الجامعة اللبنانية
كلية الحقوق والعلوم السياسية والإدارية
العمادة

التوقيع الإلكتروني

دراسة مقارنة

رسالة أعدّت لنيل شهادة دبلوم الدراسات العليا في اختصاص قانون الأعمال

إعداد

الطالب جورج جان مرعب

لجنة المناقشة

الدكتور **وسام غيّاض**	الأستاذ المشرف	رئيساً
الدكتور	.....	عضواً
الدكتور	.....	عضواً

٢٠٢٣

الجامعة اللبنانية
كلية الحقوق والعلوم السياسية والإدارية
العمادة

التوقيع الإلكتروني

دراسة مقارنة

رسالة أعدّت لنيل شهادة دبلوم الدراسات العليا في اختصاص قانون الأعمال

إعداد

الطالب جورج جان مرعب

لجنة المناقشة

الدكتور **وسام غيّاض**	الأستاذ المشرف	رئيساً
الدكتور	.....	عضواً
الدكتور	.....	عضواً

٢٠٢٣

الجامعة اللبنانية غير مسؤولة عن الآراء الواردة في هذه الرسالة وهي تعبّر عن رأي صاحبها فقط.

إهداء

أهدي هذا العمل:

إلى والديّ اللّذين بذلا جهد السنين من أجلي،

إلى من اخترتها شريكةً على دروب هذه الحياة،

إلى فلذتيّ كبدي ونبضات قلبي،

إلى العماد الذي أرتكز عليه، إخوتي،

إلى من كان لي سندًا ومعلّمًا في مهنة المحاماة المحامي مارون الحويك،

إلى الدكتورة أمل كاترين عبدالنور التي كانت لي خيرَ داعمٍ.

شكر وتقدير

أتوجّه بالشكر والتقدير للدكتور وسام غيّاض الذي أشرف على هذه الرسالة مسديًا إليّ النصائح والتوجيهات،

وإلى لجنة المناقشة،

إنّ عبارات الشكر لا يمكن أن تفيكم حقّكم، خاصّة في هذه الظروف الحالكة التي تعصف ببلادنا والتي شلّت كافّة قطاعات الدولة، فقد أثبتّم بالفعل لا بالقول أنّ التعليم رسالة، وآمنتم أنّه بالعلم وحده يمكننا أن نبدّد دياجير الظلام الذي تعيشه أمّتنا،

فلكم منّي كلّ التقدير.

المقدمة

الفصل الأول :الأحكام العامّة للتوقيع الإلكتروني

المبحث الأول: ماهيّة التوقيع الإلكتروني

الباب الأول: التوقيع اليدوي والتوقيع الإلكتروني

الفقرة الأولى: التوقيع اليدوي التقليدي

أولاً: تعريف التوقيع اليدوي

ثانياً: صيغة التوقيع اليدوي

ثالثاً: شروط صحّة التوقيع اليدوي

الفقرة الثانية: التوقيع الإلكتروني

أولاً: تعريف التوقيع الالكتروني

ثانياً: صور التوقيع الإلكتروني

الباب الثاني: الفرق بين التوقيع التقليدي والتوقيع الإلكتروني

الفقرة الأولى: الإختلافات بين التوقيع التقليدي والتوقيع الإلكتروني

أولاً: الإختلاف من الناحية المادّية

ثانياً: الاختلاف من الناحية العملية والمعنويّة

الفقرة الثانية: حجيّة التوقيع الإلكتروني في المرحلة السابقة لإقرار التشريعات المنظّمة له

أولاً: العقبات التي واجهت الإعتراف بالتوقيع الإلكتروني

ثانياً: الإستثناءات القانونية المتعلّقة بالإثبات

المبحث الثاني: حجيّة التوقيع الإلكتروني في القوانين الوضعية

الباب الأول: حجيّة التوقيع الإلكتروني

الفقرة الأولى: حجّيّة التوقيع الإلكتروني في النصوص

لائحة المختصرات

١- باللّغة العربية

ص.	الصفحة
أ.م.م.	قانون أصول المحاكمات المدنية اللبناني
ق.ع.	قانون العقوبات اللبناني

٢-باللّغة الفرنسية

Op. cit	Ouvrage précité
P.	Page
Ed.	Edition
Cass. civ	Cour de cassation Chambre civile
Bull.	Bulletin
J.C.PG	Juris-classeur périodique, Edition générale
Gaz. Pal	Gazette du Palais
L.G.D.j	Librairie générale de droit et de jurisprudence
N°	Numéro
CA.	Cour d'appel
Ch. soc	Chamber sociale
JO L	Journal officiel de l'Union européenne

المقدمة

عرف العالم تحوّلاً في تقنيّات التواصل والتبادل، سيطرت فيه الوسائل الحديثة التي قرّبت المسافات مهما بعُدت، وأخذ حجم التعاملات الإلكترونية يتعاظم ويتنامى، ممّا أدّى إلى نشوء مساحة مشتركة بين المعلوماتية والقانون.

لقد بدأ استعمال الحاسوب في مطلع الثمانيات من القرن الماضي، من قبل القطاع الخاص، إلاّ أنّ إستعماله في المعاملات اقتصر على إدخال البيانات واستخراجها وطباعة المستندات آليًا، ممّا شكّل نقلةً نوعيةً عن الطباعة على الآلة الكاتبة، أو عن حفظ الملفات ورقيًا بواسطة أنظمة أرشفة تقليدية. وقد أدّى السماح للجمهور باستعمال شبكة الإنترنت، في بدايات التسعينيات من القرن المنصرم، إلى إمكانية تبادل المعلومات في بداية الأمر، ومن ثمّ إلى تبادل الرسائل والمعاملات. وفي وقتٍ لاحقٍ جرى استعماله كوسيلة لتسليم بعض المنتجات ذات الطابع الإلكتروني، وهو ما أصبح يعرف، اليوم، بالمعاملات الإلكترونية.

فبدأت التساؤولات تُطرح حول صحة وسلامة كلّ من المستند الإلكتروني غير المطبوع ورقيًا والتوقيع، إذ أنّ نسخ التوقيع الخطي وإيراده إلكترونيًا، لا يحقّق ذات القوة الثبوتية للتوقيع الخطي على ركيزة ورقية، ذلك أنّ حماية الصورة المنسوخة قد تتعرّض للانتهاك.

يُشكّل المستند الورقي، بطبيعته، وسيلة حفظ وإثبات وحجّة على من وقّعه أو صاغه، وله قوّة ثبوتية شاملة نظرًا لكونه يسمح لأيّ شخص كان، حتى ولو لم يكن يتمتّع بمعرفة تقنية أو خبرة، باكتشاف أي تعديل يطرأ على المستند أو مضمونه. فإنه وبمجرّد النظر بالعين المجرّدة إلى مستند ورقيّ، يمكن للناظر ملاحظة أيّ حشوٍ أو إضافة أو تمزيق أو محو، ممّا يفيد الناظر بأنّ المستند لم يعد بحالته السليمة. هذه التغييرات من شأنها المساس بالقوّة الثبوتية، أو بصلاحية المستند الورقي لإنتاج المفاعيل القانونية. ويظهر، بالتالي، الفارق بين المستند الورقي والمستند الإلكتروني الذي لا يسمح، بفعل طبيعته، لمن يعاينه باكتشاف أي تعديل أو تغيير في صياغته الأساسية.

