا يجد ضالته في بعض ور التوقيع (كبصمة الإصبع مثلا) بينما يكون حضور الشخص في أحوال أخرى حكميا لا حقيقيا[2].

---

[1] نجوى أبو هيبة، مرجع سابق، ص 82.

[2] عادل رمضان الأبيوكي، مرجع سابق، ص 32.

رابعا: التصديق على محتوى المحرر ومنحه صفة الأصل

بمجرد التوقيع الالكتروني على المحرر فإن ذلك يعد تصديقا على ما ورد به من معلومات وبيانات، وبالتالي يصبح بذلك نسخة أصلية تكون حجيتها في الإثبات قائمة متى توافرت شروط التوقيع، غير أن المشكلة المطروحة تتعلق بالحالة التي يحتفظ فيها مستقبِل التوقيع الالكتروني بنسخة من التوقيع ليضعها على محرر آخر، بحيث يصبح في هذه الحالة نسخة أصلية أيضا، وبالتالي يقع على صاحب التوقيع إثبات تزوير توقيعه بالاستعانة بالخبراء، وهو أمر ليس سهلا من حيث الإثبات[1].

المطلب الثاني: حجية الإثبات بالتوقيع الالكتروني

إن حجية التوقيع الإلكتروني ترتبط ارتباطا وثيقا باستيفائه للشروط اللازمة للاعتداد به كتوقيع كامل، ولهذا بادرت العديد من الدول إلى تضمين نصوصها القانونية المنظمة للتوقيع الإلكتروني قوة الثبوتية لهذا الأخير، وتعادل تلك الممنوحة للتوقيع العادي بوضعها أحكاما خاصة بحجيته قاطعة لكل جدل حوله ذلك.

الفرع الأول: شروط تحقق حجية التوقيع الالكتروني

يرى جانب من الفقه القانوني أن الشكل الذي تطلبه القانون في التوقيع لا يتوافر في التوقيع الالكتروني، ومن ثم تصبح حجية هذا التوقيع محل شك، مما يؤدي إلى التقليل من فرص الاستفادة من الإمكانيات التي تتيحها نظم معالجة البيانات المنقولة إلكترونيا على إنجاز المعاملات في أقل وقت وبإجراءات آمنة.

أولا: أن يكون التوقيع الالكتروني خاصا بصاحبه وينفرد به

يشترط في التوقيع الإلكتروني أن يكون خاصاً بصاحبه وينفرد به حتى يتمتع بالمصداقية والأمان. هذا الشرط يضمن أن التوقيع الإلكتروني يعبر فقط عن الشخص الذي قام بإصداره ولا يمكن تزويره أو تقليده بسهولة. لتحقيق هذا الشرط، يتم عادة استخدام تقنيات تشفير متقدمة تضمن أن التوقيع الإلكتروني مرتبط بهوية محددة ولا يمكن لأي شخص آخر استخدامه.

[1] عادل رمضان الأبيوكي، المرجع السابق، ص 32-33.

فالتوقيع الالكتروني يدل على شخصية صاحبه ويميزها عن غيره، لأن التوقيع سيرتب آثارا قانونية على صاحب التوقيع دون غيره، طالما استوفى التوقيع الالكتروني كل الشروط القانونية.

ثانيا: سيطرة الموقّع على توقيعه الالكتروني

يشترط أن يكون الموقّع مسيطراً بشكل كامل على توقيعه الإلكتروني، وهذا يعني أن الموقّع يجب أن يكون الوحيد الذي يمتلك القدرة على إنشاء التوقيع الإلكتروني واستخدامه. هذا الشرط يضمن أن عملية التوقيع تتم بإرادة الموقّع نفسه دون تدخل أو وصول غير مصرّح به من طرف ثالث.

من الناحية الفنية تتحقق سيطرة الموقع وحده دون غيره على الوسيط الالكتروني المستخدم في عملية التوقيع الالكتروني عن طريق حيازة الموقع لأداة حفظ المفتاح الشفري الخاص متضمنة البطاقة الذكية المؤمنة والكود السري المقترن بها[1].

ثالثا: إمكانية اكتشاف أي تعديل أو تبديل يطرأ على التوقيع الالكتروني أو المستند

يشترط في التوقيع الإلكتروني أن يكون هناك إمكانية لاكتشاف أي تعديل أو تبديل يطرأ على التوقيع الإلكتروني أو المستند الموقّع. هذا الشرط يعد من أهم عناصر الأمان في التعاملات الإلكترونية، حيث يضمن أن التوقيع الإلكتروني والمستند المرافق له يظلان موثوقين وغير قابلين للتلاعب بعد التوقيع.

لتحقيق هذا الشرط، يتم استخدام تقنيات عديدة مثل:

1/- استخدام تقنية التجزئة للكشف عن التعديلات (Hashing): تقنية التجزئة تُعد من أهم الطرق المستخدمة في التوقيعات الإلكترونية للكشف عن أي تعديل في المستند، عند توقيع المستند إلكترونيًا، يتم إنشاء قيمة تجزئة فريدة للمستند بأكمله، أي تعديل في المستند، حتى لو كان بسيطًا، سيؤدي إلى تغيير في قيمة التجزئة، وبالتالي يسهل اكتشاف التلاعب[2].

[1] محمد أمين الرومي، النظام القانوني للتوقيع الالكتروني، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص 61.

[2] Jonathan Katz & Yehuda Lindell, Introduction to Modern Cryptography: Principles and Protocols, Chapman and Hall/CRC, 2007, P 113-118.

2/- استخدام التشفير الرقمي لضمان سلامة المستندات: التشفير الرقمي يرتبط بالتوقيع الإلكتروني لضمان أن أي تعديل في المستند بعد التوقيع يمكن اكتشافه بسهولة. يعتمد التشفير على وجود مفتاح خاص لإنشاء التوقيع ومفتاح عام للتحقق منه. إذا تم تعديل المستند، فإن المفتاح العام لن يتمكن من التحقق من التوقيع الأصلي، وبالتالي سيتم الكشف عن التعديل[1].

3/- الشهادات الرقمية للكشف عن التعديلات (Digital Certificates) : تُستخدم الشهادات الرقمية للتحقق من هوية الموقّع وضمان سلامة المستند، تعمل الشهادات الرقمية كوثيقة إلكترونية تربط هوية الموقّع بمفتاحه العام، وتستخدم أيضًا لاكتشاف أي تغيير في التوقيع أو المستند، وفي حالة تعديل المستند بعد توقيعه، ستفشل عملية التحقق باستخدام الشهادة الرقمية[2]، هذه الشهادات تُستخدم للتحقق من مصدر التوقيع الإلكتروني ومنع الاحتيال.

4/- **تقنيات متقدمة مثل blockchain لضمان عدم التلاعب:** أصبحت تقنية **Blockchain**جزءاً مهماً في تحقيق سلامة التوقيعات الإلكترونية والمستندات، لأنها توفر سجلاً غير قابل للتغيير للمعاملات والتوقيعات، يُستخدم في هذا السياق لتسجيل التوقيعات الرقمية بطريقة تسمح بالكشف عن أي تلاعب أو تغيير، مما يعزز أمان المعاملات الإلكترونية[3].

5/- توقيعات التشفير غير القابلة للتزوير(Digital Signatures) : التوقيعات الرقمية تعتمد على خوارزميات تشفير قوية لضمان عدم قدرة أي شخص على تعديل التوقيع الإلكتروني أو المستند المرافق له، يتم إنشاء التوقيع باستخدام مفتاح خاص، ويتم التحقق منه باستخدام مفتاح عام، إذا تم تعديل المستند بعد التوقيع، فسيتم اكتشاف التعديل لأن التوقيع الأصلي لن يتطابق مع المستند المعدّل[4].

---

[1] Douglas R. Stinson & Maura Paterson, Cryptography: Theory and Practice, CRC Press, 4th édition, 2018, P 347.

[2] Eric RescorlaEric Rescorla, SSL and TLS: Designing and Building Secure Systems, Addison-Wesley Professional, First édition, 2001, P 197.

[3] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, 2008.

[4] Ronald L. Rivest, Adi Shamir, Leonard Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, Association for Computing Machinery (ACM), https://dl.acm.org/doi/10.1145/359340.359342.

إن التوقيع الالكتروني وإن كان لا يناظر التوقيع الخطي التقليدي من حيث الشكل إلا أنه يناظره من حيث الوظيفة والهدف والحجية، ويبقى الاختلاف الجوهري بينهما في الوسيلة المستخدمة حيث يتم التوقيع الالكتروني باستخدام وسائط إلكترونية[1].

الفرع الثاني: حجية التوقيع الالكتروني في التشريع الجزائري

التوقيع الإلكتروني في التشريع الجزائري يعتبر وسيلة فعالة لإثبات صحة الوثائق الإلكترونية والالتزام بمحتواها، ويتميز عن التوقيع التقليدي بقدرته على تأمين الوثائق الرقمية ومنع التلاعب بها بعد التوقيع، كما يعتبر التوقيع الإلكتروني أقوى في بعض الجوانب من التوقيع التقليدي، إذ يمكن التحقق من هوية الموقع، ويصعب تزويره بسبب تشفير البيانات.

للتوقيع الالكتروني حجية قانونية في الإثبات، وذلك ما تناوله المشرع الجزائري في القانون رقم 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين حيث تعرض إلى نوعين من التوقيع الالكتروني: توقيع إلكتروني بسيط وتوقيع إلكتروني موصوف.

وقد جاء في المادة 327 وما يليها، وكذا أحكام القانون رقم 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين، والتي تؤكد أن القوة الثبوتية للمحررات تكون حجيتها بين الأطراف، وبالإضافة إلى الغير مع إمكانية الطعن فيها للإنقاص من قيمتها أو استبعادها كليا، كما أن المشرع الجزائري قد ساوى بين التوقيع الإلكتروني والتوقيع العادي في الفقرة 2 من المادة 327 من القانون المدني الجزائري، وكما يمكن الاعتداد بالتوقيع الإلكتروني وفقا لشروط المادة 237 مكرر 1 من القانون ذاته، والتي أهمها التأكد من هوية الشخص مصدر التوقيع، ولكن بالرجوع إلى القانون رقم 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين، فقد ميز بين التوقيع البسيط والتوقيع الإلكتروني الموصوف، وأقر حجية هذا الأخير حسب المادة 8 من ذات القانون، فيعتبر إذن التوقيع الإلكتروني الموصوف وحده مماثلا للتوقيع المكتوب سواء كان الشخص طبيعي أو معنوي[2].

[1] فادي محمد عماد الدين توكل، مرجع سابق، ص 154.

[2] بن مبارك ماية، مرجع سابق، ص 636.

بالنسبة للتوقيع الالكتروني البسيط اكتفى المشرع بذكر استعماله كوسيلة لتوثيق هوية الموقع، وله حجية في إثبات قبول الموقع مضمون الكتابة في الشكل الالكتروني، وهو ما نصت عليه صراحة المادة 6 من قانون رقم 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، أما التوقيع الموصوف فحسب ما جاءت به نص المادة 7 من قانون رقم 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين سالف الذكر بأن التوقيع الالكتروني الموصوف هو التوقيع الالكتروني الذي تتوفر فيه جملة من الشروط كالآتي[1]:

- أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة؛
- أن يرتبط بالموقّع دون سواه؛
- أن يمكن من تحديد هوية الموقّع؛
- أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الالكتروني؛
- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع.

كما يعتبر التوقيع الالكتروني الموصوف وحده مماثلا للتوقيع الخطي التقليدي سواء كان التوقيع منسوب لشخص طبيعي أو معنوي.

إن المشرع الجزائري بتقريره لأحكام التوقيع الالكتروني، واعتباره متكافئا ومساويا للتوقيع التقليدي كان يهدف من وراء ذلك إلى حماية المتعاملين في إطار المعاملات الإلكترونية، غير أنه تجدر الإشارة أنه رغم مبدأ التكافؤ القائم بين نوعي التوقيع إلا أن الأمر يختلف في ما يخص الحجية للتوقيعين، على اعتبار أن التوقيع الالكتروني ليست له حجية مطلقة وإنما حجيته مرتبطة بشروط وضوابط قانونية وتقنية معينة يجب توافرها.

[1] خديجة عبد اللاوي، مطبوعة بيداغوجية حول محاضرات في قانون المعاملات الإلكترونية، موجهة لطلبة السنة أولى ماستر تخصص قانون خاص، جامعة بلحاج بوشعيب، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2022/2021، ص 101.

الفرع الثالث: التصديق الإلكتروني كآلية لتوثيق التوقيع الالكتروني

تقوم جهة التصديق كطرف محايد بتوفير الأمان والثقة في صحة وسلامة التوقيع الالكتروني لدى المتعاملين بالوسائل الالكترونية من خلال ما تقدمه من خدمات متعلقة بالتوقيع الالكتروني.

فللتحقق من صحة التوقيع لا بد من وجود جهة موثوق بها لربط شخص أو كيان بعينه بالتوقيع، ويتم ذلك باستخدام طرف ثالث محايد يطلق عليه مقدم خدمات التصديق أو مورد خدمات التصديق أو جهة التوثيق[1].

أولا: ماهية التصديق الالكتروني في القانون المقارن

التصديق الإلكتروني، يقصد به عملية التأكد من صحّة الكتابة الإلكترونية والتوقيع الإلكتروني. إذ يقوم بهذه العملية طرف محايد ومستقل عن أطراف التعاقد الإلكتروني، وقد يكون فردًا عاديًا أو شركة أو جهة معينة، ويسمى مقدّم خدمات التصديق. ويتمثل دور الموثق أو المصدّق الإلكتروني في توثيق المعاملات الإلكترونية للأشخاص، وذلك بهدف منحهم الثقة في محرراتهم لإثبات تصرفاتهم القانونية.

جهة التصديق الإلكتروني، هي الجهة المرخص لها بإصدار شهادة تصديق إلكتروني، وتقدم خدمات تتعلق بالتوقيع الإلكتروني.

تعتبر عملية التصديق الالكتروني أو التوثيق الالكتروني خدمة قانونية يقوم بها طرف محايد ومستقل عن أطراف التعاقد الالكتروني، قد يكون شخصا طبيعيا أو شركة أو جهة معينة، ويسمى بذلك: "مقدم خدمات التصديق" أو "مؤدي خدمات التصديق" أو "جهة التصديق"، وتختلف التسميات من تشريع لآخر، ويتمثل دور الموثق أو المصدق الالكتروني في توثيق المعاملات الالكترونية للأشخاص، بهدف منحهم الثقة في محرراتهم لإثبات تصرفاتهم القانونية، وقد أطلق عليهم اسم "وكلاء الإثبات".

[1] إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الالكترونية، دراسة للجوانب القانونية للتعامل عبر أجهزة الاتصال الحديثة والتراسل الالكتروني، مجلس النشر العلمي، جامعة الكويت، 2003، ص 192.

التصديق الإلكتروني، يقصد به عملية التأكد من صحّة الكتابة الإلكترونية وكذا التوقيع الإلكتروني، إذ يقوم بهذه العملية طرف محايد ومستقل عن أطراف التعاقد الإلكتروني، وقد يكون فردًا عاديًا أو شركة أو جهة معينة، ويسمى مقدّم خدمات التصديق، ويتمثل دور الموثق أو المصدّق الإلكتروني في توثيق المعاملات الإلكترونية للأشخاص، بهدف منحهم الثقة في محرراتهم لإثبات تصرفاتهم القانونية[1].

أما جهة التصديق الإلكتروني، فهي الجهة المرخص لها بإصدار شهادة تصديق إلكتروني، وتقدم خدمات تتعلق بالتوقيع الإلكتروني.

التصديق الإلكتروني، المعروف أيضًا باسم التصديق الرقمي أو الشهادة الإلكترونية، هو عملية تهدف إلى ضمان قانونية وسلامة وأمان المعلومات المرسلة أو المخزنة إلكترونيًا. تعتمد على استخدام المفاتيح المشفرة (المفتاح العام والمفتاح الخاص) لتأمين البيانات والصفقات عبر الإنترنت. يستخدم التصديق الإلكتروني بشكل شائع لضمان هوية الأطراف المشاركة في معاملة إلكترونية وضمان عدم تغيير البيانات أثناء النقل.

عرف **التوجيه الأوربي** رقم 1999/93 للتوقيعات الالكترونية مزود خدمات التصديق بأنه الشخص الطبيعي أو الكيان القانوني الذي يصدر الشهادات أو يوفر الخدمات الأخرى المتعلقة بالتوقيعات الإلكترونية[2].

لقد أوجب الملحق رقم 1 للتوجيه الأوربي حول التواقيع الإلكترونية أن تتضمن شهادة المصادقة الالكترونية ما يلي[3]:

- اسم وبيانات الجهة المصدرة للوثيقة الالكترونية والبلد الذي تتمركز فيه بشكل واضح.

---

[1] موقع مديرية التجارة لولاية بسكرة، وزارة التجارة الجزائرية، على الرابط الالكتروني: https://www.dcwbiskra.dz/index.php?option=com_content&view=article&id=249&Itemid=83#:~:text=%D8%A3%D9%85%D9%91%D8%A7%20%D8%A7%D9%84%D8%AA%D8%B5%D8%AF%D9%8A%D9%82%20%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%8C%20%D9%8A%D9%82%D8%B5%D8%AF%20%D8%A8%D9%87,%D9%85%D8%B9%D9%8A%D9%86%D8%A9%D8%8C%20%D9%88%D9%8A%D8%B3%D9%85%D9%89%20%D9%85%D9%82%D8%AF%D9%91%D9%85%20%D8%AE%D8%AF%D9%85%D8%A7%D8%AA%20%D8%A7%D9%84%D8%AA%D8%B5%D8%AF%D9%8A%D9%82..

[2] فادي محمد عماد الدين توكل، مرجع سابق، ص 155.

[3] علي عبد العالي خشاب الأسدي، مرجع سابق، ص 113-115.

- اسم الموقع الحقيقي والمستعار ولقبه والإفصاح عن شخصيته.
- عنوان الموقّع وبيان وضعه المالي للتأكد من وجود دعاوى أو أحكام قضائية تتعلق بإفلاسه أو إعساره.
- الإجراء المادي الذي تم اتخاذه لمراجعة التوقيع والذي يجب أن يكون متطابقا مع الإجراء الذي يخضع لسيطرة صاحب التوقيع في إصدار ومراجعة البيانات والتوقيع الذي يقوم بإصداره.
- الرمز التعريفي لشهادة المصادقة الالكترونية.
- مدة صلاحية شهادة المصادقة الالكترونية في الحالات التي يلزم فيها ذلك.
- توقيع الكاتب العدل الكتروني مصدر شهادة المصادقة لإثبات المصادقة.

أما قانون **الأونسيترال النموذجي بشأن التوقيعات الالكترونية لعام 2001 للتوقيع الالكتروني** فقد عرف مقدم خدمات التصديق بأنه شخص يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الالكترونية، ولذلك يقوم مقدمو خدمات التصديق بدور مهم وفعال في ضمان التوقيعات والاعتراف بها قانونا.

تتمثل وظيفة شهادة المصادقة من خلال ربط المفتاح العام بشخص معين، والذي يحمل هو المفتاح الخاص المناسب على نحو يمكن كل متعامل أن يستند على هذه الشهادة للتأكد من هوية الموقع ومفتاحه العام، وعندما يرغب مستقبِل الرسالة الالكترونية التثبت من صحة التوقيع الالكتروني الملحق بها وهوية الموقع يلجأ إلى المفتاح العام الوارد في شهادة المصادقة العائدة للموقّع، ويكون رجوعه إلى شهادة المصادقة، إما مباشرة باعتبار أن هذه الشهادة تكون قد ألحقت بالرسالة، وإما من خلال الدخول إلى بنوك معلومات سلطة المصادقة المختصة من خلال شبكة الإنترنت باستعمال محطة طرفيه وهو الأكثر شيوعا، ويقارن المفتاح المذكور في الشهادة مع المفتاح الموجود لديه والمنسوب للمرسل، وتتمثل وظيفة المفتاح العام لحل الرسالة المعلوماتية وللتأكد من عدم تحريفها ومن هوية موقعها، وأن التوقيع قد أنشئ بواسطة المفتاح الخاص المقابل[1].

[1] علي عبد العالي خشاب الأسدي، مرجع سابق، ص 113.

ثانيا: ماهية التصديق الالكتروني في التشريع الجزائري

على المستوى الوطني، ينظم التصديق الإلكتروني بموجب القانون رقم 15-04 المؤرخ في 11 ربيع الثاني 1436 الموافق 1 فبراير 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين. بموجب أحكام هذا القانون، تعتمد هيكلة النظام الوطني للتصديق والتوقيع الإلكترونيين على ثلاث جهات مكملة وهي[1]:

1) **السلطة الوطنية للتصديق الإلكتروني(ANCE)**، التابعة لمصالح الوزير الاول، تلعب دورًا مركزيًا في ترقية استعمال التوقيع والتصديق الإلكترونيين وتطويرهما وضمان موثوقية استعمالهما.
2) **السلطة الحكومية للتصديق الإلكتروني(AGCE)**، الخاضعة لإشراف وزير البريد والمواصلات السلكية واللاسلكية، مسؤولة عن متابعة ومراقبة نشاط التصديق الإلكتروني للأطراف الثالثة الموثوقة وكذلك توفير خدمات التصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي.

تكلف السلطة الحكومية للتصديق الإلكتروني بمتابعة ومراقبة نشاط التصديق الإلكتروني للأطراف الثالثة الموثوقة، فضلاً عن تقديم خدمات التصديق الإلكترونية لصالح المتدخلين في الفرع الحكومي المحددين في المادة 2 من القانون 15-04، على النحو التالي: " المؤسسات والإدارات العمومية، والهيئات العمومية المحددة في التشريع المعمول به، والمؤسسات الوطنية المستقلة، وسلطات الضبط، المتدخلون في المبادلات بين البنوك، وكذا أي شخص أو كيان ينتمي إلى الفرع الحكومي"[2].

بموجب المادة 28 من القانون رقم 15-04 المذكور أعلاه، فإن السلطة الحكومية للتصديق الإلكتروني تتولى المهام الآتية:

---

[1] موقع وزارة البريد والمواصلات السلكية واللاسلكية، الجزائر، على الرابط الإلكتروني: https://www.mpt.gov.dz/%D8%A7%D9%84%D8%AA%D9%88%D9%82%D9%8A%D8%B9-%D9%88%D8%A7%D9%84%D8%AA%D8%B5%D8%AF%D9%8A%D9%82-%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D9%8A%D9%86/.

[2] موقع السلطة الحكومية للتصديق الالكتروني، الجزائر، على الرابط الالكتروني: https://agce.dz/ar/presentation-de-lagce/.

- إعداد سياستها للتصديق الإلكتروني وعرضها على السلطة الوطنية للتصديق الإلكتروني للموافقة عليها والسهر على تطبيقها؛
- الموافقة على سياسات التصديق الإلكتروني الصادرة عن الأطراف الثالثة الموثوقة والسهر على تطبيقاتها؛
- الاحتفاظ بشهادات التصديق الإلكترونية المنتهية صلاحيتها، والبيانات المرتبطة بمنحها من قبل الطرف الثالث الموثوق، بغرض تسليمها إلى السلطات القضائية المختصة، عند الاقتضاء، طبقا للأحكام التشريعية والتنظيمية المعمول بها؛
- نشر شهادة التصديق الإلكتروني للمفتاح العام للسلطة الوطنية للتصديق الإلكتروني؛
- إرسال كل المعلومات المتعلقة بنشاط التصديق الإلكتروني إلى السلطة الوطنية للتصديق الإلكتروني دوريا أو بناءً على طلب منها؛
- القيام بعملية التدقيق على مستوى الطراف الثالث الموثوق، عن طريق الهيئة الحكومية المكلفة بالتدقيق، طبقا لسياسة التصديق؛

يتم تتبع تنظيم السلطة الحكومية للتصديق الإلكتروني (AGCE) من خلال أحكام المرسوم التنفيذي رقم 16-135 المؤرخ 25 أبريل 2016 الذي يهدف إلى تحديد طبيعة السلطة الحكومية للتصديق الإلكتروني، تشكيلها وتنظيمها وسيرها. تتولى إدارة السلطة الحكومية للتصديق الإلكتروني مدير(ة) عام(ة) وتزود بمجلس للتوجيه بهياكل إدارية وتقنية.

تتولى إدارة السلطة الحكومية للتصديق الإلكتروني مدير(ة) عام(ة) وتزود بمجلس للتوجيه بهياكل إدارية وتقنية. يتشكل مجلس التوجيه من المدير(ة) العام(ة) للسلطة الحكومية، رئيسا، وممثل عن رئاسة الجمهورية وممثلين عن الوزراء المكلفين بما يأتي:

- الدفاع الوطني،
- الداخلية،
- العدل،
- المالية،

- تكنولوجيات الإعلام والاتصال،

تساعد المدير(ة) العام(ة) في مهامه، خلية تدقيق وأمانة تقنية.

3) **السلطة الاقتصادية للتصديق الإلكتروني(AECE)** ، التابعة لسلطة ضبط البريد والاتصالات الالكترونية(ARPCE) ، مسؤولة عن متابعة ومراقبة مؤديي خدمات التصديق الإلكتروني الذين يقدمون خدمات التوقيع والتصديق الإلكتروني لصالح الجمهور.

تتمثل الغاية الرئيسية من هذه الهيكلة للنظام الوطني للتصديق والتوقيع الإلكترونيين في الحصول على الاعتراف الدولي، مما يضمن التوافق مع سلطات الاعتماد الأخرى في جميع أنحاء العالم[1].

تمّ تعيين سلطة ضبط البريد والاتصالات الالكترونية بصفتها السلطة الاقتصادية للتصديق الالكتروني. فهي مُكلّفة بمتابعة ومراقبة مؤدي خدمات التصديق الالكتروني الذي يقدّمون خدمات التوقيع والتصديق الالكترونيين لصالح الجمهور، كما أنّها تتولى المهام الآتية لفائدة مؤدي خدمات التصديق الالكتروني[2]:

1) إعداد سياستها للتصديق الالكتروني وعرضها على السلطة للموافقة عليها والسهر على تطبيقها؛
2) منح التراخيص لمؤدي خدمات التصديق الالكتروني بعد موافقة السلطة؛
3) الموافقة على سياسات التصديق الصادرة عن مؤدي خدمات التصديق الالكتروني والسهر على تطبيقها؛

---

[1] تم إنشاء السلطة الحكومية للتصديق الإلكتروني بموجب القانون رقم 15-04 المؤرخ 11 ربيع الثاني 1436 الموافق 01 فبراير 2015، والذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين. حيث وضع المشرع الإستراتيجية الوطنية للتصديق الإلكتروني وأسس هيكلها التنظيمي المكون من ثلاث (03) سلطات للتصديق الإلكتروني على النحو التالي:

- السلطة الوطنية للتصديق الإلكتروني (ANCE) التي تم إنشاؤها لدى الوزير الأول.
- السلطة الحكومية للتصديق الإلكتروني (AGCE) التي تم إنشاؤها لدى الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال.
- السلطة الاقتصادية للتصديق الإلكتروني (AECE) التي كلِفت بها السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية (ARPCE).

السلطة الحكومية للتصديق الإلكتروني (AGCE) هي سلطة إدارية تتمتع بالشخصية المعنوية والاستقلال المالي.

[2] موقع سلطة ضبط البريد والاتصالات الالكترونية (ARPCE)، التصديق الإلكتروني، على الرابط الالكتروني: https://www.arpce.dz/ar/topic/ce.

4) الاحتفاظ بشهادات التصديق الالكترونية المنتهية صلاحيتها، والبيانات المرتبطة بمنحها من طرف مؤدي خدمات التصديق الالكتروني بغرض تسليمها إلى السلطات القضائية المختصة، عند الاقتضاء، طبقا للأحكام التشريعية والتنظيمية المعمول بها؛

5) نشر شهادة التصديق الالكتروني للمفتاح العمومي للسلطة؛

6) اتخاذ التدابير اللازمة لضمان استمرارية الخدمات في حالة عجز مؤدي خدمات التصديق الالكتروني عن تقديم خدماته؛

7) ارسال كل المعلومات المتعلقة بنشاط التصديق الالكتروني إلى السلطة دوريا أو بناء على طلب منها؛

8) التحقق من مطابقة طالبي التراخيص مع سياسة التصديق الالكتروني بنفسها أو عن طريق مكاتب تدقيق معتمدة؛

9) السهر على وجود منافسة فعلية ونزيهة باتخاذ كل التدابير اللازمة لترقية أو استعادة المنافسة بين مؤدي خدمات التصديق الالكتروني؛

10) التحكيم في النزاعات القائمة بين مؤدي خدمات التصديق الالكتروني فيما بينهم أو مع المستعملين طبقا للتشريع المعمول به؛

11) مطالبة مؤدي خدمات التصديق الالكتروني أو كل شخص معني بأي وثيقة أو معلومة تساعدها في تأدية المهام المخولة لها بموجب هذا القانون؛

12) إعداد دفتر الشروط الذي يحدد شروط وكيفيات تأدية خدمات التصديق الالكتروني وعرضة على السلطة للموافقة عليه؛

13) إجراء كل مراقبة طبقا لسياسة التصديق الالكتروني ودفتر الشروط الذي يحدد شروط وكيفيات تأدية خدمات التصديق الالكتروني؛

14) تقوم السلطة الاقتصادية للتصديق الالكتروني بتبليغ النيابة العامة بكل فعل ذو طابع جزائي يكتشف بمناسبة تأدية مهامها.

المحور الثالث:

مسؤولية مزودي خدمة التصديق الالكتروني

تعد مسؤولية مزودي خدمة التصديق الإلكتروني جزءًا حيويًا من النظام القانوني والأمني الذي ينظم العمليات الإلكترونية، فمع تزايد الاعتماد على التقنيات الرقمية في المعاملات التجارية والحكومية، أصبحت الثقة في الهوية الرقمية وتوثيق المعلومات أمراً بالغ الأهمية، يلعب مزودو خدمة التصديق الإلكتروني دوراً رئيسياً في هذا السياق، حيث يقومون بتوفير شهادات رقمية تساعد في التحقق من هوية الأفراد والمؤسسات، مما يعزز الأمان ويمنع التزوير أو الاحتيال الإلكتروني.

من هذا المنطلق، تنبع مسؤولية مزودي خدمة التصديق الإلكتروني من طبيعة الخدمة التي يقدمونها والالتزامات القانونية المرتبطة بها، يجب على هؤلاء المزودين الالتزام بأعلى معايير الأمان والمصداقية، وضمان حماية البيانات والمعلومات الحساسة التي يتعاملون معها، إلا أن عدم الامتثال لهذه المعايير يمكن أن يؤدي إلى عواقب قانونية خطيرة، مثل تحمل المسؤولية عن الأضرار الناجمة عن الهجمات السيبرانية أو التصديق غير الصحيح للهوية.

وعليه سوف نتعرض في البداية إلى مضمون وطبيعة التزامات مزود خدمات التصديق الالكتروني (المبحث الأول)، ثم نوضح مسؤولية مقدم خدمة التصديق الالكتروني سواء وفق القواعد العامة والخاصة (المبحث الثاني).

المبحث الأول: مضمون وطبيعة التزامات مزود خدمات التصديق الالكتروني

في ظل التطور السريع للتكنولوجيا الرقمية والاعتماد المتزايد على الخدمات الإلكترونية في مجالات مختلفة كالتجارة، الاتصالات، والمعاملات المالية، برزت الحاجة إلى تعزيز الثقة في الهوية الرقمية وضمان أمان وسلامة المعلومات المتداولة عبر الإنترنت، من هنا ظهر دور مزودي خدمات التصديق الإلكتروني، الذين يضطلعون بمهمة تأكيد هوية الأطراف المشاركة في المعاملات الإلكترونية، والتحقق من صحة الوثائق الرقمية، والتوقيعات الإلكترونية، مما يسهم في ضمان حماية البيانات ومنع التلاعب أو الاحتيال (المطلب الأول).

طبيعة التزامات مزود خدمات التصديق الإلكتروني تشمل تقديم خدمات موثوقة تتوافق مع القوانين واللوائح الوطنية والدولية المعمول بها، حيث يُطلب منهم اعتماد تقنيات أمان متقدمة لتأمين المعلومات، هذا يتضمن حفظ سرية المعلومات الشخصية، حماية البنية التحتية للتوقيع الإلكتروني، وضمان نزاهة العمليات التي يقومون بها، علاوة على ذلك، يتحمل مزود الخدمات مسؤولية تقديم الدعم التقني والقانوني لضمان استمرارية الخدمات والحفاظ على مصداقيتها، مما يعزز من ثقة المستخدمين في التعاملات الرقمية (المطلب الثاني).

المطلب الأول: مضمون التزامات مزود خدمات التصديق الالكتروني

تشمل التزامات مزود خدمات التصديق الإلكتروني العديد من الجوانب التقنية والقانونية التي تهدف إلى ضمان موثوقية وأمان المعاملات الرقمية، تشمل التزامات مزود خدمات التصديق الإلكتروني الجوانب الفنية وغير الفنية، من الناحية الفنية، يتعين على مزود خدمة التصديق الالكتروني اعتماد تقنيات متقدمة لحماية البيانات وضمان سرية وخصوصية المعلومات المتبادلة، مثل استخدام التشفير وحماية البنية التحتية الرقمية، في حين أنه من الناحية غير الفنية، فتتضمن الالتزامات القانونية والتنظيمية، التي تفرض عليهم الامتثال للمعايير الدولية والمحلية، بالإضافة إلى توفير دعم تقني متواصل وضمان شفافية العمليات. يساهم الالتزام بهذه الجوانب في بناء بيئة رقمية آمنة تحظى بثقة المستخدمين والمؤسسات على حد سواء. لذلك سنتعرض في البداية إلى تعريف مزود خدمة التصديق الالكتروني في التشريع الجزائري والقانون المقارن.

الفرع الأول: تعريف مزود خدمة التصديق الإلكتروني في التشريع الجزائري والقانون المقارن

أولا: في التشريع الجزائري

في التشريع الجزائري، تم تنظيم خدمات التصديق الإلكتروني بموجب قانون يتعلق بالتوقيع الإلكتروني والمصادقة الإلكترونية، المعروف بالقانون رقم 04/15 الصادر في 1 فبراير 2015، يعرف هذا القانون مزود خدمة التصديق الإلكتروني على أنه الجهة التي تقدم خدمات المصادقة الإلكترونية للتوقيعات الإلكترونية، بما في ذلك إصدار الشهادات الإلكترونية والتحقق من الهوية الرقمية للمستخدمين.

وفقًا للمادة **4**من القانون، مزود خدمة التصديق الإلكتروني هو كيان يقوم بتقديم "الشهادات الإلكترونية" للأشخاص الطبيعيين أو المعنويين لتوثيق هويتهم، وبالتالي يضمن موثوقية التوقيع الإلكتروني، يتعين على مزودي خدمة التصديق الالتزام بعدة متطلبات تقنية وإدارية لضمان أمن وموثوقية التوقيعات الإلكترونية.

ثانيا: في القانون الفرنسي

في فرنسا، يتم تنظيم خدمات التصديق الإلكتروني بموجب **قانون الثقة في الاقتصاد الرقمي (LCEN)** الصادر في 2004. يعرف هذا القانون مزود خدمة التصديق الإلكتروني على أنه "الجهة التي تصدر شهادات إلكترونية، والتي تُستخدم للتحقق من هوية الموقع والتوقيع الرقمي المرتبط بالمستند الإلكتروني"[1].

تنص المادة **4-1316** من القانون المدني الفرنسي على أن التوقيع الإلكتروني يتمتع بنفس القوة القانونية للتوقيع اليدوي إذا تم استيفاء الشروط المتعلقة بمصادقة الأطراف بواسطة مقدم خدمة معتمد. بالتالي، يلعب مزود التصديق الإلكتروني دورًا رئيسيًا في هذا النظام من خلال ضمان صحة الهوية الرقمية للأطراف[2].

[1] قانون الثقة في الاقتصاد الرقمي(LCEN) ، فرنسا، 2004.

[2] القانون المدني الفرنسي، المادة 1316-4.

ثالثا: في التوجيه الأوربي

عرف التوجيه الأوربي رقم 1999/93 للتوقيعات الالكترونية مزود خدمات التصديق بأنه الشخص الطبيعي أو الكيان القانوني الذي يصدر الشهادات أو يوفر الخدمات الأخرى المتعلقة بالتوقيعات الالكترونية، وتضمنت الفقرة 1 من المادة 6 من التوجيه الأوربي رقم 1999/93 للتوقيعات الإلكترونية تنظيم مسؤولية جهات التصديق في حالة عدم صحة البيانات التي تضمنتها شهادة المصادقة الالكترونية[1].

رابعا: في قانون الأونسيترال النموذجي

عرف قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001 للتوقيع الإلكتروني مقدم خدمات التصديق بأنه الشخص الذي يصدر الشهادات ويجوز أن يقدم شهادات أخرى ذات صلة بالتوقيعات الالكترونية ولذلك يقوم مقدمو خدمات التصديق بدور مهم وفعال في ضمان التوقيعات والاعتراف بها قانونا.

مقدم خدمات التصديق الإلكتروني هو المسؤول عن إصدار الشهادات الإلكترونية التي تربط هوية الموقع بمفتاح عام للتوقيع، الشهادة الإلكترونية هي وثيقة إلكترونية تؤكد هوية الموقع وتتيح له استخدام المفتاح الخاص المرتبط بتلك الشهادة للتوقيع على المستندات (المادة 2(b) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001 للتوقيع الإلكتروني.

خامسا: في التشريع الأوروبي(eIDAS Regulation)

على الصعيد الأوروبي، يتم تنظيم خدمات التصديق الإلكتروني من خلال **التنظيم الأوروبي رقم 2014/910** المعروف باسم"eIDAS" ، وهو الإطار القانوني الذي ينظم خدمات تحديد الهوية الإلكترونية والمصادقة الإلكترونية في الاتحاد الأوروبي[2].

وفقًا لهذا التنظيم، يتم تعريف مزود خدمة التصديق الإلكتروني على أنه "مزود خدمة يضمن إصدار شهادات مؤهلة للتوقيع الإلكتروني أو الختم الإلكتروني". ويشترط أن يتمتع مزودو الخدمة

[1] فادي محمد عماد الدين توكل، مرجع سابق، ص 155.

[2] التنظيم الأوروبي رقم 2014/910(eIDAS) ، الاتحاد الأوروبي.

بترخيص أو اعتماد من قبل الجهات التنظيمية في الدول الأعضاء لضمان الامتثال للمعايير الأوروبية الموحدة.

سادسا: في التشريع الأمريكي(E-SIGN Act)

في الولايات المتحدة، يتم تنظيم خدمات التصديق الإلكتروني والتوقيع الرقمي بموجب **قانون التوقيعات الإلكترونية في التجارة العالمية والوطنية (E-SIGN Act)** الصادر في عام 2000. رغم أن القانون لا يعطي تعريفًا محددًا لمزود خدمة التصديق الإلكتروني، إلا أنه ينظم استخدام التوقيعات الإلكترونية في المعاملات التجارية ويضع معايير لمصداقية الأطراف المتعاملة[1].

في إطار هذا القانون، يتم التطرق إلى فكرة التحقق من الهوية عبر جهات موثوقة (Trustworthy entities) التي تقوم بإصدار شهادات رقمية لتوثيق التوقيعات الإلكترونية.

سابعا: في القانون الألماني(Signaturgesetz – SigG)

في ألمانيا، يتم تنظيم خدمات التوقيع الإلكتروني بموجب **قانون التوقيع الإلكتروني (Signaturgesetz – SigG)**.يعرف هذا القانون مزود خدمة التصديق الإلكتروني على أنه "الجهة التي تصدر شهادات التأهيل للتحقق من الهوية الإلكترونية للأفراد". يشترط أن يتمتع مزود الخدمة بترخيص من الجهة المختصة لضمان الامتثال للمعايير القانونية والأمنية.

يضمن هذا القانون أن مزود خدمة التصديق الإلكتروني ملتزم بالمعايير التقنية والتنظيمية اللازمة لحماية البيانات والمصادقة على الهوية.

يختلف تعريف مزود خدمة التصديق الإلكتروني بين الدول بناءً على الأطر القانونية المختلفة التي تنظم التوقيع الإلكتروني والمصادقة الإلكترونية، ومع ذلك، يجمع بين هذه التشريعات ضرورة التزام مزودي الخدمة بمجموعة من المعايير القانونية والأمنية لضمان موثوقية وأمان التعاملات الإلكترونية.

[1] U.S. Code, Electronic Signatures in Global and National Commerce Act (E-SIGN), 2000.

الفرع الثاني: الالتزامات غير الفنية لمزود خدمة التصديق الالكتروني

تعتبر خدمات التصديق الإلكتروني من الأساسيات في مجال التجارة الإلكترونية والتعاملات الرقمية، حيث يتم استخدامها للتحقق من هوية المستخدمين وتأمين الوثائق الرقمية، لذلك يتعين على مزودي خدمة التصديق الإلكتروني(Certification Authorities – CAs) الالتزام بمجموعة من المسؤوليات غير الفنية لضمان الجودة والثقة في الخدمات التي يقدمونها، تتمثل هذه الالتزامات في: الالتزام بالتحقق من صحة البيانات التي تضمنتها شهادة التصديق الالكتروني، الالتزام بإصدار شهادة التصديق الالكترونية، الالتزام بإلغاء أو وقف شهادة التصديق الالكتروني إذا استدعى الأمر ذلك، والالتزام بالسرية.

أولا: الالتزام بالتحقق من صحة البيانات

يضمن مزود خدمات التوثيق الإلكتروني صحة الشهادة الإلكترونية ودقة البيانات الواردة فيها، حيث يلتزم مزود خدمات التوثيق بالتأكد وبالتالي التحقق من نسبة التوقيع الإلكتروني لصاحبه من صحة البيانات والمعلومات المقدمة من العميل صاحب الشهادة، ويتم ذلك عن طريق فحص الوثائق وقد نظمت هذا الالتزام كل من المادة 4 من التوجيه الأوروبي والأوراق التي يقدمها العميل بشأن التواقيع الإلكترونية والمادة 4 من تعليمات التواقيع الإلكترونية البريطانية The electronic Signatures Regulations 2002والمرسوم الفرنسي رقم 2001/272 كما نظمت هذا الالتزام المادة 21 من القانون الاتحادي الإماراتي رقم (1) لسنة 2006 بشأن المعاملات والتجارة الإلكترونية والمادة 1/24/ب من قانون المعاملات الإلكترونية لإمارة دبي، والمادة 12/هـ من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري، والفصل 18 من قانون المبادلات والتجارة الإلكترونية التونسي. فالأصل أن مهمة مزود خدمات التوثيق تتمثل بإصدار الشهادة الإلكترونية. هذه الشهادة يجب أن تتضمن بيانات جوهرية محددة مثل هوية صاحب الشهادة ومدة صلاحية الشهادة والمعاملات التي يمكن استخدام الشهادة بشأنها، كما يجب أن يضمن مزود التوثيق الإلكتروني دقة وصحة هذه البيانات، وإلا عدّ مسؤولا عن أي ضرر يلحق بالغير الذي عول على الشهادة الإلكترونية وعلى البيانات الموجودة

فيها وأبرم عددا من العقود مع صاحب الشهادة بناء عليها، من أجل ذلك يلتزم المزود بفحص البيانات والتأكد من صحتها[1].

مزود خدمات التصديق يلتزم بضمان صحة البيانات الواردة في الشهادة الإلكترونية، ويجب عليه التحقق بشكل دوري من عدم حدوث أي تغييرات قد تؤثر على هذه البيانات، وذلك ما نصت عليه وأكدته المادة 6 (1) من القانون النموذجي بحيث تناولت مسؤولية مزود خدمات التصديق الالكتروني في التأكد من أن البيانات المرتبطة بالتوقيع الإلكتروني صحيحة ويمكن التحقق منها.

المادة 7 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001 للتوقيع الإلكتروني، والتي أشارت إلى أهمية ضمان صحة المعلومات وتحديث الشهادات إذا لزم الأمر.

ثانيا: الالتزام بإصدار شهادة التصديق الالكترونية

ان هذا الالتزام يتمثل في الالتزام بتحقيق نتيجة، والتي هي صدور شهادة تصديق الكترونية مستوفية لكامل البيانات الأساسية، أما في حال إذا ما كانت شهادة التصديق الإلكترونية تخل بأحد الشروط التي يجب توافرها بالشهادة فعلى مقدم الخدمات إلغاء هذه الشهادة، أو تعليق العمل بها في حال توفر سبب يوجب ذلك ويكون بناء على طلب صاحب الشهادة أو من تلقاء نفسها.

يتمثل هذا الالتزام في حالة أن تكون الشهادة سلمت بناء على معلومات مغلوطة أو مزيفة، والمقصود منها أن المعلومات تكون صحيحة، وتخص ذات شخص آخر نتيجة لذلك يتعرض صاحب الشهادة المزيفة إلى المساءلة المدنية والجزائية، أيضا أن تستعمل الشهادة لغرض التدليس وذلك بأن تصدر الشهادة صحيحة وتستعمل من قبل صاحبها لكن استعمالها غير مشروع.

ثالثا: الالتزام بإلغاء أو وقف شهادة التصديق الالكتروني إذا استدعى الأمر ذلك

الالتزام بإلغاء أو وقف شهادة التصديق الإلكتروني يأتي ضمن إطار الحماية وضمان سلامة المعاملات الإلكترونية. هناك عدة حالات قد تستدعي إلغاء أو وقف الشهادة الإلكترونية، ومنها:

[1] علاء الدين الخصاونة، أيمن مساعدة، المسؤولية المدنية لمزود خدمات التوثيق الالكتروني – دراسة تحليلية في ظل نصوص التوجيه الأوربي بشأن التواقيع الالكترونية والتشريعات المقارنة، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد8، العدد1، فبراير 2011، ص 113.

1) حالات تعليق الشهادة الالكترونية

أ/- وجود قرائن: بحيث تكون تلك القرائن قائمة بناء على معلومات موثقة تدل على انتهاك منظومة إنشاء التوقيع الالكتروني، أو استعمال الشهادة بغرض التدليس.

ب/- طلب صاحب الشهادة: ويقصد به الشخص الطبيعي الذي طلب إصدار تلك الشهادة الالكترونية سواء لنفسه بصفته شخص طبيعي، أو لغيره بصفته ممثلا قانونيا للشخص الاعتباري[1]، غير أنه يشترط في هذه الحالة أن يبرر صاحب الطلب رغبته في التعليق وأن يكون تبريره معقولا ومنطقيا ومقنعا لمزود خدمة التصديق الالكتروني، خاصة وأن شهادة التصديق الالكتروني ترتب آثارا على غير صاحب الطلب، كما هو الأمر بالنسبة لعقد البيع فإذا قام البائع بطلب وقف الشهادة المتعلقة بعقد البيع فإن ذلك سوف يؤثر على المتعاقد الثاني وهو المشتري.