فكان لا بدّ من وضع معايير لحماية المستند الإلكتروني، مثل التشفير الذي يمنع الولوج إليه. وقد نشأ لهذه الغاية، ما يُعرف بالتوقيع الإلكتروني؛ وهو عبارة عن بيانات بشكل إلكتروني متّصلة أو مرتبطة منطقيًا ببيانات

إلكترونية أخرى، وهي تستعمل كوسيلة لتأكيد الموثوقية. ويتمتّع التوقيع الالكتروني بعددٍ من الإجراءات التقنيّة التي تسمح باعتماده والتأكّد من صحّته ومن صدوره عن الشخص المعني به.

١. الإشكاليات

تطرح مسألة التوقيع الإلكتروني في الواقع اللبناني إشكالية تتمحور حول سُبُل حماية التّوقيع الإلكتروني في التشريع اللبناني، والتي يتفرّع عنها عدّة تساؤلات سنسعى لمعالجتها من خلال هذا البحث، هي:

- ما هو التوقيع الإلكتروني وما مدى استجماعه لعناصر التوقيع اليدوي التقليدي؟
- ما هي الشروط الواجب توافرها في التوقيع الإلكتروني لاعتباره دليلا" كاملا" في الإثبات؟
- ما هو موقف التشريع اللبناني والتشريعات المقارنة من التوقيع الإلكتروني؟
- ما هي الوسائل التقنية والقانونية لحمايته؟
- كيف يمكن للبنان الإستفادة من تجارب التشريعات المقارنة لحسن تنظيم التوقيع الإلكتروني؟

٢. أهداف البحث

أمام فعاليّة تقنيّة التوقيع الإلكتروني على مستوى التّجارة الدولية، وبما أنّ "القانون والتقنيات تتشابك بطرق متعدّدة"،" كما اعتبر العلامة سافاتييه، فقد سنّت العديد من التشريعات العربية والأجنبية قوانين تبنّت فيها التوقيع الإلكتروني ونظّمت أُطُره. وبهدف تحقيق الغاية المرجوة من اختيارنا لموضوع بحثنا، والتي تتمثل في البحث في الأطر القانونيّة الأمثل للتوقيع الإلكتروني، وتقديم المقترحات للمشرّع اللبناني بشأن التنظيم القانوني الأمثل للتوقيع الإلكتروني، خاصّة أنّه وبعد إصداره القانون رقم ٢٠١٨/٨١ الذي لم يدخل بعد حيّز التطبيق الفعلي والكلّي نتيجة عدم إصدار المراسيم اللازمة والبطء في إطلاق عجلة المجلس الوطني للاعتماد COLLIBAC الذي أولاه القانون السالف الذكر صلاحيّات بغاية الأهميّة.

٣. المنهج المتّبع

ستعتمد دراستنا على أسلوب البحث القانوني المقارن لذا ستشمل هذه الدراسة على العديد من التشريعات التي تناولت التوقيع الإلكتروني، سواء أكانت هذه التشريعات ذات طابعٍ دولي أو وطني. فعلى المستوى الدولي، سوف نحرص على جمع كل ما أصدرته لجنة الأمم المتحدة للقانون التجاري، من قوانين نموذجية وضعت بهدف الاسترشاد بها من قبل الدول عند وضع تشريعاتها، وكذلك الإرشادات التي وضعها الاتحاد الأوروبي للدول الأعضاء فيه بشأن المسائل المتعلقة بالتوقيع الإلكتروني، وسنتطرّق إلى التشريعات الوطنية

في الدول الغربية بصفة أساسية في فرنسا، وأيضاً تشريعات الدول العربية التي نظمت التوقيع الإلكتروني مثل تونس ومصر.

أمّا على صعيد التشريع اللبناني، فسنتطرّق إلى القانون رقم ٢٠١٨/٨١ المذكور أعلاه. إضافة إلى ما تقدّم، ومن الناحية العمليّة، سنبحث في كيفيّة عمل التوقيع الإلكتروني والوسائل الأنجح لحمايته من التزوير والتلاعب.

٤. الصعوبات

تكمن أبرز الصعوبات التي واجهتنا في بجثنا بحداثة موضوع التوقيع الالكتروني والتردّد بإطلاق خطّة واضحة لإدخال القانون رقم ٢٠١٨/٨١ حيّز التنفيذ، فضلا" عن عدم صدور قراراتٍ قضائية عن المحاكم اللبنانية تتعلّق بموضوع دراستنا.

٥. خطّة البحث

تمّ تقسيم هذه الدراسة إلى فصلين، حيث سنتناول في الفصل الأول الأحكام العامّة للتوقيع الإلكتروني مستعرضين ماهيّته في المبحث الأول وحجّيته في الإثبات في المبحث الثاني. أمّا في الفصل الثاني فسنتناول وسائل حماية التوقيع الإلكتروني التقنية والقانونية، وسنتطرّق في المبحث الأول إلى دور التشفير والتوثيق في حماية التوقيع الإلكتروني، وإلى مسؤولية مقدّمي خدمات المصادقة والحماية الجزائية للتّوقيع الإلكتروني في المبحث الثاني.

الفصل الأول
الأحكام العامّة للتوقيع الإلكتروني

التوقيع هو مؤسّسة قانونية قديمة نتجت عن تطوّر الكتابة عبر العصور، فرسوم الإنسان الأولى على جدران الكهوف تعود لأكثر من عشرين ألف سنة قبل الميلاد، حيث بدأ الإنسان يعّبر عمّا يخالجه باستخدام أدوات الصيد والحجر.

وقد استلزم تطوّر التجارة في العالم، ولا سيّما في حوض البحر الأبيض المتوسط، مسك حسابات في جداول من الآجر (Argile)، وانتقل الإنسان من بعد ذلك إلى المرحلة الصوتية حيث اهتمَّ في هذه المرحلة بابتكار أسلوب يتيح له التواصل بشكل أبسط، فقام بالتعبير عن الكلمات برموز صوتية خاصّة يُفهم دون التعبير عنها بشكل صوريٍّ. وعلى هذه الأسس بنيت الكتابات المسمارية والهيروغليفية، واخترع من بعدها الفينيقيون حوالي العام ١٢٠٠ ق.م. الأحرف الأبجدية ونشروا هذا المفهوم الذي ساهم فيما بعد لظهور الأبجدية اليونانية والأرمنية وغيرها[١].....،

والكتابة في كافّة المراحل التاريخية التي مرّت بها وفي أصقاع الأرض المختلفة وإن تباينت إلا أنّها تبقى مؤلّفة من ثلاثة عناصر:

- تمثيل الموضوع المدرك حسيًّا (أي المحدّد) برسم كامل أو جزئي
- وصف ما لا يُدرك حسيًا (أي المجرّد) عن طريق الرمز
- نقل الصوت باللغز الصوتي.