2) حالات وقف الشهادة الالكترونية

أ/- انتهاء صلاحية الشهادة: عند انتهاء فترة صلاحية شهادة التصديق الإلكتروني، يجب إلغاؤها أو تجديدها لضمان عدم استخدامها بطريقة غير مشروعة.

ب/- اختراق المفتاح الخاص: إذا تعرض المفتاح الخاص المرتبط بالشهادة الإلكترونية للاختراق أو تم الوصول إليه من قبل أشخاص غير مصرح لهم، يجب إلغاء الشهادة على الفور.

ج/- فقدان الثقة في الجهة المُصدِرة: إذا تبين أن الجهة التي أصدرت الشهادة الإلكترونية غير جديرة بالثقة أو أنها خالفت اللوائح والمعايير المعتمدة فيجب إلغاء الشهادة لضمان أمن المعلومات.

د/- طلب صاحب الشهادة: يحق لصاحب الشهادة طلب إلغاءها أو وقفها إذا رأى ضرورة لذلك، كفقدان السيطرة على مفتاح التوقيع أو لأي سبب آخر يتعلق بأمانه الشخصي أو المؤسسي.

هـ/- تغييرات في المعلومات: إذا تغيرت أي معلومات أساسية متعلقة بالشهادة (مثل اسم حامل الشهادة أو بيانات الهوية)، يجب تحديث الشهادة أو إلغاؤها.

---

[1] عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون العربي النموذجي، الكتاب الثاني، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص 175.

و/- وفاة الشخص الطبيعي أو حل الشخص الاعتباري صاحب الشهادة: فوفاة الشخص يعتبر بحكم عدم الوجود وبالتالي لا تكون هناك ضرورة أو أهمية للتوقيع الالكتروني ولا لشهادة التصديق الخاصة الالكتروني[1].

بإلغاء أو وقف الشهادة، يتم ضمان أن التعاملات التي تعتمد على هذه الشهادة لن تتم أو تُعتمد، مما يحمي الأطراف المعنية من أي استخدام غير مشروع للبيانات المعتمدة على تلك الشهادة.

رابعا: الالتزام بالسرية

يلتزم مزود خدمات التصديق الالكتروني بالحفاظ على سرية البيانات ذات الطابع الشخصي تجاه العميل صاحب الشهادة، فلا يجوز للمزود إفشاء البيانات الشخصية الواردة في الشهادة[2]، فأي إخلال من مزود خدمات التصديق الالكتروني بالتزامه بالحفاظ على سرية البيانات الشخصية للعميل يؤدي إلى ثبوت مسؤوليته العقدية، بسبب استعمال البيانات الشخصية للعميل دون علمه ودون موافقته أو استعمالها في غير الغرض المعد لهذا الاستعمال.

كما يلتزم المزود بعدم حذف أو إضافة وتعديل البيانات ذات الطابع الشخصي[3]، إضافة إلى أنه يلتزم في حالة فسخ عقد تقديم خدمة التصديق الالكتروني لأي سبب من الأسباب أن يقوم بتسليم العميل كل النسخ المرتبطة بالمعلومات التي تلقاها من العميل إلى الهيئة الوطنية المختصة، ولا يجوز له الاحتفاظ بأي نسخة منها له أو لمعاونيه[4].

وفي سبيل دعم الثقة بين المتعاملين بالوسائل الإلكترونية، نص المشرع الجزائري على هذا الالتزام في نص المادة 07 من القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين، خاصة وأن

---

[1] هيثم الطاس، محمد فائز خضور، المسؤولية المدنية لمزود خدمات التصديق الالكتروني، مجلة جامعة البعث، المجلد 43، العدد 13، سوريا، 2021، ص 81.

[2] عبد الفتاح بيومي حجازي، مرجع سابق، ص 230.

[3] هيثم الطاس، محمد فائز خضور، مرجع سابق، ص 76.

[4] مدحت عبد العال، المسؤولية المدنية الناشئة ن تقديم خدمة التوقيع الإلكتروني، المركز القومي للإصدارات القانونية، مصر، الطبعة الأولى، 2010، ص 84.

معظم المعاملات الإلكترونية تتم بين اشخاص لا يلتقون ولا يعرفون بعضهم، فلولا هذه الضمانات لما أقبل الأشخاص على إبرام العقود وإتمام الصفقات عبر شبكة الإنترنت.

كما نصت على هذا الالتزام المادة 42 من القانون رقم 04/15، ويعتبر من أخطر الالتزامات التي تقع على عاتق مزودي خدمات التصديق الإلكتروني، حيث لا يحصل على المعلومات الشخصية إلا الشخص نفسه أو برضاه الصريح، ولا يجوز ملن قدمت إليه أو اتصل بها بحكم عمله إفشائها للغير، أو استخدامها في غير الغرض الذي أعدت من أجله، لكن إذا ما رخص صاحب الشهادة كتابيا أو إلكترونيا في نشرها أو الإعلام عنها، أوفي حال صدور حكم قضائي يجيز نشر تلك البيانات أو الإعلام عنها، فهنا تنتفي مسؤولية مزودي خدمات التصديق، لذلك ألزم التشريع الجزائري مزودي خدمات التصديق وأعوانهم الحرص الشديد في الحفاظ على سرية المعلومات التي عهد بها إليهم[1].

الفرع الثالث: الالتزامات الفنية لمزود خدمة التصديق الالكتروني

الالتزامات الفنية لمزود خدمة التصديق الإلكتروني تختلف حسب القوانين والتشريعات المحلية والدولية التي تنظم هذا المجال، لكن بشكل عام يمكن تلخيص الالتزامات الفنية الرئيسية على النحو التالي:

أولا: ضمان الأمان والسرية:

- استخدام تقنيات تشفير قوية لضمان سرية المعلومات المتبادلة.
- حماية المفاتيح الخاصة المستخدمة في إصدار الشهادات الرقمية.
- توفير بيئة آمنة لإصدار وإدارة الشهادات.

يعتمد مزودو خدمة التصديق الإلكتروني على بروتوكولات أمان متقدمة مثل التشفير المتماثل وغير المتماثل باستخدام مفاتيح عامة وخاصة. التشفير مهم لضمان سرية المعلومات المتبادلة ومنع أي اختراقات[2].

[1] ليندة بلحارث، النظام القانوني لمزودي خدمات التصديق الالكتروني في القانون الجزائري، مجلة العلوم القانونية والسياسية، المجلد 9، العدد 3، جامعة الشهيد حمّه لخضر بالوادي، ديسمبر 2018، ص 869.

[2] Johannes A. Buchmann, Public Key Infrastructure (PKI): Principles and Applications. Springer, 2013, P 23.

ثانيا: التوثيق والمصادقة

- التأكد من هوية الأطراف التي يتم إصدار الشهادات لها وفقًا للمعايير المعتمدة.
- الالتزام بعملية موثوقة لتوثيق هوية المستفيدين قبل إصدار الشهادة الإلكترونية.

ثالثا: إدارة الشهادات

- إصدار، تجديد، تعليق، أو إلغاء الشهادات الإلكترونية بناءً على طلبات المستفيدين أو عند الحاجة.
- الاحتفاظ بسجل دقيق لإصدار وإلغاء الشهادات.

تشمل إدارة الشهادات إصدارها وتجديدها وتعليقها أو إلغائها. يعتبر **بروتوكول OCSP** (Online Certificate Status Protocol) واحدًا من البروتوكولات التي يتم الاعتماد عليها للتحقق من حالة الشهادة[1].

رابعا: التوافق مع المعايير الدولية

- الالتزام بالمعايير والبروتوكولات المعترف بها دوليًا مثل معيار X.509 للشهادات الرقمية.

خامسا: التوافر والتعافي من الكوارث

- ضمان استمرارية الخدمة عبر وجود خطط للتعافي من الكوارث وتأمين النسخ الاحتياطية للبيانات.
- التأكد من توفر الخدمة بشكل دائم لتلبية احتياجات المستخدمين.

سادسا: الامتثال القانوني

- الالتزام بالقوانين المحلية والإقليمية المتعلقة بالتصديق الإلكتروني وحماية البيانات.

سابعا: الدعم الفني وتحديث الأنظمة

- تقديم الدعم الفني للمستخدمين لضمان استمرارية استخدام الشهادات.

[1] Eric Rescorla, Addison-Wesley, SSL and TLS: Designing and Building Secure Systems. Addison-Wesley, 2001, P 251.

- تحديث الأنظمة والتكنولوجيا المستخدمة لتلبية التغيرات في معايير الأمان أو التكنولوجيا الجديدة.

ثامنا: إدارة المخاطر

- تحليل وإدارة المخاطر المرتبطة بالخدمات الإلكترونية لضمان تقديم خدمات آمنة وموثوقة.

هذه الالتزامات تهدف إلى ضمان موثوقية الشهادات الإلكترونية وحمايتها من التزوير أو الاختراق، وتقديم خدمة موثوقة وآمنة للمستخدمين.

كما يقع على عاتق المزود الالتزام بتقديم سجل إلكتروني للشهادة بمتناول المستخدمين على شكل بنك، بيانات سهل الدخول وبشكل دائم من أجل الاطلاع عليه ومراجعته عند الحاجة، يبين هذا السجل الشهادات التي تم وقف العمل بها أو تم إلغاؤها وتلك التي لا زالت سارية المفعول، كما يجب أن تتضمن الشهادة الإلكترونية معلومات إجبارية خاصة بمستوى الشهادة والرمز أو الرقم الذي يشير للشهادة، هوية وعنوان المورد الذي يصدر الشهادة، وهوية الشخص الطبيعي أو الشخص المعنوي الحائز على الشهادة، واسم نطاقه وهوية من يدير جهاز الخادم واسم نطاقه، وكذلك تاريخ بداية وانتهاء صلاحية الشهادة باليوم والساعة والدقيقة والثانية حسب توقيت محدد، ووسيلة فحص التوقيع الإلكتروني لصاحب الشهادة، حيث يجب على مزود خدمة التوثيق أن يقدم أو يضمن دقة المعلومات المشهود بها والمتضمنة في الشهادة بتاريخ إصدارها أو تقديمها[1].

المطلب الثاني: طبيعة التزامات مزود خدمات التصديق الالكتروني

التزامات مزود خدمات التصديق الإلكتروني تتنوع بين التزام ببذل العناية والتزام بتحقيق نتيجة، حيث يرتبط كل منهما بمسؤوليات محددة تقع على عاتق المزود لضمان تقديم خدمة آمنة وموثوقة. من حيث الالتزام ببذل العناية، يجب على المزود اتخاذ كافة التدابير اللازمة والتحقق من الدقة والتفصيل في مراجعة البيانات والمعلومات المقدمة إليه من المستخدمين. هذا الالتزام يتطلب الحرص على استخدام الأدوات والتقنيات المتطورة للحفاظ على سلامة النظام وعدم تعرضه للاختراق أو التلاعب. أما الالتزام بتحقيق نتيجة، فيتجسد في مسؤولية مزود الخدمة عن توفير التصديق الإلكتروني بشكل يمكن المستخدمين من الحصول على نتائج نهائية دقيقة ومقبولة قانونيًا. يجب أن يكون المنتج أو

[1] علاء الدين الخصاونة، أيمن مساعد، مرجع سابق، ص 115.

الخدمة المقدمة قابلة للتطبيق الفعلي وتضمن مصداقية الهوية الرقمية للمستخدم بما يتفق مع القوانين والمعايير المعتمدة.

الفرع الأول: الالتزام ببذل عناية

يُعد الالتزام ببذل العناية من أهم الالتزامات القانونية التي تقع على عاتق مزودي خدمة التصديق الإلكتروني، إن مزود هذه الخدمة يُعتبر طرفًا مهمًا في التجارة الإلكترونية وفي التعاملات الرقمية، حيث يقوم بالتحقق من صحة الهويات الرقمية وتوثيق المعاملات لضمان الأمان والثقة بين الأطراف المتعاقدة، من هنا، تتعاظم أهمية الالتزام ببذل العناية لضمان دقة المعلومات والحفاظ على خصوصية البيانات ومنع التزوير والاحتيال الإلكتروني.

الالتزام ببذل العناية هو الالتزام الذي يفرض على مزود خدمة التصديق الإلكتروني أن يبذل جهوداً معقولة وملائمة وفقاً للمعايير المهنية والتقنية السائدة في مجاله، يتمثل هذا الالتزام في اتخاذ كافة الإجراءات اللازمة للتحقق من صحة المعلومات التي يتم التصديق عليها، وضمان سلامة عملية التصديق الالكتروني.

يتفق جانب كبير من الفقه على أن العديد من التزامات مزود خدمة التصديق الالكتروني تمثل التزام ببذل عناية، فالتزامه بضمان صحة البيانات يعتبر التزام ببذل عناية، كونه يكون ملزما ببذل عناية الرجل العادي وملزم باتخاذ الاحتياطات اللازمة للتأكد من صحة البيانات الواردة في الشهادة بحيث لا يكون مزود خدمة التصديق الإلكتروني بالتعويض إذا تحقق من صحة البيانات المقدمة له، كما لو كانت تلك البيانات مستمدة من وثائق أو مستندات مزورة أو محرفة[1].

ويترتب على هذا الرأي أن خطأ مزود التوثيق الإلكتروني ليس مفترضا، بل خطأ واجب محرفة الإثبات، وبذلك يكون على المتضرر أن يثبت أن المزود لم يبذل العناية المطلوبة والمعتادة، وأن يثبت إهماله في التأكد من دقة وصحة البيانات الواردة في الشهادة، وهو ما أكدته المادة التاسعة من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية باستخدامه لمصطلح (عناية معقولة) لوصف مدى

[1] هيثم الطاس، محمد فائز خضور، مرجع سابق، ص 70.

التزام المزود في هذا المجال، فقد حددت أن مزود خدمة التوثيق يلتزم ببذل العناية المعقولة لضمان التزام المزود صحة البيانات الأساسية الواردة في الشهادة الإلكترونية[1].

يُلزم مزود خدمة التصديق الإلكتروني بحماية البيانات الشخصية والمعلومات الحساسة التي يتم التعامل معها في إطار عملية التصديق، يتعين عليه اتخاذ التدابير التقنية والقانونية اللازمة لمنع الوصول غير المصرح به لهذه البيانات.

في حالة عدم التزام مزود خدمة التصديق الإلكتروني ببذل العناية المطلوبة، فإنه يكون عرضة لتحمل المسؤولية القانونية عن أي ضرر ينجم عن تقصيره، العقوبات قد تشمل الغرامات المالية أو سحب الترخيص الممنوح له من الجهات المنظمة.

الالتزام ببذل العناية من قبل مزود خدمة التصديق الإلكتروني هو عنصر جوهري للحفاظ على الثقة في المعاملات الرقمية، إن تطبيق هذا الالتزام بشكل صحيح يضمن سلامة التعاملات الإلكترونية ويحمي حقوق الأطراف المختلفة، وتعتبر هذه الخدمة دعامة أساسية للاقتصاد الرقمي، ومن الضروري تعزيز المعايير والإجراءات التي تحكمها لضمان الامتثال الأمثل.

الفرع الثاني: الالتزام بتحقيق نتيجة

في عالم التعاملات الإلكترونية، يعتبر مزود خدمة التصديق الإلكتروني طرفًا أساسيًا في ضمان مصداقية وصحة المعلومات المتداولة، ومن بين التزاماته القانونية الالتزام بتحقيق نتيجة، وهو التزام يتطلب من مزود الخدمة ليس فقط بذل الجهد أو العناية، ولكن تحقيق نتيجة محددة وملموسة يتوقعها المستخدمون، يهدف هذا الالتزام إلى تقديم ضمانة بأن الخدمة المقدمة ستؤدي إلى تحقيق الغرض المطلوب، وهو ضمان صحة وموثوقية الشهادات الإلكترونية والمعاملات الرقمية.

الالتزام بتحقيق نتيجة هو التزام على عاتق مزود خدمة التصديق الإلكتروني يتطلب منه ضمان وصول الأطراف المتعاقدة إلى نتيجة معينة، مثل إصدار شهادة تصديق إلكتروني صحيحة وآمنة، هذا

[1] نصت المادة التاسعة من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية على أن: "حيثماّ يوفر مقدم خدمات التصديق خدمات لتأييد توقيع إلكتروني يجوز استخدامه لإعطاء مفعول قانوني بصفته توقيعا، يتعيّن على مقدم خدمات التصديق المشار إليه: (أ)- أن يتصرف وفقا للتأكيدات التي يقدمها بخصوص سياساته وممارساته؛ (ب)- أن يولي قدرا معقولا من العناية لضمان دقة واكتمالّ كل ما يقدمه من تأكيدات جوهرية ذات صلة بالشهادة طيلة دورة سريانها، أو مدرجة في الشهادة طيلة مدة سريانها". ينظر سمير حامد جمال، مرجع سابق، ص 337.

الالتزام يُلزم مزود الخدمة بتحقيق الهدف المتفق عليه بشكل دقيق وفعال، وليس مجرد بذل جهد والتزام لتحقيقه.

يلتزم مزود خدمة التصديق الإلكتروني بعدم إفشاء سرية البيانات الواردة بالشهادة الالكترونية ويلتزم بتحقيق هذه النتيجة، أي الحفاظ على سرية البيانات، بحيث أن مجرد إفشائها للغير يقيم مسؤولية المزود دون البحث فيما إذا كان قد بذل العناية المعقولة في الحفاظ عليها أم لا، وتجدر الإشارة إلى أن مسؤولية مزود خدمات التوثيق الإلكتروني عن إفشاء هذه البيانات الشخصية لا تقوم إذا تم ذلك في ضوء ترخيص كتابي من العميل صاحب الشهادة يسمح له بذلك أو إذا كان ذلك قد تم لاعتبارات الأمن الوطني أو استنادا إلى حكم قضائي يسمح بذلك[1].

كما أن الالتزام بإيقاف العمل بالشهادة، فلا شك أن هذا الالتزام يعد التزاما بتحقيق نتيجة حيث يعد مزود خدمة التصديق الالكتروني مخلا بالتزامه هذا بمجرد عدم قيامه بإلغاء الشهادة أو سحبها أو إيقاف العمل بها بالرغم من طلب العميل لذلك وبالرغم من توافر أسباب الإيقاف أو الإلغاء، فالمزود يلتزم بتحقيق نتيجة معينة هي سحب أو إلغاء الشهادة أو تعليق العمل بها إذا تحققت الأسباب التي تبرر إيقاف العمل بالشهادة أو توقيفها، وعلى ذلك إذا لم يقم المزود باتخاذ الإجراءات اللازمة لإيقاف العمل بالشهادة أو إلغائها يعد مسؤولا عن الأضرار التي قد يسببها للغير أو حتى للعميل صاحب الشهادة[2].

الالتزام بتحقيق نتيجة يمثل محورًا هامًا في دور مزود خدمة التصديق الإلكتروني لضمان الثقة والموثوقية في المعاملات الرقمية، بحيث أن ضمان تحقيق النتائج المرجوة من خدمات التصديق الإلكتروني يسهم في حماية الأطراف المتعاقدة من التزوير والاحتيال، ويعزز من دور التجارة الإلكترونية كوسيلة آمنة وفعالة في الاقتصاد الحديث، لذلك فإنه رغم أهمية الالتزام بتحقيق نتيجة، إلا أنه يواجه مزودو خدمات التصديق الإلكتروني العديد من التحديات إذ يحتاج مزودو خدمات التصديق الإلكتروني إلى التحديث المستمر لأنظمتهم وبرمجياتهم لتواكب التقدم التكنولوجي وتلبي المتطلبات القانونية.

---

[1] لينا حسان، التوثيق الإلكتروني ومسؤولية الجهات المختصة بها (دراسة مقارنة)، دار الراية للنشر والتوزيع، عمان، الأردن،2009، ص 108.

[2] علاء الدين الخصاونة، أيمن مساعده، مرجع سابق، ص 118-119.

المبحث الثاني: صور المسؤولية المدنية لمزود خدمات التصديق الالكتروني

تعد المسؤولية المدنية لمزود خدمات التصديق الإلكتروني من القضايا المستجدة في ظل التطور الرقمي، وتتحدد وفق القواعد العامة بحيث يلزم مزود خدمات التصديق الإلكتروني بتقديم الخدمة دون إهمال أو تقصير، ويُسأل عن أي ضرر يلحق بالأطراف نتيجة إخلاله بالتزاماته التعاقدية أو القانونية تسري هذه المسؤولية استنادًا إلى أحكام المسؤولية التقصيرية والعقدية، التي تحدد تعويضات عن الأضرار الناتجة عن أي إخلال بهذه الالتزامات، كما تتحدد أيضا وفق القواعد الخاصة من خلال التشريعات التي توجهت لوضع قواعد خاصة لمزودي خدمات التصديق الإلكتروني وذلك لتجاوز بعض النقص الذي قد تحمله القواعد العامة.

الأصل أن مزود خدمة التصديق الإلكتروني مسؤول عن تعويض جميع الأضرار الناشئة عن أخطائه الشخصية وأخطاء تابعيه، ولكنه لا يتحمل مسؤولية الأضرار الناشئة عن أخطاء مستخدمي هذه الخدمة، أو عن عدم التزامهم بالالتزامات المختلفة والأساسية التي تفرضها عليهم شهادة التصديق الإلكتروني.

وللتفصيل في أحكام المسؤولية المدنية لمؤدي خدمات التصديق الإلكتروني، سنحاول دراستها وفقا لما هو وارد في الأحكام العامة (المطلب الأول)، ثم سوف نتطرق إلى القواعد الخاصة المنظمة لهذه المسؤولية من جهة أخرى (المطلب الثاني).

المطلب الأول: المسؤولية المدنية لمزود خدمات التصديق الالكتروني وفق القواعد العامة

تعد المسؤولية المدنية لمزود خدمات التصديق الإلكتروني جزءًا مهمًا من القانون المدني، حيث تتحدد من خلال المسؤولية العقدية والتقصيرية. في المسؤولية العقدية، يلتزم المزود بتنفيذ التزاماته التعاقدية مثل صحة الشهادات الرقمية وحماية البيانات، ويكون مسؤولاً عن أي ضرر ناتج عن إخلاله بتلك الالتزامات، مما يتيح للمتضررين المطالبة بالتعويض وفقًا لشروط العقد. أما في المسؤولية التقصيرية، فيمكن أن يتحمل المزود المسؤولية عن الأضرار حتى في غياب عقد مباشر، إذا ثبت أن خطأً أو إهمالاً منه أدى إلى وقوع الضرر، مما يستوجب التعويض استنادًا إلى القواعد العامة للمسؤولية في القانون المدني.

الفرع الأول: المسؤولية العقدية

تقوم المسؤولية العقدية في حال إخلال المدين بأحد التزاماته التعاقدية سواء كليا أو جزئيا أو تأخر في تنفيذ التزامه، ونتج عن هذا الإخلال ضرار للطرف الثاني في العلاقة التعاقدية.

قياسا على مسؤولية مزود خدمة التصديق الالكتروني فإنه قد يلحق العميل صاحب شهادة التوثيق أضرار نتيجة إخلال مزود خدمات التوثيق بأحد الالتزامات الملقاة على عاتقه بموجب عقد التوثيق المبرم بينهما أو بموجب نص القانون، حيث يحق لمزود التوثيق والعميل صاحب الشهادة وضع ما يريدون من شروط والتزامات متبادلة طبقا لمبدأ الحرية التعاقدية وسلطان الإرادة فإذا أخل مزود خدمات التوثيق أو العميل بإحدى هذه الالتزامات تنعقد مسؤوليتهما العقدية، فإذا قام مزود التوثيق بإصدار شهادة غير دقيقة أو تخالف البيانات التي قدمها له العميل ونتج عن ذلك ضرر لهذا العميل تقوم مسؤوليته العقدية[1].