وهذه العناصر هي أساس الكتابة البدائية، ويمكن النظر إليها كعناصر مستقلّة خُلقت بذاتها، ويُفسّر نشوؤها باحتياجات الإنسان في كلّ الأزمان وعند جميع الشعوب[٢].

---

[١] رانيا، صليبا، الإثبات بين التقليد والحداثة في ظل قانون أصول المحاكمات المدنية ومتطلبات العصر: دراسة مقارنة– ص. ٢٢.

[٢] فريدريش، يوهانس، تاريخ الكتابة، ترجمة د. سليمان أحمد الضاهر، منشورات الهيئة العامة السوريّة للكتاب، سوريا، ٢٠١٣، ص. ٥١.

في القرون الوسطى، بدأ استعمال الكتابة بعد تطوّر مفاهيمها، بغية تدبيج القوانين الصادرة عن الملك، وبقيت الكتابة خارج هذا الإطار محصورة برجال الدين. وقد شكّل ظهور الطباعة في العام ١٤٥٠ نقلةً نوعيةً في مفهوم الكتابة التي أخذت شيئا فشيئا تتّسم بالطابع الشخصي، بدأ من بعدها صدور المذكّرات الرسمية بصورة خطيّة.

نتيجة التطوّر على مستوى القانون المدني، أصدر ملك فرنسا فرانسوا الأول في العام ١٥٣٩ بصورةٍ مكتوبةٍ قرار (Villers–Cotterêt)، تمّ بموجبه تكليف الكهنة تسجيل المواليد والزيجات والوفيات ، وإنشاء مكتب تسجيل في كل رعية[1].

[1] A–F.Fausse, la signature électronique transaction et confiance sur internet,Dunod, Paris 2000, p.365.

المبحث الأول: ماهيّة التوقيع الإلكتروني

شهِد العالم في القرن الماضي ثورةً في مجال الاتصالات والمعلوماتية انبثق عنها ظهور المستندات الإلكترونية والتي اقترنت بظهور التوقيع الإلكتروني الذي يتلاءم بطبيعته مع طبيعة المستندات السالفة الذكر. وقد شاعَ استعمال التوقيع الالكتروني في ميدان المعاملات المصرفية، واقترن ظهوره باستخدام البطاقات المصرفية.

ونظرًا لمدى أهميته، فقد سعت معظم التشريعات لقوننة هذا النوع من التوقيع وتحديد شروط صحّته ومدى أدائه لوظيفة التوقيع اليدوي التقليدي، لذا سنتطرّق في الباب الأول أدناه إلى خصائص كلّ من التوقيع اليدوي والإلكتروني، وفي الباب الثاني سنتاول الفرق بين كلٍّ منهما.

الباب الأول: التوقيع اليدوي والتوقيع الإلكتروني

نتيجة التطوّرات في طريقة إبرام العقود وعناصرها، لم تعد مسألة توثيق الأعمال القانونية وحجيّتها في الإثبات قاصرةً على التوقيع العادي، فظهر التوقيع الإلكتروني الذي طرح مع بداية ظهوره إشكاليةً قانونيةً وأثار تضاربًا في الآراء الفقهية بشأن قبوله في الإثبات ومنحه درجةً ثبوتيةً موازيةً للتوقيع العادي.

الفقرة الأولى: التوقيع اليدوي التقليدي

يمكن اعتبار التوقيع بمثابة المظهر الخارجي للإرادة إذ يعبّر عن رضى الموقّع. والتوقيع هو العنصر الأساسي الوحيد الذي يُشترط توافره لإثبات صحّة السند العادي[1] كذلك يعتبر من أهمّ عناصر السند الرسمي، فهو ينسب السند إلى من يُراد الاحتجاج عليه به،

وسنتناول فيما يلي: تعريف التوقيع اليدوي (أولا")، صيغته (ثانيًا) وشروط صحّته (ثالثًا).

أولاً: تعريف التوقيع اليدوي

لم يعرّف قانون أصول المحاكمات المدنية اللبناني التوقيع حاله كحال معظم القوانين المقارنة، وقد أتى هذا القانون على ذكر التوقيع في عدّة مواد منه، كالمادة ١٤٤ التي عرّفت السند الرسمي، والمادة ١٥٠ التي عرّفت السند العادي الذي يؤلّف التوقيع أحد أبرز أركانه، كذلك في المادة ١٥١ المتعلّقة بإنكار الخطّ أو التوقيع وفي المادة ١٥٤ المتعلّقة بحجيّة السند.

---

[1] أدوار، عيد، موسوعة أصول المحاكمات والإثبات والتنفيذ، الجزء الرابع عشر، مطبعة المتني، الطبعة الثانية، ١٩٩٤، ص. ٩٥.

ويمكن تعريف التوقيع بأنّه علامة شخصية متميّزة بمن صدرت عنه، أو علامةً معينةً اعتاد استعمالها لتمييز هويته أو للإعلان عن إرادته بقبول التزاماته، وهناك عنصران يقتضي توافرهما في التوقيع:

- عنصر مادي يتمثّل بالإشارة الظاهرة التي يُكتب بها التوقيع، والتي تشكّل دليلا على حضور الموقّع مجلس العقد.
- عنصر معنوي يكمن في توافق إرادة الموقّع مع محتويات السند.

ثانياً: صيغة التوقيع اليدوي

يشمل التوقيع عادةً اسم الموقّع واسمه العائلي أو لقبه، ولكن قد يقتصر على أحدهما، والشرط المهم لصحّة التوقيع أن يتميّز بطابع شخصي يسمح بالتعريف عمن صدر عنه.

وقد اعتبر في هذا السياق أنّ اشتمال التوقيع على الاسم الشخصي للموقّع هو كافٍ كذلك بالنسبة لاشتماله على الأحرف الأولى من اسمه وكنيته أو على تأشيرة (Parafe)، فهذه الكتابات تصلح كتوقيع متى كانت تؤلّف علامة شخصيّة ومتميّزة بوجه أكيد، من شأنها أن تدلّ على إرادة الموقّع[1]، ويجدر بالتوقيع أن يكون مقروءًا وواضحًا، أمّا التوقيع غير المقروء فيبقى صحيحًا إذا كان الشخص الصادر عنه قد اعتاد التوقيع بهذا الشكل وأصبح بالإمكان الدلالة عليه بشكل كافٍ. كما يجب أن يكون التوقيع مكتوبًا بخطّ اليد وليس عن طريق استعمال ختم الذي يعتبر وسيلة ميكانيكية لطبع توقيع الشخص.

أمّا بالنسبة لبصمة الإصبع التي تؤلّف بحدّ ذاتها وسيلة كافية للاستدلال على شخص الموقّع وذلك لاختلاف خطوط الجلد في الطرف الداخلي للإصبع بين شخص وآخر، فقد رفض القانون المدني الفرنسي قبل تعديله حلول بصمة الإصبع محلّ التوقيع كذلك الأمر بالنسبة للختم، فالتوقيع في القانون الفرنسي قبل تعديله نجد يتّخذ شكلا واحدًا وهو الإمضاء الشخصي، ويجب أن يكون مكتوبًا ولا يمكن أن يأتي في أي شكل آخر، غير أن القانون الفرنسي الصادر في ١٦ يوليو ١٩٦٦ المتعلّق بالأوراق التجارية، قد أجاز أن يتمّ التوقيع بأيّة وسيلة إذ إنّ مبدأ حرّية الإثبات هو السائد في المعاملات التجارية.