تؤدي المسؤولية العقدية إلى تعويض المتعاقد لما أصابه من ضرر بسبب عدم تنفيذه لالتزاماته التعاقدية، وتفترض المسؤولية وجود عقد صحيح واجب التنفيذ بحيث تقوم هذه المسؤولية عند عدم الوفاء بالالتزام المتفق عليه في العقد، مما يلحق الضرر بالمتعامل، ولقيام هذه المسؤولية لمزودي خدمات التصديق الإلكتروني يجب توافر ثلاث شروط وهي: الخطأ العقدي، الضرر، العلاقة السببية بين الخطأ والضرر.

أولا: الخطأ العقدي

يتحمل مقدم خدمات التصديق الإلكتروني المسؤولية عن إخلاله بالعقد الناتج عن مخالفة أي من الالتزامات الملقاة على عاتقه، وينشأ هذا الالتزام لأنه يضمن حصول المتعاقد على شهادة تصديق تتضمن كافة البيانات الأساسية بعد التحقق من صحة البيانات المقدمة للأشخاص الذين صدرت لهم شهادات التصديق وخصائصهم المميزة، والتي تضمنتها الشهادة، ويعرف هذا النوع من الالتزامات بأنه الالتزام الأكثر دقة وصعوبة فيما يتعلق بأداء هيئات التصديق الإلكتروني، والذي يحتاج إلى كادر

[1] علاء الدين الخصاونة، أيمن مساعده، مرجع سابق، ص 120.

وظيفي وفني مناسب ومتخصصين ذوي خبرة للتحقق من البيانات المقدمة وأهلية الشخص الذي صدرت له الشهادة للطرف المتعاقد.

قد يؤدي الإخلال بالالتزام التعاقدي في المسؤولية العقدية إلى أن يتحمل المدين التعويض عن الأضرار المتوقعة وغير المتوقعة وذلك في حالتين نصت عليهما المادة 182 الفقرة 2 من القانون المدني الجزائري:

الحالة الأولي: إذا ارتكب المدين عن طريق الغش أو التدليس أو تعمد عدم الوفاء بالالتزام أو تأخر في تنفيذه، لا يمكن اعتباره حسن النية وبالتالي لا يخضع للمبدأ الواجب اتباعه في العلاقة التعاقدية.

الحالة الثانية: إذا ارتكب المدين خطأ جسيما، وهو الخطأ الذي لا يصدر من أقل الناس تبصرا، فجسامة الخطأ تجعل المدين مسؤولا عن الأضرار غير المتوقعة مع الأخذ بعين الاعتبار الأضرار المتوقعة.

إذا كان التزام مزود خدمات التصديق الالكتروني هو التزام ببذل عناية كالتزامه بالتحقق من صحة البيانات التي تتضمنها شهادة التصديق الالكتروني فيتحقق الخطأ العقدي بعدم بذل العناية الكافية من جانب مزود خدمات التصديق الالكتروني، أما إذا كان التزامه هو التزام بتحقيق نتيجة كالتزامه بالسرية فإنه يتحقق الخطأ العقدي بعدم تحقق النتيجة أو الغاية المطلوبة، وفي حال كان العقد خاليا من تحديد من يقع عليه عبء إثبات الخطأ، فإنه وتطبيقا للقواعد العامة يقع عبء إثبات الخطأ على من يدعي وقوع الخطأ[1].

يتخذ افتراض المسؤولية العقدية أساساً لتسجيل خطأ من جانب المدين الذي لم ينفذ التزامه كلياً أو جزئياً أو تأخر في تنفيذه، ولا يجوز للمدين أن ينكر افتراض الخطأ من جانبه إلا إذا أثبت أن عدم التنفيذ ناشئ عن سبب خارجي لا يد له فيه، على سبيل المثال إذا أثبتت الجهة المكلفة بالتصديق والتوثيق أن عدم تنفيذ التزامها المتعلق بضمان دقة البيانات كان بسبب فعل من جانب المدين نفسه، أي بتقديم مستندات مزورة أو وهمية، أو إذا أوضحت أن سبب عدم إصدار شهادة التصديق في الموعد

[1] هيثم الطاس، محمد فائز خضور، مرجع سابق، ص 89.

المتفق عليه كان نتيجة تأخر حامل الشهادة في نقل البيانات المتعلقة بهويته، أو أنه لم يكشف عن جميع أسرار حامل الشهادة بناءً على حكم قضائي[1].

كما يمكن تصور المسؤولية التعاقدية لمزود خدمة التصديق الالكتروني تجاه طرف ثالث إذا كان الأخير مرتبطًا بعلاقة تعاقدية مباشرة ونتج عن خرق هذا العقد ضرر له، مثل اعتماد مزود المصادقة الإلكترونية التابع للغير على الشهادة التي اطلع عليها نتيجة لعقد أبرمه مع المزود، ثم تبين أن هذه الشهادة غير صالحة أو تم إلغاؤها أو تعليقها ولم تكن هناك رسالة تعلن عن هذا الوضع من مزود خدمات المصادقة، مما تسبب في ضرر له لأنه أبرم عقودًا مع المتعاقد صاحب الشهادة الالكترونية بناءً على الثقة في الشهادة الإلكترونية.

ثانيا: الضرر

فيما يتعلق بمقدمي خدمات التصديق الإلكتروني، لا يكفي أن تنتهك جهة التصديق أيًا من الالتزامات التعاقدية المرتبطة بها، ولا يكفي خطأ تعاقدي واحد لإحداث المسؤولية التعاقدية، بل يجب أن يكون حامل الشهادة قد تضرر نتيجة لهذا الانتهاك، وإذا كان هناك سبب وجيه لتعليق أو إلغاء الشهادة الالكترونية، وفشلت جهة التصديق في تنفيذ هذا التعليق أو الإلغاء، فإنها بذلك تكون قد أخلت بأحد التزامها المفروضة عليها بموجب العقد.

فإذا فقد صاحب الشهادة مفتاحه الخاص وطلب من جهة التصديق إلغاء العمل بشهادة التصديق ولم يستجب لطلبه، وترتب عن ذلك استعمال الغير لهذا المفتاح في فعل غير مشروع باسم صاحب المفتاح دون ترخيص منه أو علم به فهنا كنتيجة حتمية تقوم المسؤولية العقدية في مساءلة مقدم خدمات التصديق الإلكتروني لتعويض صاحب الشهادة عن الضرر الذي لحق به.

هنا تجدر الإشارة أن المشرع الجزائري في قانون التوقيع والتصديق لم يذكر في مواده التزام مؤدي خدمات التصديق الإلكتروني بتعليق العمل بشهادة التصديق، بل ذكر التزامها بالإلغاء فقط، وقد حدد حالاته في الفقرة 1 و 2 من المادة 45 من نفس القانون، وبالتالي فإن أي ضرر ينتج عن الإخلال

[1] لينا إبراهيم يوسف حسان، مرجع سابق، ص 160.

بالالتزامات التعاقدية بين جهة التصديق وصاحب الشهادة، يرتب مسؤولية عقدية في مواجهة مقدم الخدمة، تلزمه بتعويض صاحب شهادة التصديق الإلكتروني[1].

في إطار المسؤولية العقدية، الضرر الذي يمكن أن ينشأ عن مزود خدمة التصديق الإلكتروني يرتبط بشكل مباشر بالتزامات هذا المزود تجاه المستخدمين وفقاً للعقد الموقع بين الطرفين، وبذلك فإنه يمكن أن تشمل الأضرار التي يتحملها مزود خدمة التصديق الإلكتروني في حال الإخلال بالتزاماته الأضرار على الشكل التالي:

- **الأضرار المالية:** إذا تسبب الإخلال في العقد بتعرض المستخدم لخسائر مالية، مثل خسارة صفقة أو دفع مبالغ إضافية بسبب تعطل الخدمة أو إصدار شهادات غير دقيقة.
- **الأضرار المتعلقة بالثقة:** قد يؤدي إصدار شهادات تصديق غير صحيحة أو غير دقيقة إلى فقدان الثقة في النظام بأكمله، مما يتسبب في ضرر للشركات أو الأفراد المعتمدين على هذه الشهادات.
- **الأضرار القانونية:** يمكن أن تترتب على مزود خدمة التصديق الإلكتروني مسؤولية قانونية إذا أدى الإخلال بالتزاماته إلى تعرض المستخدمين لمشاكل قانونية، مثل استخدام شهادات مزورة أو غير صالحة.
- **الأضرار الشخصية:** قد تؤثر بعض الحالات على حقوق المستخدمين أو سمعتهم الشخصية إذا لم يتم التأكد من هوية الأشخاص الموقعين أو المعتمدين بشكل صحيح.

لذلك فإن مزود خدمة التصديق الإلكتروني ملزم باتخاذ التدابير الضرورية لضمان صحة وموثوقية الشهادات الإلكترونية التي يقدمها.

تنص المادة 176 من القانون المدني أنه لا مسؤولية مدنية إذ لم يوجد ضرر وذلك أن وقوع الخطأ لا يكفي وحده لقيامه المسؤولية وإنما يجب أن ينتج عن هذا الخطأ ضرر يصيب الدائن، وبالتالي فإن انتفاء الضرر يحول دون قبول دعوى المسؤولية وذلك طبقا لقاعدة: "لا دعوى بدون مصلحة" والحقيقة أن الضرر ليس بركن فقط في المسؤولية المدنية بل هو مقياس مقدار التعويض الذي يستحقه

[1] دوار جميلة، المسؤولية المدنية العقدية لمقدمي خدمات التصديق الالكتروني في التشريع الجزائري، ورقة مقدمة ضمن فعاليات الملتقى الوطني الموسوم حول المسؤولية القانونية في الإدارة الالكترونية، جامعة الجزائر، 13 ديسمبر 2023.

المضرور[1]، وفي عنصر الضرر تقع مسؤولية إثبات الضرر على عاتق الدائن، فلا يكفي أن يحصل الشخص على الحقوق التي يطلبها بناءً على مطالبة، بل يجب عليه أن يثبت أنه يمتلك الأدلة التي تدعم طلبه، كما أنه من غير الممكن إثبات أن المدين لم يقم بتنفيذ التزامه، مما يؤدي إلى افتراض وقوع الضرر، لأنه قد لا يقوم المدين بتنفيذ التزامه وقد لا يلحق بالدائن أي ضرر.

ثالثا: العلاقة السببية بين الخطأ والضرر

في إطار المسؤولية العقدية، فإن العلاقة السببية بين الخطأ العقدي والضرر هي الأساس الذي يقوم عليه تحميل المسؤولية، بالنسبة لمزود خدمة التصديق الإلكتروني، يجب إثبات وجود ارتباط مباشر بين الخطأ الذي ارتكبه المزود (أي الإخلال بالتزاماته التعاقدية) وبين الضرر الذي لحق بالمستخدم نتيجة لذلك. هذه العلاقة تتطلب إثبات أن الضرر الذي حدث للمستخدم كان نتيجة مباشرة أو غير مباشرة للخطأ الذي ارتكبه مزود الخدمة، يجب أن يكون الخطأ هو السبب الأساسي الذي أدى إلى وقوع الضرر، وليس مجرد عامل عرضي. **مثال ذلك:** إذا أصدر مزود خدمة التصديق الإلكتروني شهادة إلكترونية غير صحيحة أو مزورة، واعتمد المستخدم عليها لإتمام صفقة تجارية وتعرض لخسارة مالية، هنا يمكن للمستخدم المطالبة بالتعويض إذا أثبت أن الخطأ في التصديق الإلكتروني هو السبب المباشر لهذه الخسارة.

إجمالاً، العلاقة السببية تعد ركنًا أساسيًا في المسؤولية العقدية؛ إذ لا يمكن المطالبة بالتعويض إذا لم يكن الضرر نتيجة مباشرة للخطأ المرتكب من قبل مزود خدمة التصديق الإلكتروني.

أما إذا ثبت أن جهة التوثيق لم تقترف أي خطأ من جانبها وإنما الضرر الذي حصل قد يعود إلى خطأ المضرور نفسه، وذلك في حال أن هذا المضرور كان عليه اتخاذ إجراءات وخطوات معينة للتأكد من مصداقية التوقيع الإلكتروني المثبت على الشهادة، أو أنه اعتمد على شهادة توثيق مع علمه أنها موقوفة أو ملغاة، أو أنه لم يراع القيود المفروضة على الشهادة، فهنا يسأل المضرور نفسه عن خطأه ولا تسأل جهة التوثيق عن هذا الضرر[2].

---

[1] علي فيلالي، التزامات العمل المستحق للتعويض، موفم للنشر والتوزيع، الجزائر، 2002، ص 243.

[2] دوار جميلة، مرجع سابق.

ومع ذلك يشترط انتفاء وجود السبب الأجنبي بحيث يجب أن يتم استبعاد أي أسباب خارجية غير مرتبطة بمزود الخدمة، مثل القوة القاهرة أو تدخل طرف ثالث مستقل، التي قد تكون أدت إلى وقوع الضرر.

إلا أنه تجدر الإشارة إلى أن مزود خدمات التصديق الإلكتروني يمكنه نفي العلاقة السببية بين الخطأ العقدي والضرر، وذلك متى تبين أن الخطأ كان نتيجة سبب أجنبي خارج عن إرادته يعود الى قوة قاهرة أو حادث فجائي متى توافرت شروطه، ففي هذا الصدد لا يلتزم مزود خدمة التصديق الالكتروني بالتعويض عن الضرر.

في الأخير يمكن القول أن مزود خدمة التصديق الالكتروني لا يتحمل أي التزام لا ببذل عناية ولا بتحقيق نتيجة وذلك في مواجهة الشخص الذي لا تربطه به أي علاقة تعاقدية، باعتبار أن هذه الالتزامات لا تجد محلا لها إلا في العلاقات العقدية.

الفرع الثاني: المسؤولية التقصيرية

المسؤولية التقصيرية بالنسبة لمزود خدمة التصديق الإلكتروني تتعلق بالتزام هذا المزود باتباع معايير وضوابط معينة لضمان سلامة وموثوقية الشهادات الإلكترونية التي يصدرها، وتعتبر هذه المسؤولية نوعًا من المسؤولية المدنية التي تقوم على الخطأ أو التقصير في أداء الخدمة، فإذا ارتكب مزود خدمة التصديق الإلكتروني خطأ أو تقصيرًا أدى إلى إلحاق ضرر للدائن، فإنه يتحمل المسؤولية عن هذا الضرر.

فالمسؤولية التقصيرية لمزودي خدمات التصديق الإلكتروني تتجسد في الجزاء الذي يرتبه القانون عن الإخلال بالواجبات القانونية التي تهدف في أساسها إلى التعويض عن الضرر الذي أصاب شخصا نتيجة خطأ شخص آخر دون أن يكون هذا الإخلال بالتزام تعاقدي بين مرتكب الخطأ والمتضرر وقوام هذه المسؤولية التزام قانوني يتمثل في عدم الإضرار بالغير، فالمسؤولية التقصيرية لمؤدي خدمات التصديق الإلكتروني تتجلى في مسؤولية تعويض الضرر الذي أصاب الغير[1].

[1] سعدي الربيع، حجية التوقيع الالكتروني في التشريع الجزائري، أطروحة دكتوراه في العلوم القانونية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2016، ص 153.

فالمسؤولية التقصيرية لمؤدي خدمات التصديق الإلكتروني تتجلى من مسؤولية تعويض الضرر الذي أصاب الغير الذي تتضمنها هذه الشهادة دون أن يطلبها مباشرة ودون وجود عقد يتضمن شرط الاشتراط لمصلحة الغير، ويترتب على قيام المسؤولية التقصيرية نشوء حق المضرور بسبب الفعل الضار في المطالبة بالتعويض عن الضرر الذي أصابه من المسؤول عن الضرر[1].

من أجل مساءلة مزود خدمة التصديق الإلكتروني عن تقصيره في تنفيذ التزاماته ومطالبته بالتعويض عن الضرر الذي تسبب به للغير لا بد من توافر ثلاث أركان رئيسية مثل ما هو الأمر بالنسبة للمسؤولية التعاقدية، وتتمثل هذه الأركان في: الخطأ الواقع من مزود الخدمة، الضرر الواقع على الطرف الآخر، والعلاقة السببية بين الخطأ التقصيري والضرر.

أولا: الخطأ التقصيري

الخطأ التقصيري بالنسبة لمزود خدمة التصديق الإلكتروني يشير إلى الإهمال أو التقصير الذي قد يحدث من قبل المزود عند تقديم خدمات التصديق الإلكتروني، هذه الأخطاء قد تشمل عدم الالتزام بالمعايير الأمنية المعتمدة أو تقديم خدمات غير موثوقة أو غير دقيقة، مما يمكن أن يؤدي إلى تعرض البيانات للخطر أو انتهاك حقوق المستخدمين.

في العديد من البلدان، يُطلب من مزودي خدمات التصديق الإلكتروني الالتزام بمسؤوليات قانونية معينة لضمان حماية بيانات المستخدمين وصحة المعلومات التي يتم تصديقها، وإذا تم التقصير في هذه المسؤوليات أو ارتكاب أخطاء نتيجة للإهمال، يمكن أن يكون المزود مسؤولاً قانونيًا أمام المستخدمين أو الجهات المعنية.

ومن الأمثلة الشائعة على الخطأ التقصيري فإنها قد تشمل:

- عدم التحقق من هويات المستخدمين بشكل صحيح.
- الفشل في حماية مفاتيح التشفير بشكل كافٍ.
- عدم الالتزام بالتشريعات والقوانين المتعلقة بالتصديق الإلكتروني.

[1] زهيرة عبوب، المسؤولية المدنية لمقدم خدمات التصديق الالكتروني (دراسة تحليلية لما جاء في القانون رقم 04/15)، مجلة الدراسات القانونية المقارنة، المجلد 6، العدد 2، جامعة حسيبة بن بوعلي، الشلف، 2020، ص 431.

وبما أن المسؤولية التقصيرية تقوم نتيجة للإخلال بالالتزامات التي يفرضها القانون، فإن الخطأ أو الفعل الضار ينتفي في حق جهة التوثيق إذا ما أخلت بأي من الالتزامات التي يفرضها القانون، فإذا كان القانون يوجب تعليق العمل بالشهادة أو إلغائها لأي سبب من الأسباب التي يحددها وأخلت جهة التوثيق بهذا الالتزام رغم توافر السبب الموجب لذلك مما أدى إلى الإضرار بالغير الذي استند إلى الشهادة المفروض تعليق العمل بها أو إلغاؤها، فإنها تكون مسؤولة عن تعويض الضرر الذي لحق بالغير[1].

ثانيا: الضرر

الضرر هو العنصر الحاسم الذي يؤدي إلى المسؤولية القانونية، فالضرر يشير إلى الخسائر أو الأضرار التي تلحق بالمستخدم أو الأطراف المتعاقدة نتيجة لتقصير أو إهمال مزود الخدمة، وقد يكون الضرر إما ماليا، وإما معنويا، وإما تقنيا:

- **الضرر المالي:** يحدث عندما يتسبب الخطأ أو الإهمال من مزود الخدمة في خسائر مالية للمستخدم. على سبيل المثال، إذا فشل مزود خدمة التصديق الإلكتروني في حماية المفاتيح الرقمية أو إصدار شهادات مزورة أو غير دقيقة، قد يتسبب ذلك في خسائر مالية للمستخدم نتيجة عمليات احتيالية.
- **الضرر المعنوي:** قد يشمل الضرر المعنوي فقدان السمعة أو الضرر النفسي الذي يلحق بالأطراف المتضررة نتيجة استخدام شهادات تصديق إلكتروني غير صحيحة أو مزيفة. على سبيل المثال، إذا تم استخدام تصديق غير صحيح للإضرار بسمعة مؤسسة ما أو فرد، قد يترتب على ذلك ضرر معنوي.
- **الضرر الأمني أو التقني:** إذا تسبب الإهمال في تسريب بيانات المستخدمين أو اختراق أمني أدى إلى انتهاك الخصوصية أو فقدان البيانات الشخصية الحساسة، فهذا يعتبر ضررًا أمنيًا. هذا النوع من الضرر قد يشمل تعرض المستخدمين لسرقة هوياتهم أو بياناتهم الحساسة.

[1] لينا إبراهيم يوسف حسان، مرجع سابق، ص 165.

إذا ثبت أن الضرر ناتج عن تقصير مزود خدمة التصديق الإلكتروني في الالتزام بالمعايير الأمنية أو الإجرائية المعمول بها، يكون الضرر هو أساس أي مطالبة قانونية ضد مزود خدمة التصديق الإلكتروني في حال تقصيره في أداء واجباته.

ثالثا: العلاقة السببية بين الخطأ التقصيري والضرر

العلاقة السببية هي أحد العناصر الأساسية في المسؤولية التقصيرية، وتعتبر الجسر الذي يربط بين الخطأ التقصيري الذي يرتكبه مزود خدمة التصديق الإلكتروني والضرر الذي لحق بالمستخدم أو الطرف المتضرر، بحيث أنه بدون إثبات هذه العلاقة السببية، لا يمكن للمستخدم المتضرر المطالبة بتعويض عن الضرر.

العلاقة السببية تعني أن الخطأ أو التقصير الذي ارتكبه مزود خدمة التصديق الإلكتروني هو السبب المباشر أو الرئيسي الذي أدى إلى وقوع الضرر، بمعنى آخر، يجب أن يكون الضرر نتيجة مباشرة لإهمال أو تقصير مزود الخدمة، وأنه لولا هذا الإهمال لما وقع الضرر[1].

لإثبات العلاقة السببية بين الخطأ التقصيري والضرر، يجب على المتضرر أن يثبت:

- **وجود خطأ أو تقصير**: يجب أن يثبت المستخدم أن مزود الخدمة قد ارتكب خطأ معينًا، سواء كان ذلك من خلال عدم الامتثال للمعايير الفنية أو الأمنية المعمول بها، أو من خلال إصدار شهادات تصديق إلكتروني غير دقيقة أو غير صحيحة.
- **وقوع الضرر**: يجب أن يكون هناك ضرر ملموس أو مادي لحق بالمستخدم. يمكن أن يكون هذا الضرر ماديًا (مثل خسارة مالية) أو معنويًا (مثل الإضرار بالسمعة أو الخصوصية).
- **العلاقة السببية**: يجب أن يثبت المستخدم أن الضرر الذي تعرض له هو نتيجة مباشرة للخطأ الذي ارتكبه مزود خدمة التصديق الإلكتروني، هذا يعني أن الإهمال أو التقصير كان العامل الأساسي الذي أدى إلى حدوث الضرر.

ومن أمثلة العلاقة السببية: إصدار شهادة تصديق غير صحيحة بحيث إذا قام مزود خدمة التصديق الإلكتروني بإصدار شهادة غير صحيحة لهوية شخص معين، وتم استخدام هذه الشهادة

[1] محمد المدني، نظرية السبب في القانون المدني، دار الفكر العربي، القاهرة، مصر، 1995، ص 245.

للقيام بعملية احتيالية أدت إلى خسائر مالية للطرف المتضرر، فإن العلاقة السببية تكون واضحة بين الخطأ التقصيري (إصدار الشهادة الخاطئة) والضرر (الخسارة المالية).

كذلك في حالة فشل في تأمين البيانات فإذا تقاعس مزود الخدمة في اتخاذ تدابير أمان كافية لحماية مفاتيح التشفير أو البيانات الشخصية، وتم اختراق النظام وسرقة بيانات المستخدمين مما أدى إلى انتهاك الخصوصية أو تعرضهم للاحتيال، فإن العلاقة السببية بين الإهمال في تأمين البيانات والضرر الناتج تكون مثبتة.

في بعض الحالات، قد يكون هناك تدخل لعوامل خارجية تؤدي إلى انقطاع العلاقة السببية بين الخطأ والضرر، إذا كان هناك عامل خارجي أو طارئ هو الذي تسبب في حصول الضرر وليس خطأ مزود الخدمة، فقد يؤدي ذلك إلى انقطاع العلاقة السببية، وبالتالي لا يكون مزود الخدمة مسؤولاً عن التعويض[1].

مثال ذلك: إذا قام مزود الخدمة بتقديم شهادات تصديق صحيحة وأمنة، ولكن تعرضت الأجهزة الخاصة بالمستخدم للاختراق نتيجة إهماله الشخصي أو استخدامه لنظم غير مؤمنة، فإن العلاقة السببية قد تنقطع هنا لأن سبب الضرر لا يعود إلى تقصير مزود الخدمة.

في الأخير يجدر بالذكر أن مزود خدمات التصديق الالكتروني قد يكون مسؤولا قانونا بمبلغ كبير من المال تجاه عدة أشخاص بحكم أنه مخوّل بصنع الكثير من التواقيع الالكترونية خلال فترة قصيرة جدا لما تتطلبه هذه المعاملات من سرعة ودقة، وبذلك لا يكون أمام مزود خدمة التصديق الالكتروني الوقت الكافي لإدراك الخطأ واكتشافه.

المطلب الثاني: المسؤولية المدنية لمزودي خدمة التصديق الالكتروني وفق القواعد الخاصة

تعد المسؤولية المدنية لمزود خدمات التصديق الإلكتروني موضوعًا تنظمه التشريعات المقارنة في مختلف الدول لتأمين الثقة في المعاملات الإلكترونية. في العديد من الأنظمة القانونية، مثل قانون الاتحاد الأوروبي للتوقيعات الإلكترونية، والقانون النموذجي للأمم المتحدة بشأن التوقيعات الإلكترونية، يتحمل مزود الخدمة مسؤولية مباشرة عن أي ضرر يلحق بالأطراف نتيجة تقديم شهادات رقمية غير

[1] عبد الرحمن الفقي، أصول المسؤولية المدنية، دار وائل للنشر، عمان، الأردن، 2003، ص 98.

دقيقة أو إخفاقه في تأمين البيانات الشخصية، هذه التشريعات تلزم مزودي الخدمات بالتقيد بمعايير صارمة لضمان سلامة وموثوقية الشهادات الرقمية.

على غرار ذلك، يفرض التشريع الجزائري، من خلال القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكتروني، التزامات على مزودي الخدمة لضمان صحة الشهادات وتأمين المعلومات، إذا أخل المزود بهذه الالتزامات، فإنه يتحمل المسؤولية المدنية ويُلزم بتعويض المتضررين، مما يضع التشريع الجزائري في سياق مشابه للتشريعات المقارنة التي تسعى لحماية حقوق المستخدمين في البيئة الرقمية.

الفرع الأول: مسؤولية مزودي خدمة التصديق الالكتروني وفقا للتشريعات المقارنة

تعد مسؤولية مزودي خدمة التصديق الإلكتروني أحد المواضيع الحيوية في التشريعات المتعلقة بالتوقيعات الإلكترونية، حيث تفرض هذه المسؤولية ضمان أمن وصحة التوقيعات الرقمية والمعلومات المرتبطة بها. وفقًا للتوجيه الأوروبي للتوقيعات الإلكترونية (Directive 1999/93/EC) يتم تحديد التزامات مزودي الخدمات لضمان أن التوقيعات الرقمية تتوافق مع معايير الأمان والمصداقية. أما في التشريع الفرنسي، فإن القانون رقم 2000-230 المؤرخ في 13 مارس 2000، المتعلق بتكييف القانون المدني مع التوقيعات الإلكترونية، ينص على التزامات واضحة لمزودي الخدمة، حيث يتحملون مسؤولية اتخاذ التدابير اللازمة للحفاظ على أمان البنية التحتية الرقمية ومنع إساءة الاستخدام أو الاحتيال. هذه التشريعات تهدف إلى تعزيز الثقة في المعاملات الإلكترونية من خلال تحديد واضح للمسؤوليات والواجبات القانونية لمزودي الخدمات.

أولا: مسؤولية مزود خدمة التصديق الالكتروني وفقا للتوجيه الأوربي 1999/93

التوجيه الأوروبي للتوقيعات الإلكترونية (Directive 1999/93/EC) هو أحد المعايير التي وضعت لضمان الموثوقية في استخدام التوقيعات الإلكترونية عبر دول الاتحاد الأوروبي، بحيث أنه وفقًا للمادة 6 من التوجيه، يتحمل مزودو خدمة التصديق الإلكتروني مسؤولية التأكد من دقة المعلومات

المقدمة من العملاء قبل إصدار الشهادات الرقمية، كما يجب عليهم استخدام تكنولوجيا حديثة لضمان أمان التوقيعات ومنع التلاعب بها[1].

وقد خصص التوجيه الأوروبي قواعد لتنظيم كيفية تحميل مقدم خدمات المصادقة المسؤولية بقواعد خاصة تتوافق مع طبيعة العمل الذي يقوم به والغرض الذي يخدمه، فضلاً عن الأهمية الكبيرة لعملية المصادقة الإلكترونية في التعاقد عبر الإنترنت وزيادة الثقة في التجارة، وقد جاء هذا التوجيه بعدة قواعد تصف على وجه التحديد طبيعة المسؤولية عن الخدمات الإلكترونية والمصادقة الإلكترونية، وتتميز هذه القواعد عن القواعد العامة للمسؤولية.

وقد أرسى التوجيه الأوروبي نظاماً رسمياً من القواعد فيما يتصل بمسؤولية مؤدي خدمات التصديق الالكتروني، يقوم على ضرورة التمييز بين السجل الإلكتروني المعتمد والسجل غير المعتمد. كما حاول التوجيه الأوروبي زيادة مسؤوليتهم باعتبارها مسؤولية مفترضة، بالإضافة إلى أنه سمح بإمكانية الحد من نطاق أو مدى مسؤوليته، ما لم يثبت المورد خلاف ذلك، فيما يتصل بقيمة أو نوع المعاملات التي تتم عبر التصديق الإلكتروني.

لقد نظم التوجيه الأوروبي لسنة 1999 مسؤولية مزود خدمات التصديق الإلكتروني بموجب قواعد خاصة تنسجم مع طبيعة المهمات التي يقوم بها هؤلاء المزودين، والوظيفة التي يضطلعون بها، وبالنظر إلى الأهمية البالغة التي تمثلها عملية التوثيق الإلكتروني في التعاقد عبر الإنترنت، ومنح الثقة في التجارة الإلكترونية، وقد جاء هذا التوجيه بتعريز خصوصية قواعد المسؤولية عن خدمات التوثيق الإلكتروني والتي تتميز عن القواعد العامة في المسؤولية.

ثانيا: مسؤولية مزود خدمة التصديق الأوربي وفقا للقانون الفرنسي

في فرنسا، يتم تنظيم التوقيعات الإلكترونية بموجب قانون الثقة الرقمية الصادر عام 2000. تماشياً مع التوجيه الأوروبي، يتحمل مزودو خدمة التصديق مسؤولية كبيرة لضمان أمان التوقيعات

[1] نذكر في هذا الشأن قضية عام 2017، حيث قررت محكمة العدل الأوروبية تحميل مزود خدمة تصديق مسؤولية نتيجة عدم كفاية التحقق من هوية أحد الموقعين، مما أدى إلى استخدام الشهادة الرقمية بطريقة احتيالية لتوقيع عقد تجاري مزور، هذه القضية أبرزت أهمية الإجراءات الصارمة للتحقق من هوية المستخدمين لتجنب استغلال التوقيعات بشكل غير قانوني.

والتحقق من صحة الشهادات الممنوحة. يتم إلزام مزودي الخدمة بتقديم كافة المعلومات المتعلقة بعملية التصديق لمستخدميهم لضمان الشفافية، ففي إحدى القضايا المتعلقة بمزود خدمة فرنسي، أصدرت المحكمة حكماً بتغريمه بسبب إهماله في استخدام تقنيات حديثة لتأمين البيانات، مما أدى إلى اختراق بيانات التوقيع الإلكتروني واستخدامها بشكل غير قانوني.

القانون الفرنسي يعتبر التصديق الإلكتروني جزءاً من القواعد التي تضمن أمان المعاملات الرقمية. يخضع مزودو خدمات التصديق الإلكتروني في فرنسا إلى إطار قانوني ينظم مسؤولياتهم ويحدد كيفية العمل مع الجهات الحكومية والقطاع الخاص. من أهم التشريعات التي تحكم هذا المجال هي **قانون الثقة في الاقتصاد الرقمي (LCEN)** لعام 2004، والذي يحدد بوضوح متطلبات الثقة والسلامة الواجب على مزودي خدمات التصديق الالتزام بها[1].

تُعتبر اللائحة الأوروبية **eIDAS**، التي دخلت حيز التنفيذ في عام 2016، مرجعاً أساسياً أيضاً حيث وضعت الإطار العام للتوقيع والتصديق الإلكتروني وتوحيد القواعد في جميع دول الاتحاد الأوروبي بما فيها فرنسا. هذه اللائحة تضمن لمزودي خدمات التصديق الإلكتروني المسؤولية عن توفير أدوات موثوقة ومتوافقة مع متطلبات الأمان العالية[2].

كما نص القانون رقم 575 لسنة 2004، والخاص بتعزيز الثقة في الاقتصاد الرقمي، على القواعد الخاصة بمسؤولية جهة التصديق وذلك في المادة 33 منه، المتضمنة مسؤولية جهة التصديق الإلكتروني على أساس الخطأ المفترض منها، وأن للمضرور إثبات حالة من الحالات التالية[3]:

المعلومات الواردة في الشهادة؛

عدم اكتمال البيانات التي أوجب القانون توافرها في شهادة التصديق الإلكتروني، إذا لم تقم جهة التصديق الإلكتروني بتسجيل إلغاء الشهادة في القائمة الخاصة بالشهادة الملغاة.

[1] Eric Capitaine, The Law on Digital Economy Trust and its Applications, European Law Publishing House, France, 2005, P 45.

[2] Nicolas Bernard, The Legal Framework of Trust in Digital Services in the European Union: eIDAS Regulation, European Legal Publishing House, Belgique, 2017, P 70.

[3] زهرة عبوب، مرجع سابق، ص 434.

ثالثا: مسؤولية مزود خدمة التصديق الالكتروني وفقا لبعض التشريعات العربية

1/- التشريع التونسي

التشريع الرئيسي الذي يحكم التصديق الإلكتروني في تونس هو القانون رقم 83 لسنة 2000 المتعلق بالمبادلات والتجارة الإلكترونية. هذا القانون ينظم شروط وضوابط التصديق الإلكتروني ومسؤوليات المزودين لضمان أمان المعاملات الإلكترونية،[1] نص القانون التونسي على أن مزودي خدمات التصديق الإلكتروني يجب أن يلتزموا بحماية البيانات الشخصية للمستخدمين وضمان سرية المعاملات، ويخضعون لقوانين حماية البيانات مثل القانون رقم 63 لسنة 2004 المتعلق بحماية المعطيات الشخصية[2].

يتعرض مزودو خدمات التصديق في تونس للمساءلة القانونية في حالة وقوع أضرار ناتجة عن إصدار شهادة غير صحيحة أو إخفاق في حماية بيانات المستخدمين. يشير القانون إلى أنه يجب على المزود تحمل المسؤولية تجاه الأضرار الناتجة عن التقصير أو الخطأ.

2/- التشريع الإماراتي

القانون الأساسي الذي يحكم خدمات التصديق الإلكتروني في الإمارات هو القانون الاتحادي رقم 1 لسنة 2006 بشأن التجارة الإلكترونية والمعاملات الرقمية. ينظم هذا القانون شروط وضوابط التصديق الإلكتروني ومسؤوليات مقدمي الخدمات، من مسؤوليات مزودي خدمة التصديق التحقق من هوية المستخدمين قبل إصدار الشهادات الرقمية. يتطلب القانون الإماراتي اعتماد آليات صارمة للتحقق لضمان موثوقية وأمن التعاملات الإلكترونية[3].

---

[1] عبد الحميد بن منصور، القانون التونسي للمبادلات والتجارة الإلكترونية: دراسة تحليلية، دار الفكر القانوني، تونس، 2002، ص 45.

[2] فاتن الكوكي، حماية المعطيات الشخصية في البيئة الرقمية في تونس، المركز العربي للدراسات القانونية، 2005، ص 80.

[3] عبد الله المزروعي، التوقيع الإلكتروني وإصدار الشهادات في القانون الإماراتي، دار النهضة القانونية، الإمارات العربية المتحدة، 2015، ص 120.

3/- التشريع المصري

يُعتبر قانون التوقيع الإلكتروني رقم 15 لسنة 2004 الإطار القانوني الرئيسي الذي ينظم عمل مزودي خدمات التصديق الإلكتروني في مصر، ويحدد ضوابط تقديم الخدمة والتزامات مقدم الخدمة،[1] من المسؤوليات الأساسية لمزودي خدمات التصديق الإلكتروني في مصر التأكد من هوية المستخدمين قبل إصدار الشهادات الرقمية، قانون التوقيع الإلكتروني يفرض إجراءات تحقق صارمة للتأكد من الهوية لضمان موثوقية وأمن المعاملات.

يتحمل مزودو خدمات التصديق الإلكتروني في مصر المسؤولية القانونية عن أي أضرار ناتجة عن أخطاء في إصدار الشهادات أو الإخفاق في حماية البيانات، وذلك وفقًا لقانون التوقيع الإلكتروني والقوانين المدنية.

الفرع الثاني: مسؤولية مزودي خدمة التصديق الالكتروني وفقا لتشريع الجزائري

القانون الأساسي الذي ينظم خدمات التصديق الإلكتروني في الجزائر هو القانون رقم 04/15 لسنة 2015 المتعلق بالتوقيع والتصديق الإلكتروني، والذي يحدد الضوابط العامة لتقديم الخدمات الإلكترونية وأدوار ومسؤوليات مقدمي الخدمات.

القانون الجزائري رقم 04/15 الصادر في 1 فبراير 2015 يتعامل مع التوقيعات الإلكترونية وخدمات الثقة بشكل شامل، بحيث ينص القانون في إطار المادة 53 منه على أن مزود الخدمة يتحمل مسؤولية التحقق من دقة وصحة البيانات المقدمة عند إصدار الشهادات الإلكترونية، إضافة إلى ذلك، يحدد القانون مجموعة من الإجراءات لضمان أمان التوقيعات وحماية المستخدمين من أي عمليات احتيال محتملة، إذ تعرضت إحدى الجهات الحكومية لخسائر مالية بسبب استخدام شهادة توقيع إلكتروني غير موثوق بها صادرة عن مزود لم يلتزم بالتحقق الكافي من هوية المستخدمين، مما أدى إلى دخول جهات غير مرخصة إلى أنظمة الإدارة المالية.

[1] محمد كمال السيد، حماية البيانات الشخصية في التشريع المصري، المركز المصري للدراسات القانونية، مصر، 2021، ص 80.

بالرجوع الى نص المادة 13 نجد أن مؤدي خدمات التصديق الإلكتروني مسؤولين عن الأضرار التي تلحق بالشخص الذي يتعاقد معه سواء كان طبيعيا أو معنويا، أو اتجاه أي شخص اعتمد بصورة معقولة على الشهادة التي أصدرتها، وذلك في حالة توافر إحدى الحالات المنصوص عليها.

فالمشرع الجزائري حدد بدقة حالات مسؤولية مؤدي خدمات التصديق الإلكتروني عند إصداره لشهادة إلكترونية موصوفة في المادة 53 الفقرات 1-2-3 من القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين، وهذه الحالات هي[1]:

- التأكد من صحة جميع المعلومات الواردة في شهادة التصديق الالكتروني الموصوفة في التاريخ الذي منحت فيه، ووجود جميع البيانات الواجب توفرها في شهادة التصديق الالكتروني الموصوفة ضمن هذه الشهادة؛
- التأكد من منح شهادة التصديق الإلكتروني أن الموقع الذي تم تحديد هويته في شهادة التصديق الإلكتروني الموصوفة يحوز كل بيانات إنشاء التوقيع الموافقة لبيانات التحقق من التوقيع المقدم و/أو المحددة في شهادة التصديق الإلكتروني؛
- التأكد من إمكانية استعمال بيانات إنشاء التوقيع والتحقق منه بصفة متكاملة.

يتبين أن المشرع الجزائري من خلال هذه المادة قد مكّن مؤدي خدمات التصديق الإلكتروني من نفي مسؤوليته متى قام بإثبات أنه قام بواجبه دون أي إهمال.

أما المادة 54 من القانون رقم 04/15 فقد نصت على أنه يكون مؤدي خدمات التصديق الإلكتروني الذي سلم شهادة تصديق إلكتروني موصوفة مسؤولا عن الضرر الناتج عن عدم إلغاء شهادة التصديق الإلكتروني هذه والذي يلحق بأي هيئة أو شخص طبيعي أو معنوي اعتمدوا على تلك الشهادة إلا إذا قدّم مؤدي خدمات التصديق الإلكتروني ما يثبت أنه لم يرتكب أي إهمال.

ما يلاحظ على هذه المادة أن المشرع الجزائري أقر بمسؤولية مؤدي خدمات التصديق الإلكتروني في حالة حصول ضرر لكل شخص طبيعي أو معنوي نتيجة عدم إلغاء شهادة التصديق الإلكترونية، ويكون إلغاء الشهادة وفقا لمقتضيات المادة 45 من القانون 04/15 المتعلق بالتوقيع والتصديق

[1] المادة 53 الفقرة 1-2-3 من القانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين.

الإلكترونين على أنه يلغي مؤدي خدمات التصديق الإلكتروني أيضا شهادة التصديق الإلكتروني الموصوفة عندما يتبين:

- أنه قد تم منحها بناء على معلومات خاطئة أو مزورة، أو إذا أصبحت المعلومات الواردة في شهادة التصديق الإلكتروني غير مطابقة، أو إذا تم انتهاك سرية ببيانات إنشاء التوقيع؛
- أنها لم تصبح مطابقة لسياسة التصديق؛
- أنه تم إعلام مؤدي خدمات التصديق الإلكتروني بوفاة الشخص الطبيعي، أو بحل الشخص المعنوي صاحب شهادة التصديق الإلكتروني[1].

يلاحظ من خلال المادة 54 من القانون 04/15 أنها تشدد على ضرورة توفير الضمانات المالية والتعويض للأطراف المتضررة نتيجة الإهمال أو الخطأ من قبل مزودي خدمات التصديق، بما يضمن حماية حقوق المستخدمين والمصداقية في البيئة الرقمية.

[1] زهيرة عبوب، مرجع سابق، ص 436.

المحور الرابع:

التحديات المستقبلية وتطور المعاملات الالكترونية

مع التقدم السريع للتكنولوجيا في العصر الرقمي، أصبحت المعاملات الإلكترونية جزءًا أساسيًا من الحياة اليومية، سواء على المستوى الفردي أو المؤسساتي، ومع ذلك، يواجه هذا المجال تحديات متزايدة تتعلق بالتنظيم القانوني والتقني، حيث يجد المشرعون صعوبة في مواكبة التطورات التقنية المتسارعة التي تُعيد تشكيل البنية الاقتصادية والاجتماعية، تشمل هذه التحديات إيجاد التوازن بين حرية الابتكار وضمان حقوق المستخدمين وأمن البيانات، فضلاً عن الحاجة إلى تطوير قوانين أكثر مرونة تستجيب للتغيرات المستمرة في الفضاء الرقمي.

إلى جانب التحديات التقنية مثل الأمن السيبراني، والخصوصية، والتعامل مع الذكاء الاصطناعي، تظهر أيضًا الحاجة الملحة لتكييف التشريعات الحالية مع الواقع الجديد للمعاملات الإلكترونية، بحيث من المتوقع أن تشهد السنوات المقبلة تعديلات قانونية تهدف إلى تعزيز الأمن والثقة في العمليات الرقمية، بالإضافة إلى تقديم حلول تشريعية مرنة لمواكبة التطور السريع للتقنيات، كما تعد الاستجابة الفعالة لهذه التحديات ضرورية لضمان بيئة قانونية وتشغيلية تعزز الثقة بين جميع الأطراف وتدعم استدامة وتطور الاقتصاد الرقمي.

وعليه سوف نتعرض في البداية إلى أهم التحديات القانونية والتقنية في ظل التطورات السريعة للتكنولوجيا (المبحث الأول)، ثم نحاول الوصول إلى أهم التوقعات المستقبلية ومقترحات التعديلات التي يمكن اعتمادها في مختلف القوانين الحالية (المبحث الثاني).

المبحث الأول: التحديات القانونية والتقنية في ظل التطورات السريعة للتكنولوجيا

في ظل التطور التكنولوجي السريع، أصبحت المعاملات الإلكترونية جزءاً لا يتجزأ من الحياة اليومية، حيث ساهمت هذه التقنية في تبسيط وتسريع الإجراءات المالية والتجارية عبر الإنترنت. من الخدمات المصرفية إلى التجارة الإلكترونية، أصبحت المعاملات الإلكترونية أداة ضرورية لتحقيق النمو الاقتصادي وتوفير الوقت والجهد للمستخدمين. لكن مع هذه الفوائد، يظهر جانب آخر يتطلب عناية خاصة، وهو التعامل مع الجوانب القانونية والتنظيمية لضمان أمان وسلامة هذه المعاملات.

التحديات القانونية والتقنية في هذا المجال تتعلق بشكل أساسي بحماية البيانات الشخصية، وضمان الأمان السيبراني، ووضع تشريعات تنظم التجارة الرقمية وتمنع الاحتيال. كما أن التطورات السريعة تفرض على الحكومات والمؤسسات تحديث قوانينها بصفة مستمرة لضمان استجابة ملائمة لمتطلبات التكنولوجيا الحديثة وضمان توازن بين الابتكار والأمان، مما يعزز الثقة لدى المستخدمين ويضمن استدامة هذا التحول الرقمي.

المطلب الأول: التحديات القانونية للمعاملات الالكترونية في ظل التطورات السريعة للتكنولوجيا

مع التطورات السريعة التي تشهدها التكنولوجيا، أصبحت المعاملات الإلكترونية جزءًا لا يتجزأ من حياتنا اليومية، حيث تسهل الوصول إلى الخدمات المالية والتجارية بطرق أكثر كفاءة وسرعة. من خلال الأجهزة المحمولة والتطبيقات الذكية، يتم إجراء العديد من المعاملات بكبسة زر واحدة، مما يجعل العمليات أسهل وأقل تعقيدًا من ذي قبل. ومع ذلك، فإن هذا التحول الرقمي الضخم يطرح تحديات قانونية لا يمكن تجاهلها، خاصة مع تطور وتزايد الجرائم الإلكترونية وأساليب الاحتيال الرقمي.

التحديات القانونية المتعلقة بالمعاملات الإلكترونية تشمل جوانب مثل حماية البيانات الشخصية، تحديد المسؤوليات القانونية بين الأطراف المختلفة، والتعامل مع الأنشطة الاحتيالية المتزايدة في البيئة الرقمية. كما تتطلب هذه التطورات إصدار تشريعات حديثة قادرة على مواكبة التحولات السريعة، ووضع أطر قانونية تضمن حقوق المستخدمين وتحميهم من المخاطر المحتملة. تعد معالجة هذه التحديات أمرًا ضروريًا لضمان بيئة معاملات إلكترونية آمنة تُعزز من ثقة الأفراد والشركات في استخدام التكنولوجيا.