أمّا قانون أصول المحاكمات المدنية اللبناني فقد أجاز في المادة 150 منه استعمال بصمة الإصبع دون الختم، ويشترط بالتوقيع أن يكون بخطّ صاحبه إلا أنّه يمكن أن يتمّ بخطّ شخص آخر غير الأطراف الموقعين على السند وذلك متى كان هذا الشخص وكيلا حيث يقوم بالتوقيع بإمضائه على الورقة نيابةً عن الموكل.

[1] أدوار، عيد، المرجع السابق، ص. ٩٥.

ثالثاً: شروط صحّة التوقيع اليدوي

مّما سبق بيانه أعلاه، يمكننا أن نستخلص ضرورة توافر ثلاثة شروط لصحّة التوقيع وهي المطابقة، الديمومة، وأن يكون مباشرًا.

١. مطابقة التوقيع

ويُقصد بذلك أن يتمّ التوقيع بالطريقة ذاتها التي اعتاد الشخص على استعمالها بغية التعبير عن موافقته ورضاه على مضمون المستند، فيقتضي بالتالي أن يدلّ التوقيع على هويّة صاحبه.

٢. ديمومة التوقيع

يجب أن يستعمل وسيلة للتوقيع تترك أثرًا متميزًا، يبقى ولا يزول، ويتحقق هذا الأمر عن طريق استعمال أحبار غير متلاشية، وهي عبارة عن أحبار تتكوّن من ثلاثة عناصر أساسية:

- المواد الملوّنة أو المواد الجافة: تمثّل ٢٥ بالمئة من مكوّنات الحبر وتتألّف من صباغ أو خضاب (pigment) أو كلاهما، وهي مواد غير متطايرة تترسّب على سطح الركيزة الورقية وتتغلغل بين أليافها.
- الحامل: يشكّل ٥٠ بالمئة من مكوّنات الحبر، وهو عبارة عن مواد متطايرة.
- الإضافات: تشكّل ٢٥ بالمئة من مكوّنات الحبر وهي عبارة عن عوامل تحكم بالأكسدة والتآكل[١].

وهذه الأحبار تختلف بطبيعتها عن الأحبار المتوارية أو المتلاشية التي يدخل في تركيبتها مادة ذات أساس حمضي، وهي أحبار تختفي بعد مرور وقت قصير على استعمالها.

٣. أن يكون التوقيع مباشرًا

ويعنى بذلك أن يتولّي الشخص بنفسه وضع التوقيع فيجب أن يصدر التوقيع ممن يراد أن يحتجّ به عليه، ويجوز التوكيل في التوقيع كما سبق بيانه. كذلك يشترط أن يرد هذا التوقيع على السند بحيث يكونان كلًّا لا يتجزأ.

---

[١] رياض، فتح الله بصلة، حدود الإثبات العلمي في قضايا التزييف والتزوير، دار نوبار للطباعة، الطبعة الأولى،٢٠٠١، مصر، ص٣١١.

عموماً، يوضع التوقيع في نهاية السند، حتى ينسحب على جميع البيانات الواردة فيه، ويعلن بشكل صريح عن موافقة الموقع على مضمون هذا السند[١]، أمّا في حال ورود التوقيع في مكان آخر، فليس من شأنه أن ينفي هذه الموافقة، إنّما يخضع لتقدير قاضي الموضوع.

وفي حالة تعدّد نسخ السند الواحد، وعدم توقيع كلّ نسخة على حدة، بل وضع التوقيع على نسخة واحدة، وبالكربون على بقيّة النسخ، فيُترك الأمر لقاضي الموضوع لتحديد مدى قابليّة النسخ الكربونية في الإثبات وتعتبر في هذه الحالة كبدء بيّنة خطيّة،

وفي حالة تعدّد أوراق السند واقتصار التوقيع على الصفحة الأخيرة من السند، فإنه يعود أيضًا في هذه الحالة لقضاة الموضوع مهمّة تحديد ما إذا كان مجموع الأوراق يشكّل كلًّا متكاملًا، بحيث ينسحب عليها جميعها التوقيع، أو ما إذا كان اجتماع هذه الأوراق قد تمّ بصورةٍ عارضة[٢].

الفقرة الثانية: التوقيع الإلكتروني

يتّجه عالمنا اليوم شيئًا فشيئا إلى التخلّي عن الواقع الملموس ليصل إلى واقع افتراضي، وقد طال هذا التحوّل كافّة القطاعات فبدأنا نشهد انتشارًا واسعًا للعملات الرقميّة أهمّها Bitcoin و Etherium وغيرها،

حتّى إنّ الفنّ قد تأثّر بهذا التطوّر فبدأنا نلمس تخلّي بعض الفنانين عن الدعامة الورقية أو القماش الكتاني (Canvas) ليحلّ محلّه الفنّ الرقمي أو ما يعرف بالـ و NFT وهي اختصار لـ non-fungible tokens أو رموزٍ غير قابلةٍ للاستبدال[٣]. وبطبيعة الحال، فإنّ هذا التطوّر قد طال أيضًا التعامل التجاري فازدهر التعاقد عن بُعد عبر شبكة الإنترنت، لذا ظهرت الحاجة لتوقيع إلكتروني من شأنه أن يؤمّن وظائف التوقيع العادي أو اليدوي.

وكانت بداية استعمال هذا التوقيع في المعاملات المصرفية، عن طريق استعمال الرقم السرّي، ومن ثمّ بدأت تتطوّر هذه التقنيات وقد بدأ تنظيمها وقوننتها في تسعينيات القرن الماضي. ويطرح التوقيع الإلكتروني على

---

[١] إدوار، عيد، المرجع السابق، ص.١٠٦.

[٢] إدوار، عيد، المرجع السابق، ص. ١٠٨.

[٣] سيد، محمد، ما هي الـ NFT أو NFTs؟ كيف تعمل؟ كيف تنشأها وتبيعها؟، عبر الرابط التالي: https://tech-echo.com/2021/09/nft-what-is-nfts-crypto-how-work-create-sell-buy/، تمّ الإطلاع عليه بتاريخ: ١٠-٠٧-٢٠٢٢.

بساط البحث عدّة إشكاليّاتٍ وتساؤلاتٍ أبرزها مدى استجماعه لشروط التوقيع التقليدي. وسنبحث أدناه تعريف التوقيع الإلكتروني (أولا") وصوره (ثانيًا).

أولاً: تعريف التوقيع الالكتروني

اختلفت التعريفات المعطاة للتوقيع الإلكتروني نظرًا لتنوّع الأسس المعتمدة للتعريف، فمنهم من اعتمد لتعريف التوقيع على وظيفته ومنهم من استند على وسيلة تنظيمه.

وسنتطرّق أدناه لتعريف التوقيع الإلكتروني على صعيد المنظمات الدولية والإقليمية كذلك في القوانين الوضعية وتعريفاته الفقهية.