الفرع الأول: التحديات المتعلقة بحماية البيانات الشخصية

مع تزايد استخدام المعاملات الإلكترونية في حياتنا اليومية، أصبحت حماية البيانات الشخصية تحديًا معقدًا يعاني من ضعف الضمانات القانونية الحالية، التي غالبًا ما تعجز عن توفير حماية كافية للمستخدمين. فالقوانين والتشريعات القائمة لا تواكب سرعة التطور التكنولوجي، مما يفتح المجال أمام العديد من الشركات لاستغلال البيانات الشخصية لأغراض تجارية دون موافقة واضحة من الأفراد. هذا الاستغلال يثير القلق بشأن خصوصية المستخدمين واستخدام بياناتهم بشكل يتعدى نطاق الفائدة الشخصية إلى تحقيق أرباح تجارية، الأمر الذي يتطلب تطوير سياسات قانونية أكثر قوة وتطبيق آليات فعّالة لحماية خصوصية الأفراد في العالم الرقمي.

أولا: عدم كفاية القوانين التقليدية لحماية البيانات في البيئة الرقمية

مع تطور البيئة الرقمية بوتيرة متسارعة، أصبح واضحًا أن القوانين التقليدية لحماية البيانات لم تعد تلبي المتطلبات الحالية، حيث تتطلب هذه البيئة الرقمية آليات حماية تتسم بالمرونة لمواجهة التحديات الجديدة، لكن القوانين التقليدية لا تزال غير قادرة على مواكبة هذا التغير السريع.

1/- التطورات التكنولوجية وتأثيرها على البيانات الشخصية

أصبحت البيانات الشخصية تُجمع من خلال مختلف المنصات الرقمية ووسائل التواصل الاجتماعي بغرض الإعلانات المستهدفة أو حتى التلاعب السياسي، فالتكنولوجيا الحديثة مثل الذكاء الاصطناعي وتحليل البيانات الضخمة أصبحت تتطلب جمع كميات هائلة من البيانات، مما يضع القوانين التقليدية في موقف صعب.

ويمكن أن نوضح في هذا المجال وجود مجموعة من الدراسات نذكر على سبيل المثال تلك الدراسة التي أنجزها الدكتور أحمد عبد الحميد من جامعة القاهرة بحيث أشار في دراسة سابقة له إلى أن التشريعات التقليدية لا تحتوي على بروتوكولات تتناسب مع النمو المتزايد لتقنيات الذكاء الاصطناعي واستخداماتها في البيئة الرقمية[1].

[1] أحمد عبد الحميد، التحديات القانونية للذكاء الاصطناعي في البيئة الرقمية، جامعة القاهرة، مصر،2021، ص 25.

2/- القوانين التقليدية وعجزها عن مواكبة التغيرات الرقمية

القوانين القديمة، مثل قوانين حماية البيانات التي وضعتها العديد من الدول العربية في الثمانينات والتسعينات، لم تكن مجهزة للتعامل مع التحديات الحديثة مثل الإنترنت ووسائل التواصل الاجتماعي.

إن أغلب التشريعات المتعلقة بحماية البيانات في العالم العربي لم تُحدث لتتواكب مع التطورات الرقمية، حيث أن هذه التشريعات غالبًا ما تعتمد على البنية القديمة في حماية البيانات[1].

3/- التحديات الأمنية الجديدة والتعقيدات القانونية

من أكبر التحديات الأمنية الحالية هي الهجمات السيبرانية وتسريب البيانات. حسب تقرير من الاتحاد العربي للأمن السيبراني(2022)[2] فإن التشريعات القديمة لا توفر آليات كافية للتعامل مع التهديدات السيبرانية الحديثة، كما أن هناك نقصًا في القوانين الرادعة التي تحمي البيانات الشخصية بشكل فعال، هذا الأمر يُظهر ضرورة العمل على تطوير إطار قانوني محدث يستطيع مواجهة التهديدات المتزايدة في البيئة الرقمية ويضمن حماية حقوق الأفراد.

4/- قوانين جديدة وممارسات مبتكرة

ظهرت بعض المحاولات لتحديث القوانين العربية، حيث اعتمدت المملكة العربية السعودية مؤخرًا قوانين تتعلق بحماية البيانات الشخصية مستوحاة من النظام الأوروبي العام لحماية البيانات (GDPR) كما أن دولة الإمارات العربية المتحدة طورت إطارًا قانونيًا أكثر شمولًا لحماية البيانات الشخصية، لكنه لا يزال يواجه تحديات تتعلق بالتطبيق الفعلي.

إن التشريعات الجديدة تمثل خطوة هامة، لكنها تواجه تحديات متعلقة بالتنفيذ على مستوى الشركات الكبرى والمنصات الرقمية العالمية[3].

---

[1] المركز العربي للأبحاث ودراسة السياسات، حماية البيانات الشخصية في العالم العربي: الواقع والتحديات، المركز العربي للأبحاث، قطر، 2019، ص 44.

[2] الاتحاد العربي للأمن السيبراني، "تقرير الأمن السيبراني العالمي، الاتحاد العربي للأمن السيبراني، المملكة العربية السعودية، 2022، ص 63.

[3] محمد الكعبي، التحديات القانونية لحماية البيانات في العالم العربي، مجلة القانون الرقمي، الإمارات العربية المتحدة، 2020، ص 17.

ثانيا: اختلاف مستوى الحماية القانونية بين الدول وصعوبة تطبيق قوانين موحدة

تختلف التشريعات المتعلقة بالمعاملات الإلكترونية من دولة إلى أخرى بناءً على السياقات القانونية والاقتصادية لكل بلد، فالدول المتقدمة غالبًا ما تكون لديها قوانين قوية لحماية المستهلك والمعاملات الإلكترونية، بينما تواجه الدول النامية تحديات تتعلق بالبنية التحتية القانونية وغياب اللوائح الواضحة، بحيث تشير إلى أن الدول العربية تختلف بشكل ملحوظ في مستويات حماية المعاملات الإلكترونية، حيث أن بعض الدول مثل الإمارات العربية المتحدة والسعودية طورت أنظمة متقدمة، بينما لا تزال دول أخرى تعاني من نقص في التشريعات الملائمة.

كما أن الاختلاف في القوانين المحلية يخلق صعوبات في التجارة الإلكترونية الدولية، بحيث عند إجراء معاملات عبر الحدود، تواجه الشركات تحديات في الامتثال للمتطلبات المختلفة في كل بلد. هذا يجعل من الصعب تحقيق الحماية الكافية للمستهلكين.

يواجه التجار الدوليون صعوبة في التكيف مع التشريعات المتباينة للمعاملات الإلكترونية بين الدول، بحيث أشار تقرير منظمة التجارة العالمية إلى أن غياب التوحيد القانوني يعيق نمو التجارة الإلكترونية عبر الحدود ويزيد من تكاليف الامتثال[1].

إضافة إلى ذلك فإن محاولة توحيد القوانين المتعلقة بالمعاملات الإلكترونية على المستوى الدولي تواجه تحديات عديدة، إذ تختلف الدول في رؤيتها لحماية البيانات، مستوى الشفافية، وأدوار الجهات المعنية في حماية حقوق المستهلكين، بعض الدول تركز على حماية خصوصية البيانات بشكل صارم مثل الاتحاد الأوروبي من خلال القانون العام لحماية البيانات(GDPR) ، في حين تركز دول أخرى على تعزيز التجارة وزيادة سهولة إجراء المعاملات.

إن محاولة تطبيق قوانين موحدة تواجه تحديات ثقافية وسياسية، حيث تختلف أولويات الحكومات من حيث حماية المستهلك مقابل تعزيز التجارة، هذه التباينات تجعل من الصعب إيجاد حل قانوني موحد.

[1] منظمة التجارة العالمية، (WTO) تحديات التجارة الإلكترونية عبر الحدود، منظمة التجارة العالمية، جنيف، 2020، ص 45.

الفرع الثاني: التحديات المتعلقة بالمسؤولية القانونية والجرائم الإلكترونية

مع تزايد الاعتماد على التكنولوجيا في الحياة اليومية، أصبحت المعاملات الإلكترونية جزءاً أساسياً من الأنشطة الاقتصادية والاجتماعية. إلا أن هذا التطور صاحبه العديد من التحديات المتعلقة بالمسؤولية القانونية وحماية المستخدمين من الجرائم الإلكترونية. من أبرز هذه التحديات استخدام البيانات الشخصية دون موافقة المستخدمين لأغراض الدعاية والتسويق، مما يشكل انتهاكاً للخصوصية وخرقاً للقوانين التي تهدف لحمايتها. بالإضافة إلى ذلك، تزداد احتمالية تعرض هذه البيانات للاختراق أو السرقة، مما يثير القلق بشأن قدرة الجهات المختصة على حماية الحقوق الرقمية وضمان الأمان السيبراني. هذه القضايا تتطلب تطوير سياسات وإجراءات أكثر صرامة لضمان سلامة المعلومات وحقوق الأفراد.

أولا: استخدام البيانات الشخصية دون موافقة المستخدمين لأغراض الدعاية والتسويق

استخدام البيانات الشخصية دون موافقة المستخدمين يثير العديد من المخاطر والتأثيرات السلبية، من بينها انتهاك الخصوصية، فقدان الثقة بين المستخدمين والشركات، بالإضافة إلى استغلال البيانات في التلاعب السياسي والتجاري. هذه الممارسات يمكن أن تؤدي إلى شعور المستخدمين بعدم الأمان والخصوصية، مما يؤثر على تجربة استخدام الإنترنت بشكل عام.

تمتد التأثيرات السلبية إلى إمكانية التلاعب بسلوك المستهلكين والسيطرة على اختياراتهم من خلال الإعلانات الموجهة، والتي تعتمد على تحليل البيانات الشخصية التي لم يتم الحصول عليها بموافقة صريحة[1].

الدول النامية تواجه تحديات كبيرة في تنظيم استخدام البيانات الشخصية. يظل الإطار القانوني في هذه الدول ضعيفًا أو غير مكتمل، مما يجعل المستخدمين عرضةً لاستخدام بياناتهم دون موافقتهم. تفتقر العديد من هذه الدول إلى تشريعات حديثة تعالج خصوصية البيانات أو تضع قيودًا واضحة على الشركات التي تجمع البيانات لأغراض الدعاية والتسويق.

[1] محمد الكعبي، استخدام البيانات الشخصية والإعلانات الموجهة، مجلة القانون الرقمي، الإمارات العربية المتحدة، 2021، ص 18.

بحسب تقرير من المركز العربي للأبحاث ودراسة السياسات، فإن بعض الدول العربية بدأت في تطوير قوانين لحماية البيانات، لكن مستوى الحماية لا يزال متدنيًا مقارنةً بالمعايير الدولية، وهناك فجوة في التنفيذ بسبب نقص الخبرات والتوعية بين المواطنين حول حقوقهم[1].

ثانيا: زيادة احتمالية تعرض البيانات للاختراق أو السرقة

في السنوات الأخيرة، ارتفع معدل الهجمات السيبرانية بشكل كبير، مما زاد من احتمالية تعرض بيانات العملاء للاختراق، يستهدف المهاجمون منصات التجارة الإلكترونية بشكل متزايد نظرًا لما تحتويه من بيانات شخصية ومالية قيمة.

وفقًا لتقرير الاتحاد العربي للأمن السيبراني(2021) ، فإن منصات التجارة الإلكترونية العربية شهدت زيادة ملحوظة في عدد الهجمات الإلكترونية، التي كانت تهدف بشكل أساسي إلى سرقة البيانات المالية للمستخدمين. ويرجع ذلك إلى نقص تدابير الحماية في العديد من المواقع، بالإضافة إلى ضعف التوعية بمخاطر الأمان السيبراني بين أصحاب الشركات الصغيرة[2].

كما أن العديد من منصات التجارة الإلكترونية، خاصة الصغيرة منها، لا تتبع أفضل الممارسات الأمنية، مما يجعلها أهدافًا سهلة للاختراق، التحول الرقمي السريع في ظل جائحة COVID-19 أدى إلى زيادة عدد المواقع الإلكترونية دون تزويدها بحلول أمنية قوية.

إضافة إلى ذلك فإن هجمات الفدية أصبحت شائعة بشكل خاص في مجال التجارة الإلكترونية، حيث يتم تشفير بيانات الشركات ومن ثم طلب فدية لفك التشفير، هذا النوع من الهجمات يضع البيانات المالية والشخصية للعملاء في خطر شديد.

إن ضعف التوعية بأهمية الأمن السيبراني لدى المستخدمين في الدول النامية يسهم بشكل كبير في زيادة الهجمات السيبرانية على منصات التجارة الإلكترونية.

---

[1] المركز العربي للأبحاث ودراسة السياسات، حماية البيانات الشخصية في الدول العربية: التحديات والفرص، المركز العربي للأبحاث، قطر، 2020، ص 42.

[2] الاتحاد العربي للأمن السيبراني، تقرير الهجمات السيبرانية على التجارة الإلكترونية، الاتحاد العربي للأمن السيبراني، المملكة العربية السعودية، 2021، ص 33.

المطلب الثاني: التحديات التقنية للمعاملات الالكترونية في ظل التطورات السريعة للتكنولوجيا

تشهد المعاملات الإلكترونية نموًا ملحوظًا نتيجة التطورات السريعة في التكنولوجيا، إلا أن هذا النمو صاحبه تحديات تقنية تعرقل استخدام هذه المعاملات بشكل آمن وفعال، تتعلق هذه التحديات بالأمان، البنية التحتية، التوافق مع الأنظمة القديمة، وإمكانية الوصول إلى التقنيات المتقدمة.

الفرع الأول: التحديات الأمنية في المعاملات الإلكترونية

الأمان يعد من أكبر التحديات التي تواجه المعاملات الإلكترونية. التطور السريع في الهجمات السيبرانية، مثل البرمجيات الخبيثة وهجمات الفدية، يجعل من الضروري على منصات المعاملات الإلكترونية تحسين أنظمتها الأمنية بشكل مستمر، بحيث أصبحت الهجمات السيبرانية تتطور بسرعة هائلة، مما يجعل الحلول التقليدية للحماية غير كافية.

التكنولوجيا تتغير بسرعة، ومعها تتطور أنظمة المعاملات الإلكترونية، إلا أن هذا التطور يقابله تحديات تتعلق بالتوافق مع الأنظمة القديمة المستخدمة في العديد من المؤسسات هذه الأنظمة غالبًا ما تكون بطيئة في التكيف مع التطورات الحديثة، مما يعقد العمليات ويجعل من الصعب تطبيق الحلول الجديدة، وهو الأمر الذي أشار إليه تقرير المركز العربي للأبحاث ودراسة السياسات بأن الأنظمة القديمة التي ما زالت تعتمدها بعض المؤسسات الحكومية والخاصة تمثل عقبة كبيرة في تطوير نظم المعاملات الإلكترونية الحديثة[1].

كما أن البنية التحتية التكنولوجية تلعب دورًا حاسمًا في تعزيز أو تقييد قدرة المنصات على تنفيذ المعاملات الإلكترونية بشكل فعال، ففي العديد من الدول النامية، البنية التحتية للشبكات ضعيفة، مما يسبب بطء في سرعة المعاملات وارتفاع معدل الانقطاعات.

[1] المركز العربي للأبحاث ودراسة السياسات، تحديات التوافق في الأنظمة القديمة مع التكنولوجيا الحديثة، المركز العربي للأبحاث، قطر، 2021، ص 27.

الفرع الثاني: التحديات المتعلقة بالتفاوت في التقنية

تشهد المعاملات الإلكترونية نموًا ملحوظًا نتيجة التطورات السريعة في التكنولوجيا، إلا أن هذا النمو صاحبه تحديات تقنية تعرقل استخدام هذه المعاملات بشكل آمن وفعال، وتتعلق هذه التحديات بالأمان، البنية التحتية، التوافق مع الأنظمة القديمة، وإمكانية الوصول إلى التقنيات المتقدمة.

التطور السريع في التكنولوجيا قد يكون مفيدًا للكثيرين، ولكنه يُشكل تحديًا للمستخدمين الذين لا يتمتعون بإمكانية الوصول إلى التكنولوجيا الحديثة، مثل الهواتف الذكية المتطورة أو الإنترنت عالي السرعة، هذا التفاوت في إمكانية الوصول يخلق فجوة رقمية بين المستخدمين، مما يؤثر على العدالة في استخدام المعاملات الإلكترونية.

إن التفاوت في إمكانية الوصول إلى التكنولوجيا يعيق العديد من الأفراد من المشاركة الفعالة في الأنشطة التجارية الإلكترونية حيث أن هذه الفجوة تحتاج إلى معالجة سريعة من خلال سياسات تعزز من الوصول العادل للتكنولوجيا في المجتمعات النامية[1].

التطور السريع للتكنولوجيا قد يتجاوز أحيانًا التشريعات القائمة، مما يؤدي إلى صعوبات في الامتثال للوائح القانونية المتعلقة بالمعاملات الإلكترونية، فالتشريعات لا تواكب دائمًا التغيرات التكنولوجية، مما يخلق فجوات قانونية يمكن أن تؤثر على الأمان والثقة في الأنظمة الإلكترونية.

تقرير الأمم المتحدة للتجارة والتنمية (UNCTAD) أوضح أن العديد من الدول النامية تفتقر إلى إطار قانوني متكامل ينظم المعاملات الإلكترونية، مما يعرض المستخدمين لمخاطر قانونية وأمنية، التقرير شدد على ضرورة تحديث القوانين لتواكب التطورات التكنولوجية السريعة وتضمن حماية المستهلكين بشكل فعال[2].

[1] عبد الحميد، أحمد، التفاوت في الوصول إلى التكنولوجيا وتأثيره على المعاملات الإلكترونية، جامعة القاهرة، مصر، 2021، ص 33.

[2] الامتثال والتشريعات في المعاملات الإلكترونية، الأمم المتحدة للتجارة والتنمية UNCTAD، جنيف، 2022، ص 48.

المبحث الثاني: التوقعات المستقبلية والتعديلات المتوقعة في القوانين الحالية

التوقعات المستقبلية والتعديلات المتوقعة في القوانين الحالية تُعبر عن استجابة المجتمعات لمواجهة التحديات المتغيرة وتلبية احتياجات الأفراد والمؤسسات، مع التطورات السريعة في التكنولوجيا والاقتصاد العالمي، أصبحت الدول مجبرة على مراجعة تشريعاتها وتعديلها بشكل مستمر للحفاظ على توازنها القانوني والاجتماعي، مثل هذه التعديلات تُسهم في تعزيز الاستدامة الاقتصادية والعدالة الاجتماعية، وتساعد في تكييف الإطار القانوني مع المتطلبات المستجدة للمجتمع.

يُعد تحسين القوانين الحالية عنصرًا أساسيًا لضمان الأمن القانوني وتحفيز النمو والتنمية. التعديلات المستقبلية تهدف إلى معالجة نقاط الضعف الحالية والتأقلم مع التغيرات في البيئة العالمية مثل التحولات الرقمية والمناخية، إضافةً إلى التحولات الاجتماعية والسياسية. بالتالي، فإن التوقعات المستقبلية للتشريعات تعكس الاتجاه نحو قوانين أكثر مرونة وشفافية، تسعى إلى تحقيق توازن بين حماية الحقوق الفردية وتشجيع الابتكار والنمو المستدام.

المطلب الأول: التوقعات المستقبلية للقوانين في مجال المعاملات الالكترونية

مع التطور السريع للتكنولوجيا وزيادة استخدام المعاملات الإلكترونية في الحياة اليومية، أصبحت الحاجة لتطوير القوانين المنظمة لهذا المجال أمرًا لا مفر منه، التكنولوجيا الرقمية لم تعد مجرد أدوات مساعدة بل أصبحت أساسًا لكثير من الأنشطة الاقتصادية والاجتماعية، هذا الواقع الجديد يتطلب قوانين حديثة تحكم هذه المعاملات، وتضمن حقوق المستخدمين، وتوفر بيئة آمنة وموثوقة للتجارة الإلكترونية والخدمات الرقمية.

توقعات المستقبل في مجال القوانين المرتبطة بالمعاملات الإلكترونية تتوجه نحو تعزيز الحماية الرقمية، وزيادة شفافية العمليات، وتنظيم العلاقة بين الأطراف المختلفة بطرق أكثر فعالية، تشمل هذه التعديلات حماية البيانات الشخصية، ومنع الجرائم الإلكترونية، وتحديد المسؤوليات القانونية لكل من المستخدمين ومقدمي الخدمات. يُعد هذا التحديث ضروريًا لضمان التوازن بين التحفيز على الابتكار وضمان الأمان والاستقرار في البيئة الرقمية المتطورة.

تتطور القوانين بمرور الوقت لتلائم التغيرات الاجتماعية، الاقتصادية، والتكنولوجية، ومع التطورات السريعة في مجالات مثل التكنولوجيا الرقمية، التجارة الإلكترونية، والذكاء الاصطناعي، يُتوقع إجراء تعديلات كبيرة على القوانين الحالية لضمان حوكمة فعالة، حماية الخصوصية، وتعزيز الأمن السيبراني.

الفرع الأول: التعديلات المستقبلية في مجال التكنولوجيا الرقمية والتجارة الالكترونية

توجد عدة مبادرات دولية تهدف إلى تقليل الفجوة بين القوانين المتعلقة بالمعاملات الإلكترونية. من أبرز هذه المبادرات، قانون الأمم المتحدة النموذجي للتجارة الإلكترونية، الذي يهدف إلى تقديم إطار مرجعي للدول عند تطوير تشريعاتها الوطنية. ومع ذلك، تواجه هذه المبادرات تحديات في التنفيذ نتيجة للتباين الكبير في الاستجابة والتكيف بين الدول.

وفقًا لتقرير الأمم المتحدة للتجارة والتنمية(UNCTAD) ، فإن الدول النامية تواجه صعوبة في تطبيق هذه القوانين بسبب نقص الموارد والخبرات الفنية، مما يؤدي إلى عدم التكافؤ في مستوى الحماية القانونية بين الدول[1].

هناك عدة مبادرات تسعى إلى تعزيز حماية البيانات الشخصية على مستوى العالم، من هذه المبادرات، قانون خصوصية المستهلك في كاليفورنيا(CCPA) ، الذي يتيح للمستخدمين الحق في معرفة البيانات التي تجمع عنهم والتحكم فيها. هذه المبادرات تضع معايير جديدة يمكن للدول الأخرى اتباعها لتحسين حماية البيانات[2].

إن تطبيق هذه المعايير على نطاق واسع يواجه تحديات، خصوصًا في الدول ذات البنية التحتية القانونية الضعيفة، وهو ما يساهم في تباين مستوى حماية البيانات بين دول العالم.

يمكن التقليل من احتمالية تعرض بيانات المستخدمين للاختراق من خلال تطبيق بروتوكولات الأمان الحديثة مثل التشفير القوي واستخدام المصادقة الثنائية .(Two-Factor Authentication)

[1] تقرير عن التجارة الإلكترونية والتنمية UNCTAD، الأمم المتحدة للتجارة والتنمية، جنيف، 2021، ص 53.

[2] التحديات العالمية في حماية البيانات الشخصيةUNCTAD، الأمم المتحدة للتجارة والتنمية، جنيف، 2021، ص 50.

بالإضافة إلى ذلك، يلزم على الحكومات والمؤسسات زيادة الاستثمار في مجال الأمان السيبراني لضمان حماية بيانات المستخدمين.

على الدول العربية يجب أن تركز على تطوير سياسات وتشريعات تفرض على منصات التجارة الإلكترونية تطبيق معايير الأمن السيبراني، كما أن تطبيق هذه السياسات سيسهم في تقليل معدلات الهجمات السيبرانية بشكل كبير[1].