١. تعريف المنظّمات الدوليّة للتوقيع الالكتروني

حظي التوقيع الإلكتروني باهتمامٍ كبيرٍ على المستويين التشريعي والفقهي، وقد كثّفت المنظّمات الدوليّة جهودها، بهدف تذليل الصعوبات التي تواجه المعاملات الإلكترونية بشكلٍ عام، والتوقيع الإلكتروني بشكلٍ خاصّ، وإصدار إرشاداتٍ وتوصياتٍ لتأمين حلول ناجعة تستهدي بها التشريعات الوطنيّة عند وضعها للنصوص القانونية التي ترعى قواعد الإثبات،

وقد تمحورت هذه التوصيات على تحديد مفهوم جديد ومتطوّر للكتابة التي لم تعد تقتصر على الكتابة الخطّية التقليدية بل توسّع مفهومها لتشمل الكتابة الإلكترونية، بالإضافة إلى السعي لمساواة التوقيع الإلكتروني بالتوقيع الخطّي.

وسنحصر بحثنا أدناه بالجهود الدولية المبذولة بهذا الخصوص على المستويين الدولي والإقليمي بلجنة الأمم المتحدة للتجارة الدولية[1]، الإتّحاد الأوروبي وفي القانون العربي الاسترشادي للإثبات بالطرق الحديثة.

أ. تعريف قانون الأونسيترال النموذجي

[1] تعرف باللغة الفرنسية: Commission Des Nations Unies Pour Le Droit Commercial International (CNUDCI)،
كما تعرف بالإنكليزية: United Nations Commision For International Trade (UNCITRAL)

عرّفت الفقرة "أ" من المادة ٢ من قانون الأونسيترال النموذجي[١] التوقيع الالكتروني، بأنّه "عبارة عن بيانات في شكل الكتروني مدرجة في رسالة بياناتٍ، أو مضافة إليها أو مرتبطة بها منطقيًا، يجوز أن تستخدم لتعيين هويّة الموقّع، بالنسبة إلى رسالة البيانات ولبيان موافقة الموقّع على المعلومات الواردة في رسالة البيانات".

ب. تعريف الاتحاد الأوروبي للتوقيع الالكتروني

ميّز التوجيه الأوروبي رقم 93/1999/CE[2] تاريخ ١٩٩٩/١٢/١٣ بين نوعين من التوقيعات الالكترونية وهما:

- التوقيع الالكتروني البسيط أو العادي
- التوقيع الالكتروني المتقدّم أو المعزّز

فعرّفت الفقرة الأولى من المادة ٢ التوقيع الالكتروني العادي بأنه "معلومة في شكل الكتروني مرتبطة أو متصلة منطقيا ببيانات الكترونية أخرى، تستخدم كأداة للتوثيق"، أمّا الفقرة الثانية من المادة ٢ أعلاه فقد عرّفت التوقيع الإلكتروني المعزّز وهو التوقيع الذي تتوافر فيه الشروط التالية:

- أن يحدّد هوية الموقع ويمكّن من التعرف عليه.
- أن يكون مرتبطا بشخص صاحبه.
- أن يتمّ إنشاؤه بوسائل تضمن السرّية التامّة، وتمكن الموقع من الاحتفاظ بها، ووضعها تحت مراقبته وسيطرته وحده دون غيره.

---

[١] قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية مع دليل الإشتراع، ٢٠٠١، منشورات الأمم المتحدة، رقم المبيع A.02.V.8، تمّ تحميله بصيغة PDF، عبر الرابط التالي:
https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/ar/ml-elecsig-a.pdf
تمّ الاطلاع عليه بتاريخ: ٠٦-٠٢-٢٠٢٢.

[2] DIRECTIVE 1999/93/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques (JO L 13 du 19.1.2000, p. 12), telechargé en version PDF du site: https://eur-lex.europa.eu/legal-content, Consulté le: 06-02-2022.

– أن يكون مرتبطا بالبيانات التي يلحق بها بشكل يجعل أي تغيير أو تعديل في المستقبل على تلك البيانات قابلاً للكشف عنه".

وقد جرى لاحقًا إلغاء التوجيه أعلاه ليحلّ محلّه لائحة eIDAS خدمات تحديد الهوية والمصادقة والائتمان الإلكترونية) رقم ٢٠١٤/٩١٠[1] ابتداءً من ٣٠ حزيران ٢٠١٦، التي تهدف إلى بثّ الثقة في التعاملات الإلكترونية والإشراف على عمليات مصادقة التوقيع الإلكتروني وأختام التوقيع وخدمات التوصيل المسجلة والختم الزمني من أجل تنظيم عملية التوقيع على المستندات بجعلها مريحة وآمنة.

وقد أبقت هذه لائحة eIDAS على الأنواع الثلاثة للتوقيع الإلكتروني السالفة الذكر، مضيفة إليها نوعًا جديدًا وهو التوقيع الإلكتروني المؤهّل.

ج. التوقيع الإلكتروني المؤهّل

بحسب أحكام الفقرة ١٢ من المادة ٣ من لائحةeIDAS ، إنّ التوقيع الإلكتروني المؤهل هو توقيع إلكتروني متقدّم يتم إنشاؤه باستخدام جهاز إنشاء توقيع إلكتروني موصوف، حدّدت شروط اعتماده في الملحق رقم ٢ من اللائحة أعلاه، ويستند على شهادة مؤهلة للتوقيعات الإلكترونية.

د. تعريف التوقيع الإلكتروني في القانون العربي الاسترشادي للإثبات بالطرق الحديثة:

عرّف القانون العربي الاسترشادي للإثبات بالطرق الحديثة[2]، المُصادق عليه من قبل مجلس وزراء العدل العرب بموجب القرار ذات الرقم 24 د / 771 تاريخ ٢٠٠٨/١١/٢٧ ، التوقيع الإلكتروني في الفقرة الثالثة من مادّته الأولى بأنّه:

---

[1] RÈGLEMENT (UE) Nº 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, Publié au JO L, Nº L 257/73,28/8/2014, telechargé en version PDF du site: https://eur-lex.europa.eu/legal-content, Consulté le: 06-02-2022.

[2] القانون العربي الإسترشادي للإثبات بالتّقنيّات الحديثة، تمّ إعتماده من قبل مجلس وزراء العدل العربن قرار رقم ٧٧١/د٢٤، بتاريخ ٢٠٠٨/١١/٢٧، عبر الرابط التالي:

http://www.protectionproject.org/wp-content/uploads/2013/12/proofing-by-new-technology.docx، تمّ الإطلاع عليه بتاريخ: ٠٨-٠٨-٢٠٢٢.

"ما يوضع على محرّر إلكتروني ويتّخذ شكل حروف أو أرقام أو إشارات أو غيرها، ويكون له طابع منفرد يسمح بتحديد شخص الموقّع ويميّزه عن غيره"

٢. تعريف التوقيع الإلكتروني في الفقه والتشريع

لم تتأخّر التشريعات الوطنية لسنّ نصوص بغية الاعتراف بالتوقيع الإلكتروني، فبعض الدول قد لجأت لوضع قوانين خاصّة في هذا المجال، وبعضها أجرى تعديلات على النصوص القائمة، وسنستعرض أدناه تعريف التوقيع الإلكتروني وفق ما جاء في القوانين الأجنبية والعربية .

أ. في القانون الفرنسي

عرّف المشرّع الفرنسي التوقيع الالكتروني، في البند الثاني من الفقرة الرابعة من المادة ١٣١٦ من القانون المدني الفرنسي المعدّلة بموجب القانون رقم ٢٣٠-٢٠٠٠[1]، والتي أضحت المادة ١٣٦٧ بعد تعديلها بموجب القرار رقم ٢٠١٦-١٣١ تاريخ ٢٠١٦/٢/١٠، الذي تبنّى توجيه eIDAS ، بأنّه:

"استخدام طريقة موثوق بها لتمييز هوية صاحبه و ضمان ارتباطه بالتصرف القانوني المقصود[2]."

---

[1] Loi n° 2000-230 du 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, avec toutes ses modifications disponible sur le web: https://www.legifrance.gouv.fr/, consulté le: 08-02-2022.

[2] Article 1316-4:

La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.

Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.

يستنتج من هذا التعريف، أن المشرّع الفرنسي ركّز على وظيفة التوقيع الإلكتروني، فاعتبر أنّ كلّ توقيع يحقّق وظيفة التوقيع العادي هو توقيعٌ صحيحٌ مشترطًا توفّر قدرٍ كافٍ من الثقة واتّصال التوقيع أو المستند المرتبط به.

ب. تعريف التوقيع الالكتروني في القوانين العربية

يلاحظ أن أغلب التشريعات العربيّة، التي نظّمت التجارة والتوقيع الالكتروني، حرصت على وضع تعريفٍ للتوقيع الالكتروني وسنستعرض أدناه التعريفات الواردة في كلّ من القوانين المصري والتونسي واللّبناني.

- **تعريف القانون المصري**

عرّف المشرع المصري التوقيع الالكتروني، في الفقرة (ج) من المادة الأولى من القانون الخاص بتنظيم التوقيع الالكتروني رقم ٢٠٠٤/١٥[١] تاريخ ٢٠٠٤/٤/٢٢ بأنّه "ما يوضع على محرر الكتروني ويتّخذ شكل حروفٍ وأرقام أو رموزٍ وإشارات أو غيرها، ويكون له طابع متفرد يسمح بتحديد شخص الموقّع، ويميّزه عن غيره".

ومن مراجعة هذا التعريف نلاحظ أنّ المشرّع المصري لم يحصر التوقيع الالكتروني بصورةٍ معيّنة إنّما جاء شاملا" بهذا الخصوص فاعتبر أنّ التوقيع يمكن أن يتّخذ شكل حروفٍ أو أرقامٍ...

كذلك حدّد المشرّع المصري الخصائص والشروط الواجب توافرها في التوقيع الالكتروني، بغية منحه الحجّية في الإثبات القانونية، والتي تتمثّل في طابع المتفرّد وتحديد التوقيع لشخصية الموقّع وإمكانية تمييزه عن غيره، ومن الملاحظ أنّ المشرّع المصري لم يأتِ على ذكر وظيفة أساسية للتوقيع الالكتروني التي تتمثّل في التعبير عن إرادة الموقّع وموافقته على مضمون السند.

- **تعريف القانون التونسي**

[١] القانون رقم ٢٠٠٤/١٥ تاريخ ٢٠٠٤/٤/٢٢، المتعلّق بتنظيم التوقيع الالكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، تمّ تحميله بصيغة PDF عبر الرابط التالي: https://manshurat.org/node/13789، تمّ الاطلاع عليه بتاريخ: ١٠-٠٢-٢٠٢٢.

لم يعطِ القانون التونسي رقم ٢٠٠٠/٨٣[١] تاريخ ٢٠٠٠/٨/٩ المتعلّق بالمبادلات والتجارة الالكترونية تعريفًا مباشرًا للتوقيع الالكتروني فاكتفى بتحديد العناصر المؤدية إلى إحداثه، وقد نصّ الفصل الخامس من القانون المذكور على ما يلي:

"يمكن لكل من يرغب في إمضاء وثيقة الكترونية إحداث إمضائه الالكتروني بواسطة منظومة موثوق بها، يتم ضبط مواصفاتها التقنية، بقرار من وزير الاتصالات".

كذلك نجد أنّ المشرّع التونسي قد أورد في الفقرة ٦ من الفصل ٢ تعريفًا لمنظومة إحداث التوقيع الالكتروني معتبرًا أنّها:

"مجموعة وحيدة من عناصر التشفير الشخصيّة، أو مجموعة من المعدات التي تمكن من التدقيق في الإمضاء الالكتروني".

- **تعريف القانون اللبناني**

عرّفت الفقرة الثالثة من المادة الأولى من القانون رقم ٢٠١٨/٨١[٢] التوقيع بأنّه "التوقيع اللازم لاكتمال عمل قانوني يعرف بصاحبه، ويثبت رضاه عن العمل القانوني المذيّل بالتوقيع"، ونجد أنّ ما نصّ عليه المشرّع اللبناني في هذا المجال لا يأتلف مع طبيعة التوقيع الإلكتروني بل ينطبق على التوقيع التقليدي.

فعبارة "المذيّل بالتوقيع" تتعلّق بالتوقيع التقليدي الذي أثبتنا سابقًا في دراستنا أنّ السند الورقي يقتضي أن يوقّع في ذيله بغية الاعتداد به،

---

[١] القانون التونسي رقم ٢٠٠٠/٨٣ تاريخ ٢٠٠٠/٨/٩ المتعلّق بالمبادلات والتجارة الالكترونية، تمّ تحميله بصيغة PDF عبر الرابط التالي:
https://www.justice.gov.tn/fileadmin/medias/Textes_et_documents/References_juridiques/L_2000_83_ar.pdf ، تمّ الاطلاع عليه بتاريخ ١١-٠٢-٢٠٢٢.

[٢] قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي اللبناني رقم ٢٠١٨/٨١ تاريخ ٢٠١٨/١٠/١٠، تمّ تحميله بصيغة PDF عبر الرابط التالي: https://www.bdl.gov.lb/files/laws/Law81.pdf، تمّ الاطلاع عليه بتاريخ: ١١-٠٢-٢٠٢٢.

فعبارة الذّيل تعني بحسب المعجم[1] "آخِرُ كلِّ شيء" وبطبيعة الحال إنّ واقع التوقيع الإلكتروني لا يتناسب مع هذا الأمر باعتبار أنّ التوقيع هو جزء من السند الالكتروني لا يمكن فصله عنه أو تحريك مكانه.

وتجدر الإشارة إلى أنّه وقبل إقرار القانون اللبناني المذكور كانت النائب الدكتورة غنوة جلّول قد سبق وتقدّمت باقتراح قانون بتاريخ ٢٠٠١/١٠/٩، مقتبث من قانون الأنسيترال النموذجي، وقد نصّ هذا المشروع على تعريفٍ واضحٍ للتوقيع الإلكتروني والذي يعني بحسب الفقرة الأولى من المادّة الثانية من اقتراح القانون المذكور "بيانات في شكلٍ إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيًّا، يجوز أن تُستخدم لتعيين هويّة الموقّع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقّع على المعلومات الواردة في رسالة البيانات."