من بين الحلول المقترحة للتغلب على هذه التحديات:

- **تحسين البنية التحتية الأمنية** :من خلال تطبيق أحدث تقنيات التشفير وتحديث الأنظمة بشكل مستمر.
- **تحديث الأنظمة القديمة** :استثمار الشركات والمؤسسات في تحديث أنظمتها لتتوافق مع التطورات الحديثة.
- **تعزيز البنية التحتية للشبكات** :من خلال زيادة الاستثمارات في تحسين الشبكات، خاصة في المناطق النامية.
- **سد الفجوة الرقمية** :عبر تقديم برامج تعليمية ودعم تقني للأفراد غير القادرين على الوصول إلى التكنولوجيا الحديثة.

الواقع المعزز والواقع الافتراضي سيلعبان دورًا متزايدًا في التجارة الإلكترونية، حيث ستتمكن الشركات من تقديم تجارب تسوق افتراضية تتيح للمستخدمين معاينة المنتجات بشكل ثلاثي الأبعاد قبل الشراء، فتقرير شركة برايس ووترهاوس كوبرز (PwC) لعام 2022 أوضح أن تقنيات الواقع الافتراضي ستصبح جزءًا لا يتجزأ من تجربة التسوق الإلكترونية، مما يساعد على تحسين تجربة العميل وزيادة التفاعل مع المنتجات. التقرير أشار إلى أن هذه التعديلات التكنولوجية ستتطلب أيضًا تعديلات في السياسات المتعلقة بحماية البيانات وضمان حقوق الملكية الفكرية للأصول الرقمية[2].

[1] أحمد عبد الحميد، مرجع سابق، ص 38.

[2] الواقع المعزز والافتراضي في التجارة الإلكترونية PwC، برايس ووترهاوس كوبرز، الولايات المتحدة، 2022، ص34.

مع هذه التطورات التكنولوجية السريعة، من المتوقع أن يتم إجراء تعديلات على اللوائح والقوانين لتنظيم التجارة الإلكترونية بشكل أفضل، هذه التعديلات ستشمل قوانين حماية البيانات وخصوصية المستخدمين، لضمان الامتثال للتغيرات الجديدة في الأنظمة الرقمية.

إن الدول ستكون مجبرة على تحديث قوانينها التجارية والقانونية لمواكبة التغيرات في أنظمة التجارة الإلكترونية، خاصة فيما يتعلق بالتحقق من هوية العملاء وحماية البيانات، وهذا ما يتطلب تنسيقًا بين الدول لتفادي التباين في القوانين الذي قد يؤثر سلبًا على التجارة الدولية.

الفرع الثاني: التعديلات المستقبلية في مجال الذكاء الاصطناعي

مع التقدم السريع في تقنيات الذكاء الاصطناعي، أصبح استخدام هذه التقنيات في المعاملات الإلكترونية جزءًا أساسيًا من التجارة الرقمية. من تحسين تجربة المستخدم إلى تعزيز الأمان وتحليل البيانات، يتزايد الاعتماد على الذكاء الاصطناعي في هذا المجال. يهدف هذا البحث إلى دراسة التعديلات المستقبلية المتوقعة على استخدام الذكاء الاصطناعي في المعاملات الإلكترونية، وتسليط الضوء على القضايا القانونية والأخلاقية المرتبطة بها.

أولا: تحسين تجربة المستخدم باستخدام الذكاء الاصطناعي

أحد أبرز التعديلات المستقبلية في مجال المعاملات الإلكترونية هو استخدام الذكاء الاصطناعي لتحسين تجربة المستخدم من خلال تقديم توصيات مخصصة وتحليل سلوكيات العملاء، يُتوقع أن تصبح هذه التحسينات أكثر دقة وفعالية مع تطور تقنيات التعلم العميق.

إن التعديلات المستقبلية ستشمل تحسين خوارزميات التوصيات بشكل يجعل تجربة المستخدم أكثر سلاسة وتوافقًا مع احتياجاته الفردية، كما أن هذه التقنيات ستسمح للشركات بتقديم خدمات مخصصة لكل عميل، مما يعزز من الولاء للعلامة التجارية وزيادة معدلات التحويل[1].

ثانيا: الذكاء الاصطناعي في دعم العملاء والروبوتات الذكية

التعديلات المستقبلية في مجال دعم العملاء تتجه نحو استخدام روبوتات المحادثة الذكية (Chatbots)التي تعتمد على الذكاء الاصطناعي للتفاعل مع العملاء والإجابة على استفساراتهم، هذه التقنية من المتوقع أن تُحسن من كفاءة خدمة العملاء وتقلل من الوقت المستغرق لحل المشاكل.

[1] محمد الكعبي، مرجع سابق، ص 22.

تقرير صادر عن شركة ماكنزي (McKinsey) لعام 2023 يشير إلى أن استخدام روبوتات المحادثة الذكية في المعاملات الإلكترونية سيتضاعف خلال السنوات القليلة القادمة، حيث ستكون هذه الأنظمة قادرة على التعلم من التفاعلات السابقة لتحسين مستوى الاستجابة والقدرة على تقديم إجابات دقيقة وسريعة. كما أشار التقرير إلى أن هذه التعديلات ستسهم في تقليل تكاليف التشغيل وتحسين رضا العملاء[1].

ثالثا: الأمان السيبراني باستخدام الذكاء الاصطناعي

من المتوقع أن يلعب الذكاء الاصطناعي دورًا حاسمًا في تعزيز الأمان السيبراني في المعاملات الإلكترونية. تقنيات الذكاء الاصطناعي قادرة على اكتشاف التهديدات بسرعة وتحليل الأنماط غير العادية في البيانات، مما يمكن الشركات من منع الهجمات السيبرانية قبل حدوثها.

إن استخدام الذكاء الاصطناعي في تعزيز الأمان السيبراني أصبح ضرورة في ظل تزايد الهجمات على منصات التجارة الإلكترونية، كما أن التعديلات المستقبلية ستشمل تطبيقات التعلم الآلي لمراقبة الشبكات واكتشاف التهديدات السيبرانية بفاعلية أكبر، مما يساعد على تقليل الخسائر الناجمة عن الاحتيالات والهجمات.

رابعا: التحديات القانونية والأخلاقية المرتبطة بالذكاء الاصطناعي

رغم الفوائد الكبيرة لاستخدام الذكاء الاصطناعي في المعاملات الإلكترونية، هناك تحديات قانونية وأخلاقية يجب التعامل معها. تتعلق هذه التحديات بخصوصية البيانات، المسؤولية القانونية في حالات الخطأ، وأيضًا التحيز الخوارزمي الذي قد يؤثر سلبًا على العملاء.

جامعة كامبريدج نشرت دراسة في عام 2022 توضح أن التعديلات المستقبلية يجب أن تشمل قوانين واضحة تحدد المسؤوليات عند وقوع أخطاء ناجمة عن استخدام الذكاء الاصطناعي في المعاملات الإلكترونية. الدراسة تشير إلى أن عدم وجود إطار قانوني مناسب يضع الشركات في

[1] روبوتات المحادثة الذكية في التجارة الإلكترونية، شركة ماكنزي للاستشارات، McKinsey، الولايات المتحدة، 2023، ص 18.

مواجهة مخاطر قانونية وأخلاقية كبيرة. كما أشارت إلى أن هناك حاجة لآليات تحقق وضبط لضمان عدم وجود تحيزات خوارزمية تؤثر على قرارات الذكاء الاصطناعي[1].

خامسا: الذكاء الاصطناعي وتحليل البيانات في التجارة الإلكترونية

تحليل البيانات يعد جزءًا أساسيًا من التجارة الإلكترونية، واستخدام الذكاء الاصطناعي لتحليل كميات ضخمة من البيانات سيساهم في تحسين استراتيجيات التسويق وزيادة فعالية الإعلانات المستهدفة. من المتوقع أن تزداد دقة التحليلات التنبؤية التي تساعد الشركات على فهم احتياجات العملاء المستقبلية بشكل أفضل.

من المحتمل أن يستخدم الذكاء الاصطناعي بشكل أكبر لتحليل البيانات الضخمة، مما سيمكن الشركات من اتخاذ قرارات أكثر دقة واستنادًا إلى معلومات فعلية، مما يساعد على تعزيز التنافسية وتحقيق مكاسب اقتصادية أكبر، إلا أنها تتطلب أيضًا قوانين صارمة لحماية خصوصية البيانات.

سادسا: تعزيز عمليات الدفع الذكية باستخدام الذكاء الاصطناعي

الذكاء الاصطناعي يمكن أن يسهم في تحسين أنظمة الدفع الإلكتروني من خلال تعزيز الأمان، وتقليل عمليات الاحتيال، وزيادة سهولة الاستخدام. يُتوقع أن يكون هناك تطوير مستمر لنظم الدفع لتكون أكثر ذكاءً وقدرة على تحديد الاحتيال بشكل فوري.

التعديلات المستقبلية في أنظمة الدفع الإلكترونية ستشمل استخدام تقنيات التعلم الآلي للتعرف على الأنماط غير الاعتيادية ومنع العمليات المشبوهة بشكل فوري. وأوضح أن هذا سيسهم في تعزيز ثقة المستخدمين بنظم الدفع الإلكتروني وزيادة الاعتماد عليها[2]، كما تُعد التعديلات المستقبلية في مجال الذكاء الاصطناعي في المعاملات الإلكترونية أمرًا ضروريًا لتعزيز تجربة المستخدم، تحسين الأمان، وتقديم خدمات أكثر دقة وتخصيصًا، يجب أن تتزامن هذه التعديلات مع تطوير الأطر القانونية لضمان الاستخدام الآمن والعادل للذكاء الاصطناعي، وتجنب التحديات الأخلاقية المتعلقة بالخصوصية والتحيز.

---

[1] التحديات القانونية للذكاء الاصطناعي في المعاملات الإلكترونية"، جامعة كامبريدج، المملكة المتحدة، 2022، ص30.

[2] أحمد عبد الحميد، مرجع سابق، ص 24.

المطلب الثاني: التوقعات المستقبلية المتعلقة بالحوكمة الرقمية

في ظل التطورات التكنولوجية المتسارعة، أصبح من الضروري تحقيق حوكمة رقمية فعالة لتنظيم المعاملات الإلكترونية وتعزيز الثقة بين المستخدمين والشركات. تهدف الحوكمة الرقمية إلى وضع معايير وسياسات تنظم العلاقات بين الجهات الفاعلة في البيئة الرقمية، بما يضمن الأمان والشفافية وحماية حقوق المستخدمين. يتناول هذا البحث التوقعات المستقبلية للحوكمة الرقمية في مجال المعاملات الإلكترونية، والتحديات التي تواجه تحقيقها بشكل فعال.

الفرع الأول: تعزيز الشفافية والكفاءة في إدارة المعاملات الرقمية

إحدى الجوانب الرئيسية للحوكمة الرقمية المستقبلية تتعلق بزيادة الشفافية والمساءلة في التعاملات الإلكترونية. من المتوقع أن تتجه الحكومات والشركات إلى استخدام تقنيات مثل سلسلة الكتل (Blockchain) لضمان الشفافية وتسجيل جميع المعاملات بطريقة لا يمكن التلاعب بها.

تقرير منظمة التعاون الاقتصادي والتنمية (OECD) أشار إلى أن الحوكمة الرقمية ستعتمد بشكل متزايد على تقنيات سلسلة الكتل لضمان المساءلة في التعاملات التجارية ومنع الاحتيالات. هذا سيؤدي إلى تعزيز الثقة في الأنظمة الإلكترونية وتحسين الشفافية بين الجهات المعنية، بما في ذلك المستهلكين والشركات[1].

من المتوقع أن تتضمن الحوكمة الرقمية في المستقبل تطوير أطر قانونية وتنظيمية تهدف إلى تحقيق بيئة رقمية آمنة ومنظمة. ستركز هذه الأطر على حماية البيانات، تنظيم العلاقات التجارية، وتوفير ضمانات قانونية للمستهلكين في المعاملات الإلكترونية.

حماية البيانات الشخصية وحقوق الخصوصية هي من أهم القضايا التي ستركز عليها الحوكمة الرقمية في المستقبل، يتوقع أن يتم تطوير قوانين أكثر صرامة تحكم كيفية جمع، تخزين، واستخدام البيانات الشخصية في المعاملات الإلكترونية.

[1] استخدام سلسلة الكتل في تعزيز الشفافية في المعاملات التجارية، منظمة التعاون الاقتصادي والتنمية، OECD، باريس، 2022، ص 22.

كما أن التعاون الدولي سيكون جزءًا أساسيًا من الحوكمة الرقمية في المستقبل، حيث تتطلب التحديات المتزايدة في مجال الأمان السيبراني وحماية البيانات تعاونًا عالميًا لمواجهتها بفعالية. من المتوقع أن تعمل الدول على توحيد معايير الحوكمة الرقمية لضمان تطبيق قوانين موحدة عبر الحدود.

هذا وتتجه الحوكمة الرقمية المستقبلية أيضًا نحو تعزيز الثقة الرقمية، من خلال تطوير آليات لتحسين تجربة المستخدم وضمان الشفافية في جمع واستخدام البيانات. هذه الجهود ستسهم في تعزيز الابتكار الرقمي وتشجيع المزيد من الأفراد والشركات على الدخول إلى الاقتصاد الرقمي.

إن الثقة الرقمية هي حجر الأساس لنجاح المعاملات الإلكترونية في المستقبل، لذلك يجب على الحكومات يجب أن تتبنى سياسات تعزز من ثقة الأفراد في المنصات الرقمية من خلال توفير الشفافية والضمانات القانونية الكافية، مما يسهم في تعزيز الابتكار والنمو الاقتصادي[1].

رغم الفوائد المتوقعة، إلا أن هناك تحديات مستقبلية قد تعرقل تحقيق الحوكمة الرقمية بشكل فعال. من بين هذه التحديات، التباين في البنية التحتية الرقمية بين الدول، وعدم وجود توافق على معايير الحوكمة بين مختلف الحكومات، بالإضافة إلى التهديدات السيبرانية المستمرة.

الفرع الثاني: التعاون بين القطاعين العام والخاص لتحقيق بنية تحتية رقمية آمنة

مع التوسع السريع في المعاملات الإلكترونية، أصبحت البنية التحتية الرقمية أساسًا لضمان الأمن والاستدامة في الاقتصاد الرقمي. التعاون بين القطاعين العام والخاص يعد أحد العناصر الأساسية لتحقيق هذه البنية التحتية الآمنة، حيث يمكن للطرفين العمل معًا لتوفير حلول فعالة للتحديات التكنولوجية وتعزيز الأمن السيبراني.

التعاون بين القطاعين العام والخاص يُعد محوريًا في تعزيز الأمن السيبراني من خلال تبادل المعلومات والتجارب لتحديد الثغرات الأمنية ووضع الحلول الفعالة لها. القطاع الخاص يمتلك التكنولوجيا والخبرة اللازمة، بينما يمتلك القطاع العام القدرة على وضع السياسات التنظيمية المناسبة.

[1] أحمد عبد الحميد، مرجع سابق، ص 32.

فالتعاون بين القطاعين العام والخاص يعد أمرًا بالغ الأهمية لتحقيق البنية التحتية الرقمية الآمنة، حيث يمكن للقطاعين توحيد الجهود لتطوير بروتوكولات أمان قوية، وإنشاء أنظمة استجابة سريعة للتهديدات السيبرانية.

أحد الجوانب المهمة للتعاون بين القطاعين هو تبادل المعلومات المتعلقة بالتهديدات السيبرانية والممارسات الجيدة للتعامل معها، هذه العملية تمكن الأطراف المعنية من التصدي للتهديدات بشكل أسرع وأكثر فعالية، بحيث أن التعاون في مجال الأمن السيبراني يتطلب وجود قنوات تواصل فعالة بين القطاعين العام والخاص لتبادل المعلومات الحساسة والمتعلقة بالتهديدات السيبرانية، مما يؤكد على ضرورة وجود إطار قانوني يشجع الشركات على الإبلاغ عن الحوادث السيبرانية دون التعرض للعقوبات، مما يسهم في تحسين مستوى الأمان الرقمي.

القطاعين العام والخاص يمكن أن يتعاونا في تدريب العاملين على المهارات اللازمة للتعامل مع التهديدات السيبرانية وتحسين مستوى الأمان في البنية التحتية الرقمية. هذه الشراكة يمكن أن تتضمن تنظيم ورش عمل وتدريبات مشتركة لتعزيز جاهزية العاملين على التعامل مع التهديدات المتطورة.

تقرير صادر عن الأمم المتحدة للتجارة والتنمية (UNCTAD) أشار إلى أن الشراكة بين القطاعين العام والخاص يمكن أن تساعد في تعزيز قدرات العاملين في مجال الأمن السيبراني، حيث يوفر القطاع الخاص الخبرات الفنية، بينما يسهم القطاع العام في توفير الدعم التنظيمي واللوجستي. ويؤكد التقرير أن بناء القدرات في مجال الأمن الرقمي يعد ضروريًا للحفاظ على البنية التحتية الرقمية آمنة وفعالة[1].

وعلى الرغم من الفوائد الكبيرة المتوقعة من هذا التعاون، إلا أن هناك تحديات تواجه تحقيق الشراكة المثلى بين القطاعين، من أبرز هذه التحديات هي الفجوة بين الأهداف الربحية للقطاع الخاص والهدف التنظيمي للقطاع العام، بالإضافة إلى نقص الثقة بين الطرفين فيما يتعلق بتبادل المعلومات الحساسة.

[1] تعزيز القدرات في مجال الأمن السيبراني من خلال الشراكة بين القطاعين، الأمم المتحدة للتجارة والتنمية، UNCTAD، جنيف، 2022، ص 35.

ولتعزيز التعاون بين القطاعين العام والخاص في المستقبل، يُتوقع أن تُطوّر الحكومات أطر قانونية وتنظيمية لتشجيع الشراكات بين القطاعين وتوفير حوافز مالية للشركات التي تستثمر في تطوير البنية التحتية الرقمية. كما يجب تعزيز التعاون الدولي لإنشاء معايير مشتركة للأمن السيبراني وتبادل أفضل الممارسات على مستوى العالم.

إن الحكومات يجب أن تعمل على توفير بيئة تنظيمية تدعم الشراكة بين القطاعين من خلال تقديم الحوافز المالية والضريبية للشركات الخاصة التي تستثمر في الأمن الرقمي، وأوضح التقرير أن هذه الإجراءات يمكن أن تعزز من دور القطاع الخاص في تطوير البنية التحتية الرقمية الآمنة والمستدامة[1].

من الواضح أن التعاون بين القطاعين العام والخاص يُعد عنصرًا حاسمًا لتحقيق بنية تحتية رقمية آمنة للمعاملات الإلكترونية. يتطلب هذا التعاون وجود أطر قانونية وتنظيمية تدعم الشراكة، بالإضافة إلى تعزيز الثقة بين الطرفين من خلال تبادل المعلومات وبناء القدرات المشتركة، وبالتالي يمكن القول أنه بالعمل معًا، يمكن للقطاعين العام والخاص تقديم بيئة رقمية أكثر أمانًا وكفاءة تدعم الاقتصاد الرقمي وتضمن حماية المستخدمين.

[1] الاستراتيجيات المستقبلية لتعزيز التعاون بين القطاعين، منظمة التجارة العالمية.، WTO، جنيف، 2023، ص 45.

قائمة المصادر والمراجع

المصادر

أولا: القوانين الجزائرية

- أمر رقم 58-75 مؤرخ في 20 رمضان 1395 هـ الموافق لـ 26 سبتمبر 1975 المتضمن القانون المدني المعدل والمتمم .الجريدة الرسمية، العدد ،78 السنة ،12 مؤرخة في 24 رمضان 1395 الموافق لـ 30 سبتمبر 1975، المعدل والمتمم بالقانون 10-05 مؤرخ في 20 جوان 2005 الموافق لـ 13 جمادى الأولى 1426.
- مرسوم تنفيذي رقم 162/07 مؤرخ في 30 ماي 2007 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، جريدة رسمية عدد 37 يعدل ويتمم للمرسوم التنفيذي رقم 123/01 المؤرخ في 09 ماي 2001.
- قانون رقم 04/15 مؤرخ 10 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، جريدة رسمية عدد 06 الصادرة في10 فيفري 2015.
- قانون رقم 05/18 مؤرخ في: 25 شعبان 1439هـ الموافق ل 10 مايو 2018، يتعلق بالتجارة الالكترونية، ج.ر عدد 28، مؤرخة في: 30 شعبان 1439هـ الموافق ل 16 مايو 2018.

ثانيا: القوانين الأجنبية

- قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية(1996)، تاريخ الاعتماد: 12 حزيران/يونيه 1996، منشورات الأمم المتحدة، نيويورك، 2000.
- قانون التوقيع الإلكتروني العراقي رقم 15 لسنة 2004، الصادر بتاريخ: 24 ديسمبر 1980، نشر في الجريدة الرسمية العراقية "الوقائع العراقية" في العدد رقم 2760 في سنة 1980.
- قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، القانون رقم 15 لسنة 2004، مطبعة الهيئة المصرية العامة للكتاب، مصر، 2004.

- القانون الاتحادي رقم (1) لسنة 2006 بشأن المعاملات والتجارة الإلكترونية، الصادر بتاريخ: 2006/01/30، الجريدة الرسمية لدولة الإمارات العربية المتحدة.
- Loi n° 2004-575 du 21 juin 2004, Loi pour la confiance dans l'économie numérique, Journal Officiel de la République Française, France, 2004.
- French National Assembly, Loi n° 2004-575 pour la confiance dans l'économie numérique, French Official Gazette, France, 2004, Article 1369-1.
- Loi n° 86-1067 du 30 décembre 1986, Code des postes et des communications électroniques, Journal Officiel de la République Française.

المراجع

الكتب

- إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الالكترونية، دراسة للجوانب القانونية للتعامل عبر أجهزة الاتصال الحديثة والتراسل الالكتروني، مجلس النشر العلمي، جامعة الكويت، 2003.
- أحمد المهدي، الإثبات في التجارة الالكترونية، دار الكتب القانونية، مصر، 2004.
- أحمد عبد الحميد، التحديات القانونية للذكاء الاصطناعي في البيئة الرقمية، جامعة القاهرة، مصر،2021.
- أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الانترنت، دار النهضة العربية، القاهرة، مصر، 2003.
- أمين الغزالي، التجارة الإلكترونية والعولمة: دراسة تحليلية، دار الجسور، الجزائر، 2020.
- ثروت عبد الحميد، التوقيع الالكتروني، دار النيل للطباعة والنشر، مصر، 2001.
- جيمس ماكنزي، القانون الرقمي والتجارة الإلكترونية، مطبعة جامعة أوكسفورد، المملكة المتحدة، 2018.
- خالد السعدي، أهمية البطاقات البنكية في الاقتصاد الرقمي، دار الجيل، بيروت، لبنان، 2020.
- سالم عبد العزيز، "تحليل كفاءة أنظمة الدفع الإلكترونية"، المجلة العربية للدراسات المالية، المجلد 8، العدد 3، القاهرة، مصر، 2020.
- سامي بن زيد، أمن المعلومات في التجارة الإلكترونية، دار الحافظ، الجزائر، 2020.