كذلك سبق للنائب ياسين جابر أن تقدّم باقتراح قانونٍ بتاريخ ٢٠٠١/١١/٢٦ وقد نصّت المادة ١٤٢ مكرّر ٥ من هذا الإقتراح على ما حرفيّته:

"يعتبر التوقيع الالكتروني قائمًا حين تُستخدم وسائل أو إجراءات موثوقٌ بها من شأنها تأمين التعريف بصاحب التوقيع وتأكيد الصّلة بين التوقيع وبين السند الذي يقترن به.

تحدّد بمراسيم تصدر عن مجلس الوزراء بناءً على اقتراح وزير العدل، الشروط التي تنظّم إجراء التوقيع الالكتروني وتحدّد الأسس التي تضمن تأكيد هويّة الموقّع وسلامة السند، في هذه الحالة، تُعطى الوسائل والإجراءات المستخدمة في التوقيع موثوقيّة مفترضة حتّى إثبات العكس."

- **تعريف الفقه للتوقيع الالكتروني**

تباينت التعريفات الفقهية المعطاة للتوقيع الالكتروني، فقد عرّفه بعض الفقهاء معتبرًا إيّاه بمثابة بديلٍ لتوقيع التقليدي "التوقيع الناتج عن اتباع إجراءات محددة – تؤدي في النهاية – الى نتيجة

[1] معجم المعاني الإلكتروني، عبر الرابط التالي:
https://www.almaany.com/ar/dict/ar-ar/%D8%B0%D9%8A%D9%84/، تمّ الاطلاع عليه بتاريخ: ٠١-٠٧-٢٠٢٢).

معروفة مقدّمًا ، ويكون مجموع هذه الإجراءات هو البديل الحديث للتوقيع بمفهومه التقليدي"[1]. وقد عرّفه البعض الآخر بأنّه "كلّ إشارات أو رموز أو حروف مرخّص بها من الجهة المختصّة باعتماد التوقيع ومرتبطة ارتباطًا وثيقًا بالتصرّف القانوني تسمح بتمييز شخص صاحبها وتحديد هويّته، وتتمّ دون غموض من رضاه بهذا التصرف القانوني[٢]"

ويّلاحظ أنّ هذا التعريف قد تناول البنية التقنيّة للتوقيع الالكتروني من جهة ومن جهة أخرى تناول ضرورة توافر شروط قانونية للتوقيع من حيث قدرته على التعريف بهوية الموقع والتعبير عن رضاه بمضمون العمل القانوني المثبت بصيغة الكترونية.

كما عرّف البعض الآخر[٣] التوقيع الالكتروني بأنّه "كلّ إشارات أو رموز أو حروف مرخّص بها من الجهة المختصّة باعتماد التوقيع ومرتبطة ارتباطًا وثيقًا بالتصرّف القانوني، تسمح بتمييز شخص صاحبها وتحديد هويته، وتتمّ دون غموض، عن رضاه بهذا التصرّف القانوني. ويلاحظ أنّ هذا التعريف يشدّد من جهة على تأمين التوقيع الالكتروني لشروط التوقيع التقليدي ومن جهة أخرى لا يغفل إجراءات إصدار التوقيع وتوثيقه.

ثانياً: صور التوقيع الإلكتروني

تختلف صور التوقيع الإلكتروني بحسب الوسيلة أو الطريقة المستعملة للتوقيع، كذلك تتباين هذه الصور أو الأنواع من حيث درجة الأمان والموثوقية التي تؤمّنها وذلك ناتج عن الإجراءات والتقنيات المعتمدّة في كلّ من هذه الصور. وسنبيّن أدناه أبرز صور التوقيع الإلكتروني.

١. التوقيع الالكتروني المرقمن

---

[1] محمد المرسي، زهرة، الدليل الكتابي وحجية مخرجات الكومبيوتر في الاثبات في المواد المدنية والتجارية – من بحوث مؤتمر القانون والكومبيوتر والانترنت – ١-٣ أيار – جامعة الامارات العربية المتحدة –ص ٢١.

[2] C. DEVYS, Du sceau numérique à la signature numérique, Rapp. OJTI, nov.1995, pub.in OJTI, ss dir. C. –DHENIN, Vers une administration sans papiers, Paris, La documentation française, 1996, p. 96.

[٣] ثروت، عبد الحميد، التوقيع الإلكتروني– ماهيته– مخاطره وكيفية مواجهتها– مدى حجيته في الإثبات، دار الجامعة الجديدة، مصر، ٢٠٠٧، ص. ٥٠.

يتمّ تحويل التوقيع اليدوي المكتوب إلى توقيع إلكتروني عن طريق استعمال الماسح الضوئي (scanner). وبعد أن يتمّ تحويله إلى ملف معلوماتي يمكن إضافته إلى أي مستند يراد التوقيع عليه. إلاّ أنه ورغم سهولة هذه التقنية فقد أجمع الفقه والإجتهاد أنها لا تحقّق الأمان الكافي للتعامل إذ يمكن لأيّ كان خلق آلية توقيع عائدة لشخص آخر إذا كان يمتلك نموذجا" عن توقيعه اليدوي[١].

وقد قُضيَ في فرنسا أن التوقيع المنقول عبر الماسح الضوئي لا يعتبر توقيعًا إلكترونيًا[٢] كونه لا يؤمّن رابطا بين الموقّع والسند باعتبار أنّه لا يثبت موافقة الشخص على مضمون هذا المستند ولا سلامته، وقد خلصت محكمة استئناف Besançon[3] لاعتبار هذا النوع من التوقيع كأثر بياني أو عنصر مؤسس لبدء بيّنة أكثر مما يمكن اعتباره كتوقيع حقيقي[٤].

ومما لاشكّ فيه أنّ هذا النوع من التوقيع لا يتمتّع بأيّة درجةٍ من درجات الأمان التي يمكن أن تحقّق الثقة اللّازمة في التوقيع، إذ أن المرسل إليه يستطيع أن يحتفظ بنسخة عن صورة التوقيع ويعيد لصقها على أيّة وثيقة من الوثائق المستندة إلى وسيط الكتروني.

٢. التوقيع باستخدام القلم الإلكتروني

تتمّ هذه الطريقة عن طريق كتابة الموقّع لتوقيعه الشخصي باستخدام قلم إلكتروني خاصّ على شاشة جهاز الإعلام الآلي، ويتمّ التحقق من صحّة التوقيع عن طريق برنامج خاصّ بالإستناد إلى حركة القلم والأشكال التي يتّخذها من انحناءات ودوائر أو إلتواءات[٥]، وبالتالي إنّ إدخال التوقيع يتمّ بطريقة مشابهة للتوقيع العادي إذ يقوم الموقّع بالتوقيع مستعملا القلم الخاصّ بالشكل نفسه الذي يقوم به عادة بالتوقيع العادي على الدعامة الورقية.