- سلطان عبد الله محمود الجواري، عقود التجارة الالكترونية والقانون الواجب التطبيق – دراسة قانونية مقارنة، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، لبنان، 2010.
- سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة، دار النهضة العربية، القاهرة، مصر، 2006.
- صقر ن، مكاري ن، الوسيط في القواعد الإجرائية والموضوعية للإثبات في المواد المدنية، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2009.
- ضياء أمين مشيمش، التوقيع الالكتروني، دراسة مقارنة، المنشورات الحقوقية، بيروت لبنان، 2003.
- عادل رمضان الأبيوكي، التوقيع الإلكتروني في التشريعات الخليجية (دراسة مقارنة)، المكتب الجامعي الحديث، الطبعة الأولى، الإسكندرية، مصر، 2009.
- عبد الباسط جاسم محمد، إبرام العقد عبر الانترنت، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، لبنان، 2010.
- عبد الحميد بن منصور، القانون التونسي للمبادلات والتجارة الإلكترونية: دراسة تحليلية، دار الفكر القانوني، تونس، 2002.

عبد الرحمن الفقي، أصول المسؤولية المدنية، دار وائل للنشر، عمان، الأردن، 2003.

- عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الالكترونية (الحاسب الآلي وشبكة المعلومات "الإنترنت")، دار الوراق، دار النيربين للطباعة والنشر والتوزيع، الطبعة الثالثة، 2006.
- عبد العزيز عبد الله، الآثار القانونية للعقود الإلكترونية، دار النهضة العربية، الجزائر، 2018.
- عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون العربي النموذجي، الكتاب الثاني، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2006.
- عبد الله المزروعي، التوقيع الإلكتروني وإصدار الشهادات في القانون الإماراتي، دار النهضة القانونية، الإمارات العربية المتحدة، 2015.
- عبد المجيد الحكيم، عبد الباقي البكري، محمد طه البشير، الوجيز في نظرية الالتزام في القانون المدني العراقي، مصادر الالتزام، مطبعة جامعة بغداد، 1986.

- عصمت عبد المجيد بكر، أثر التقدم العلمي على العقد – تكوين العقد، إثبات العقد، دار صباح صادق جعفر، بغداد، العراق، 2007.
- علي أبو حيدر، أثر التكنولوجيا الرقمية في العمليات التجارية، دار الفكر العربي، مصر، 2019.
- علي فيلالي، التزامات العمل المستحق للتعويض، موفم للنشر والتوزيع، الجزائر، 2002.
- علي صادق، التكنولوجيا المالية والمعاملات الإلكترونية، دار الكتاب العربي، دبي، الإمارات العربية المتحدة، 2018.
- علي عبد العالي خشاب الأسدي، حجية الرسائل الإلكترونية في الإثبات المدني، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ،2013.
- فاتن الكوكي، حماية المعطيات الشخصية في البيئة الرقمية في تونس، المركز العربي للدراسات القانونية، 2005.
- فادي محمد عماد الدين توكل، عقد التجارة الالكترونية، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، لبنان، 2010.
- لينا إبراهيم يوسف حسان، التوثيق الإلكتروني ومسؤولية الجهات المختصة بها (دراسة مقارنة)، دار الراية للنشر والتوزيع، عمان، الأردن،2009.
- ماجد القرني، التجارة الإلكترونية وتطور نظم الشفافية، المكتبة الدولية، السعودية، 2021.
- محمد أمين الرومي، النظام القانوني للتوقيع الالكتروني، دار الفكر الجامعي، الإسكندرية، مصر، 2006.
- محمد السعيد رشدي، وسائل الاتصال الحديثة في الإثبات، مؤسسة دار الكتب للطباعة والنشر والتوزيع، الكويت، 1997.
- محمد الكعبي، التحديات القانونية لحماية البيانات في العالم العربي، مجلة القانون الرقمي، الإمارات العربية المتحدة، 2020.
- محمد الكعبي، استخدام البيانات الشخصية والإعلانات الموجهة، مجلة القانون الرقمي، الإمارات العربية المتحدة، 2021.
- محمد المدني، نظرية السبب في القانون المدني، دار الفكر العربي، القاهرة، مصر، 1995.

- محمد بن علي، تحليل قانون 18-05: التجارة الإلكترونية في الجزائر، مجلة القانون والمجتمع، جامعة وهران2، الجزائر، 2019.
- محمد سعد خليفة، مشكلات البيع عبر انترنت، دار النهضة العربية، القاهرة، مصر، 2002.
- محمد عبد الغني، التجارة الإلكترونية: القانون والواقع، مكتبة القانون العربي، بيروت، لبنان، 2021.
- محمد علي القيسي، قانون المعاملات والتجارة الإلكترونية في دولة الإمارات العربية المتحدة، دار النهضة العربية، الإمارات العربية المتحدة، 2015.
- محمد كمال السيد، حماية البيانات الشخصية في التشريع المصري، المركز المصري للدراسات القانونية، مصر، 2021.
- محمود علي، المخاطر والتحديات المرتبطة باستخدام البطاقات البنكية، مجلة الاقتصاد الرقمي، د.ب.ن، العدد 12، 2021.
- مدحت عبد العال، المسؤولية المدنية الناشئة ن تقديم خدمة التوقيع الإلكتروني، المركز القومي للإصدارات القانونية، مصر، الطبعة الأولى، 2010.
- ممدوح محمد خيري هاشم المسلمي، مشكلات البيع الالكتروني عن طريق الانترنت في القانون المدني – دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2000.
- نجوى أبو هيبة، التوقيع الالكتروني (تعريفه- مدى حجيته في الإثبات)، دار النهضة العربية، مصر، دون سنة نشر.
- نضال إسماعيل برهم، أحكام عقود التجارة الإلكترونية، دار الثقافة، عمان، الأِدن، 2005.
- وائل أنور بندق، قانون التجارة الإلكترونية (قواعد الأونسيترال ودليلها التشريعي)، مكتبة الوفاء القانونية، الإسكندرية، مصر، الطبعة الأولى، 2009.
- وسيم شفيق الحجار، الإثبات الالكتروني، منشورات صادر الحقوقية، بيروت، لبنان، 2001.
- يوسف حسن يوسف، الاقتصاد الالكتروني، المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة، مصر، 2012.
- يوسف حسن يوسف، العقود التجارية الالكترونية الدولية، المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة، مصر، 2012.

- يوسف الخليفي، الاقتصاد الرقمي: الفرص والتحديات، دار الفكر العربي، مصر، 2019.
- يوسف محمد، أنواع البطاقات البنكية واستخداماتها في المعاملات الإلكترونية، دار الندوة، القاهرة، مصر، 2019.

المقالات العلمية

- بن مبارك ماية، الإثبات الالكتروني في مجال القانون الخاص الجزائري، مجلة البحوث في العقود وقانون الأعمال، المجلد 7، العدد 2، 2022/06/10.
- خالد أحمد، "التحديات القانونية لأنظمة المقاصة الإلكترونية"، المجلة الدولية للقانون المالي، المجلد 5، العدد 2، دار النشر القانونية، عمان، الأردن.
- خرباش جميلة، الشيك الإلكتروني أداة وفاء عن بعد في التجارة الإلكترونية، مجلة البيبان للدراسات القانونية والسياسية، المجلد3 العدد1، 2018.
- زهيرة عبوب، المسؤولية المدنية لمقدم خدمات التصديق الالكتروني (دراسة تحليلية لما جاء في القانون رقم 04/15)، مجلة الدراسات القانونية المقارنة، المجلد 6، العدد 2، جامعة حسيبة بن بوعلي، الشلف، 2020.
- علاء الدين الخصاونة، أيمن مساعدة، المسؤولية المدنية لمزود خدمات التوثيق الالكتروني – دراسة تحليلية في ظل نصوص التوجيه الأوربي بشأن التواقيع الالكترونية والتشريعات المقارنة، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد8، العدد1، فبراير 2011.
- غنية باطلي، الكتابة الالكترونية، المجلة الجزائرية لقانون الأعمال، كلية الحقوق والعلوم السياسية، المسيلة، العدد الثاني، ديسمبر 2020.
- ليلى محمد العطار، التحديات القانونية للتجارة الإلكترونية في الوطن العربي، مجلة الحقوق، جامعة الكويت، العدد 4، 2020.
- ليندة بلحارث، النظام القانوني لمزودي خدمات التصديق الالكتروني في القانون الجزائري، مجلة العلوم القانونية والسياسية، المجلد 9، العدد 3، جامعة الشهيد حمّه لخضر بالوادي، ديسمبر 2018.

- محمد فائز خضور، هيثم الطاس، المسؤولية المدنية لمزود خدمات التصديق الالكتروني، مجلة جامعة البعث، المجلد 43، العدد 13، سوريا، 2021.
- هشام عبد الحليم، "الثقة والشفافية في أنظمة المقاصة الإلكترونية"، مجلة الدراسات المصرفية، المجلد 6، العدد 1، المعهد العربي للدراسات المالية والمصرفية، القاهرة، مصر، 2020.
- يوسف عبد القادر، وسائل الإثبات في التجارة الإلكترونية، مجلة القانون والاقتصاد، العدد 7، 2021.

المطبوعات الجامعية

- خديجة عبد اللاوي، مطبوعة بيداغوجية حول محاضرات في قانون المعاملات الإلكترونية، موجهة لطلبة السنة أولى ماستر تخصص قانون خاص، جامعة بلحاج بوشعيب، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2022/2021.

المداخلات

- دوار جميلة، المسؤولية المدنية العقدية لمقدمي خدمات التصديق الالكتروني في التشريع الجزائري، ورقة مقدمة ضمن فعاليات الملتقى الوطني الموسوم حول المسؤولية القانونية في الإدارة الالكترونية، جامعة الجزائر، 13 ديسمبر 2023.

الرسائل الجامعية

- بلقاسم حامدي، إبرام العقد الإلكتروني، أطروحة مقدمة لنيل شهادة الدكتوراه، تخصص قانون الأعمال، جامعة الحاج لخضر، باتنة، 2015.
- سعدي الربيع، حجية التوقيع الالكتروني في التشريع الجزائري، أطروحة دكتوراه في العلوم القانونية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2016.
- عائشة قصار الليل، حجية المحرر والتوقيع الإلكتروني في الإثبات، دراسة تحليلية مقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم الحقوق، باتنة، 2017.

- عايض راشد المري، مدى حجية الرسائل التكنولوجية الحديثة في إثبات العقود التجارية، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 1998.
- محمد أحمد محمد نور إسماعيل، مدى حجية التوقيع الإلكتروني في عقود التجارة الالكترونية، أطروحة دكتوراه، كلية الحقوق، القاهرة، مصر، 2008.

القرارات

- قرار محكمة التمييز الاتحادية في العراق رقم 1014، استئنافية، 2005/11/12، قرار غير منشور.

التقارير

- المركز العربي للأبحاث ودراسة السياسات، حماية البيانات الشخصية في العالم العربي: الواقع والتحديات، المركز العربي للأبحاث، قطر، 2019.
- المركز العربي للأبحاث ودراسة السياسات، حماية البيانات الشخصية في الدول العربية: التحديات والفرص، المركز العربي للأبحاث، قطر، 2020.
- منظمة التجارة العالمية، (WTO) تحديات التجارة الإلكترونية عبر الحدود، منظمة التجارة العالمية، جنيف، 2020.
- الاتحاد العربي للأمن السيبراني، تقرير الهجمات السيبرانية على التجارة الإلكترونية، الاتحاد العربي للأمن السيبراني، المملكة العربية السعودية، 2021.
- الاتحاد العربي للأمن السيبراني، "تقرير الأمن السيبراني العالمي، الاتحاد العربي للأمن السيبراني، المملكة العربية السعودية، 2022.
- U.S. Congress. Electronic Signatures in Global and National Commerce Act (E-SIGN Act). Washington, DC: U.S. Library of Congress, 2000.
- U.S. Congress U.S. Congress, Electronic Signatures in Global and National Commerce Act (ESIGN), Library of Congress, United States of America, 2000, Section 101, ESIGN Act.

المراجع الأجنبية

- Alain Bensoussan, Le commerce électronique, aspects juridique, édition HERMES, Paris, 1998.

- Amy Webb, The Signals Are Talking: Why Today's Fringe is Tomorrow's Mainstream, PublicAffairs, USA, 2018.
- Brown, P. "Legal Obligations of Debit Cardholders." International Journal of Electronic Transactions Law, Vol. 28, 2018.
- Doe, A. "Advantages of Debit Cards in Modern Banking." Banking Review Quarterly, Issue 12, 2020.
- Douglas R. Stinson & Maura Paterson, Cryptography: Theory and Practice, CRC Press, 4th édition, 2018.
- Eric Rescorla, SSL and TLS: Designing and Building Secure Systems, Addison-Wesley Professional, First édition, 2001.
- Eric Capitaine, The Law on Digital Economy Trust and its Applications, European Law Publishing House, France, 2005.
- Jean Smith, E-commerce Law : Digital Transactions, Cambridge University Press, U.K, 2019.
- Johannes A. Buchmann, Public Key Infrastructure (PKI): Principles and Applications. Springer, 2013.
- Johnson, William, E-Commerce and Cost Reduction Strategies, McGraw-Hill, United Kingdom, 2018.
- Jonathan Katz & Yehuda Lindell, Introduction to Modern Cryptography: Principles and Protocols, Chapman and Hall/CRC, 2007.
- Linda Davis. "Cybersecurity Challenges in E-Check Systems." Cybersecurity Journal, vol. 8, no. 4, 2020.
- Miller, K. "Security Measures for Debit Cardholders." Electronic Banking Security Journal, Vol. 17, 2021.
- Nicolas Bernard, The Legal Framework of Trust in Digital Services in the European Union: eIDAS Regulation, European Legal Publishing House, Belgique, 2017.
- Philip Kotler, Marketing in the Digital Age, Pearson, USA, 2020.
- Sara Peterson, International Trade and Internet Laws, Blackwell Publishing, New York, USA, 2017
- Sarah Wilson. "The Benefits of E-Checks in Modern Banking." Journal of Financial Innovation, vol. 15, no. 3, 2022.
- Smith, David. "Digital Preservation and the Future of Digital Content." Journal of Digital Information, 2005.
- Smith, Julia. "Components of Credit Cards and Their Security Features." Financial Instruments Journal, vol. 58, no. 1, 2019.
- Thomas Roche, L'impact des directives européennes sur le droit français des transactions électroniques, Éditions LGDJ, France, 2003.

- Yves POULLET, Mireille ANTOINE, Vers la confiance ou comment assurer le développement du commerce électronique, collection LEEPRESSE, Paris France, 2001.

المراجع الإلكترونية

- أميمة لعروسي، حجية المحرر الالكتروني، موقع المكتب القانوني الالكتروني (e-legal office)، https://e-legaloffice.com/authentic-electronic-contract/، تم الاطلاع بتاريخ: 2024/08/17.

- موقع وزارة البريد والمواصلات السلكية واللاسلكية، الجزائر، على الرابط الإلكتروني: https://www.mpt.gov.dz/%D8%A7%D9%84%D8%AA%D9%88%D9%82%D9%8A%D8%B9-%D9%88%D8%A7%D9%84%D8%AA%D8%B5%D8%AF%D9%8A%D9%82-%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D9%8A%D9%86/.

- موقع مديرية التجارة لولاية بسكرة، وزارة التجارة الجزائرية، على الرابط الالكتروني: https://www.dcwbiskra.dz/index.php?option=com_content&view=article&id=249&Itemid=83#:~:text=%D8%A3%D9%85%D9%91%D8%A7%20%D8%A7%D9%84%D8%AA%D8%B5%D8%AF%D9%8A%D9%82%20%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%8C%20%D9%8A%D9%82%D8%B5%D8%AF%20%D8%A8%D9%87,%D9%85%D8%B9%D9%8A%D9%86%D8%A9%D8%8C%20%D9%88%D9%8A%D8%B3%D9%85%D9%89%20%D9%85%D9%82%D8%AF%D9%91%D9%85%20%D8%AE%D8%AF%D9%85%D8%A7%D8%AA%20%D8%A7%D9%84%D8%AA%D8%B5%D8%AF%D9%8A%D9%82

- موقع سلطة ضبط البريد والاتصالات الالكترونية (ARPCE)، التصديق الإلكتروني، على الرابط الالكتروني: https://www.arpce.dz/ar/topic/ce.

- موقع السلطة الحكومية للتصديق الالكتروني، الجزائر، على الرابط الالكتروني: https://agce.dz/ar/presentation-de-lagce/.

- Bea tanese, The History of Ecommerce: From the 1960s to the 2020s, 06/10/2021, https://www.shipmonk.com/blog/the-history-of-ecommerce-from-the-1960s-to-the-2020s.
- Vladimir Zwass, E-commerce History, Britannica, 28/08/2024, https://www.britannica.com/money/e-commerce.
- History And Evolution of Ecommerce - How It Began?, SpiralClick, 05/08/2019, https://spiralclick.com/blog/history-and-evolution-of-ecommerce.

- National Conference of Commissioners on Uniform State Laws. Uniform Electronic Transactions Act (UETA). 1999. Available online at : https://www.lawschool.cornell.edu/.
- "What Is a Prepaid Debit Card and How Does It Work?", The Balance, https://www.thebalancemoney.com/, Accessed September 2023.
- The Physics Classroom. (n.d.). *The Electron*. Retrieved September 17, 2024, from https://www.physicsclassroom.com/class/modern/Lesson-1/The-Electron , Accessed September 2024.
- United Nations. (2017). United Nations Convention on the Use of Electronic Communications in International Contracts. Retrieved from https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications_international_contracts
- United Nations. (1996). Mali Declaration on Electronic Commerce. Retrieved from https://unctad.org/webflyer/mali-declaration-electronic-commerce
- U.S. Congress. (2000). Electronic Signatures in Global and National Commerce Act. Retrieved from https://www.congress.gov/bill/106th-congress/house-bill/1714/text
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910 , visité le : 28/07/2024.
- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, 2008.
- Ronald L. Rivest, Adi Shamir, Leonard Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, Association for Computing Machinery (ACM), https://dl.acm.org/doi/10.1145/359340.359342.

الـــفـهـــرس

العـنـــــوان	الصفحة
مـقـدمــة	**1**
المحور الأول: مفهوم المعاملات الالكترونية- أنواعها- آثارها القانونية	**5**
المبحث الأول: الإطار النظري للمعاملات الالكترونية (النشأة – التعريف – الخصائص)	**7**
المطلب الأول: نشأة المعاملات الالكترونية	**7**
الفرع الأول: أسباب ظهور المعاملات الالكترونية	**7**
الفرع الثاني: أهمية المعاملات الالكترونية	**9**
المطلب الثاني: تعريف المعاملات الالكترونية وخصائصها	**11**
الفرع الأول: تعريف المعاملات الالكترونية	**11**
الفرع الثاني: خصائص المعاملات الالكترونية	**16**
المبحث الثاني: الإطار العملي للمعاملات الالكترونية	**19**
المطلب الأول: أنواع المعاملات الالكترونية	**19**
الفرع الأول: الشيك الالكتروني والمقاصة الالكترونية	**19**
الفرع الثاني: البطاقات البنكية والأوراق التجارية الالكترونية	**23**
المطلب الثاني: العقد الالكتروني في قانون 05/18	**31**
الفرع الأول: تعريف العقد الالكتروني	**31**
الفرع الثاني: خصائص العقد الالكتروني	**34**
المحور الثاني: طرق الاثبات في المعاملات الالكترونية	**39**
المبحث الأول: إقرار الإثبات بالكتابة الإلكترونية	**41**
المطلب الأول: مفهوم الكتابة الإلكترونية	**41**
الفرع الأول: تعريف الكتابة الإلكترونية وخصائصها	**41**

الفرع الثاني: الشروط القانونية للكتابة الإلكترونية	**48**
المطلب الثاني: حجية الكتابة الإلكترونية وصورها	**52**
الفرع الأول: حجية الكتابة الإلكترونية	**52**
الفرع الثاني: صور الكتابة الإلكترونية	**54**
المبحث الثاني: إقرار الإثبات بالتوقيع الالكتروني	**58**
المطلب الأول: ماهية التوقيع الإلكتروني	**58**
الفرع الأول: تعريف التوقيع الإلكتروني	**58**
الفرع الثاني: صور التوقيع الالكتروني	**62**
الفرع الثالث: خصائص وعيوب التوقيع الالكتروني	**67**
الفرع الرابع: وظائف التوقيع الالكتروني	**71**
المطلب الثاني: حجية الإثبات بالتوقيع الإلكتروني	**73**
الفرع الأول: شروط تحقق حجية التوقيع الالكتروني	**73**
الفرع الثاني: حجية التوقيع الالكتروني في التشريع الجزائري	**76**
الفرع الثالث: التصديق الإلكتروني كآلية لتوثيق التوقيع الالكتروني	**78**
المحور الثالث: مسؤولية مزودي خدمة التصديق الالكتروني	**85**
المبحث الأول: مضمون وطبيعة التزامات مزود خدمات التصديق الالكتروني	**87**
المطلب الأول: مضمون التزامات مزود خدمات التصديق الالكتروني	**87**
الفرع الأول: تعريف مزود خدمة التصديق الإلكتروني في التشريع الجزائري والقانون المقارن	**88**
الفرع الثاني: الالتزامات غير الفنية لمزود خدمة التصديق الالكتروني	**91**
الفرع الثالث: الالتزامات الفنية لمزود خدمة التصديق الالكتروني	**95**
المطلب الثاني: طبيعة التزامات مزود خدمات التصديق الالكتروني	**97**
الفرع الأول: الالتزام ببذل عناية	**98**
الفرع الثاني: الالتزام بتحقيق نتيجة	**99**
المبحث الثاني: صور المسؤولية المدنية لمزود خدمات التصديق الالكتروني	**101**

المطلب الأول: المسؤولية المدنية لمزود خدمات التصديق الالكتروني وفق القواعد العامة	**101**
الفرع الأول: المسؤولية العقدية	**102**
الفرع الثاني: المسؤولية التقصيرية	**107**
المطلب الثاني: المسؤولية المدنية لمزودي خدمة التصديق الالكتروني وفق القواعد الخاصة	**111**
الفرع الأول: مسؤولية مزودي خدمة التصديق الالكتروني وفقا للتشريعات المقارنة	**112**
الفرع الثاني: مسؤولية مزودي خدمة التصديق الالكتروني وفقا للتشريع الجزائري	**116**
المحور الرابع: التحديات المستقبلية وتطور المعاملات الالكترونية	**119**
المبحث الأول: التحديات القانونية والتقنية في ظل التطورات السريعة للتكنولوجيا	**121**
المطلب الأول: التحديات القانونية للمعاملات الالكترونية في ظل التطورات السريعة للتكنولوجيا	**121**
الفرع الأول: التحديات المتعلقة بحماية البيانات الشخصية	**122**
الفرع الثاني: التحديات المتعلقة بالمسؤولية القانونية والجرائم الإلكترونية	**125**
المطلب الثاني: التحديات التقنية للمعاملات الالكترونية في ظل التطورات السريعة للتكنولوجيا	**127**
الفرع الأول: التحديات الأمنية في المعاملات الإلكترونية	**127**
الفرع الثاني: التحديات المتعلقة بالتفاوت في التقنية	**128**
المبحث الثاني: التوقعات المستقبلية والتعديلات المتوقعة في القوانين الحالية	**129**
المطلب الأول: التوقعات المستقبلية للقوانين في مجال المعاملات الالكترونية	**129**
الفرع الأول: التعديلات المستقبلية في مجال التكنولوجيا الرقمية والتجارة الالكترونية	**130**
الفرع الثاني: التعديلات المستقبلية في مجال الذكاء الاصطناعي	**132**
المطلب الثاني: التوقعات المستقبلية المتعلقة بالحوكمة الرقمية	**135**
الفرع الأول: تعزيز الشفافية والكفاءة في إدارة المعاملات الرقمية	**135**
الفرع الثاني: التعاون بين القطاعين العام والخاص لتحقيق بنية تحتية رقمية آمنة	**136**
قائمة المصادر والمراجع	**139**
الفهرس	**150**