وتتميّز هذه التقنية بالمرونة والسهولة إلا أنّها تواجه مشكلة أساسية تتمثّل بصعوبة إثبات الصلة بين التوقيع والسند كذلك، وكما حال التوقيع الالكتروني المرقمن أعلاه، يمكن للمرسل إليه الاحتفاظ بنسخة من التوقيع الذي سبق واستلمه وأن يستعمل هذا التوقيع مستقبلا بغية الاستفادة من منافع دون وجه حقّ[٦].

---

[١] وسيم، الحجار، الإثبات الإلكتروني، المنشورات الحقوقية صادر، بيروت، ٢٠٠٢، ص ١٨٦.

[2] Cass. 2e civ., 28 mai 2020, n° 19-11.744, Bull, disponible sur le site: https://www.legifrance.gouv.fr ,consulté le: 01-07-2022.

[3] CA Besançon, ch soc. 20 oct 2000; SARL Chalets Boisson c/Gros: Jurisdata n° 2000-125582.

[4] Cass. 2e civ 30 avril 2003, 00-46.467, Bull 2003 II N° 118 p. 101.

[٥] طارق، حمزة، النقود الإلكترونية كإحدى وسائل الدفع- تنظيمها القانوني والمسائل الناتجة عن استعمالها، منشورات زين الحقوقية بيروت،٢٠١١، ص. ٣٩٩.

[٦] ثروت، عبد الحميد، المرجع السابق، ص. ٥٥.

٣. التوقيع باستخدام الخواصّ الذاتية أو التوقيع البيومتري

يعتمد هذا النوع من التوقيع على استخدام خصائص فيزيائية فريدة في كلّ شخص، وهذه الخصائص من شأنها تمييز صاحبها والتعريف عنه، وتشمل هذه الطرق:

- فحص بصمة الإصبع
- مسح الأوعية الدموية العائدة لشبكة العين أو قزحية العين
- التحقّق من طبقة ونبرة الصوت
- فحص شكل اليد الهندسيش
- التحقق من ملامح وتقسيمات الوجه
- فحص ديناميكية خطّ اليد في التوقيع.

يتمّ تخزين الخواصّ أعلاه داخل الدائرة الإلكترونية للجهاز المُراد التعامل معه بحيث لا يمكن أن يستجيب للشخص إلاّ بعد النطق بكلمات محدّدة أو بوضع البصمة[١].

نظرًا لفرادة هذه الخواص وارتباطها بشكلٍ وثيقٍ بصاحبها، يجري استثمارها للدخول إلى غرف محميّة أو خزائن كما في التحقيقات الجنائية[٢]. كذلك تستعمل بشكل كبير في العديد من الشركات والإدارات الرسمية لتحلّ محلّ التوقيع العادي للأجير أو الموظف كونها أكثر فعاليّة لارتباطها الوثيق بالشخص الموقّع ولعدم إمكانيّة تزويرها بسهولة. وبالفعل نجد مثلا" في لبنان أنّ نظام التوقيع ببصمة الإصبع معمولٌ به ف بعض الوزارات والإدارات العامة مثل وزارة المالية وذلك لإثبات حضور الموظفين، وهناك سعي من التفتيش المركزي لتعميم هذا الأمر على كافّة الدوائر الرسمية.

يصطدم استعمال هذا النوع من التوقيع الإلكتروني بكلفته العالية فضلا" عن وجوب تأمين جهاز خاصّ يهدف إلى ترقيم هذه الخواصّ الذاتية، كذلك يمكن لهذه الخواصّ أن تتغيّر مع الوقت، لذا يفضّل كثيرون تجنّب استعمال هذا النوع من التواقيع.

ويرى بعض الفقهاء أنّه ورغم نجاح التقنيات أعلاه بإثبات هويّة الموقّع إلا أنّه ليس بالضرورة أن تثبت رضاه على العمل القانوني موضوع توقيعه[٣]، إذ يمكن أن يتمّ إرغام شخص على البصم مثلا" أو تقليد البصمة (البصمات البلاستيكية أو المطاطية) أو تسجيل صوته على آلة تسجيل.

٤. التوقيع باستخدام الرقم السرّي Pin Code

---

[١] طارق، حمزة، المرجع السابق، ص. ٣٩٨.

[2] D.Gobert et E. Montero, op. Cit, p. 7.

[3] D.Gobert et E. Montero, op. cit.

هو أبسط أنواع التوقيع الإلكتروني والأكثر شيوعًا لدى الجمهور، فهو لا يتطلّب عناءً كثيرًا لاستعماله أو خبرةً معيّنة. ويتمّ توثيق المراسلات والتعاملات الإلكترونية باستخدام مجموعة من الأرقام أو الرموز التي يختارها صاحب التوقيع لتحديد شخصيته ولتشكّل رمزًا سريًا خاصًّا به[١].

يُفترض أن يبقى الرمز السرّي المذكور معلومًا فقط من صاحبه أو ممّن يبلغه به وغالبًا ما يرتبط استعماله ببطاقات الدفع الممغنطة والبطاقات ذات الشريحة الإلكترونية كبطاقات الائتمان. ومن أبرز الأمثلة العملية والأكثر شيوعًا للتوقيع الرقمي هو اعتماد المصارف اللبنانية الرقم السرّي في ميدان الخدمات المصرفية الإلكترونية، وقد نصّت العقود، التي يطلب من العملاء توقيعها، صراحة على اعتبار الرمز السي بمثابة توقيع إلكتروني يتمتّع بكافة خصائص التوقيع العادي.

ونظرًا لأهمية هذا النوع من التوقيع وسهولة استعماله، أصدر مصرف لبنان القرار الأساس رقم ٧٥٤٨ تاريخ ٢٠٠٠/٣/٣٠[٢]، الذي نظّم خلاله عملية التوقيع الإلكتروني عبر استعمال الرمز السرّي فاعتبر انّ الرقم الشخصي (Personal Identification Number PIN) هو بمثابة التوقيع الالكتروني لعملية سحب الاموال من الصراف الآلي، على أن تطبق على العمليات المالية والمصرفية المنفّذة بالوسائل الالكترونية القوانين والقواعد التي ترعى العمليات المنفّذة بالوسائل العادية.

كذلك صدر عن وزير المالية القرار رقم ١/٤٥٣ تاريخ ٢٠٠٩/٤/٢٢، يتعلّق بتحديد دقائق تطبيق أحكام المادة ٣٨ من قانون الإجراءات الضريبية والمتعلّقة بأصول وشروط التسجيل واستعمال النظام الضريبي الإلكتروني، وقد تمّ اعتماد المفتاح الشخصي الإلكتروني E-pin ليحلّ محلّ التوقيع العادي ويرتّب ذات المفاعيل القانونية.

تتميّز هذه الصورة من التوقيع الإلكتروني بقدرٍ كبيرٍ من الثّقة والأمان خاصّة في حال اقترانها باستعمال بطاقة ممغنطة صادرة عن مؤسسة ائتمانية أو مصرف التي تسعى دائمًا لتطوير أنظمة حمايتها. وهذا الأمان مردّه أنّ العمليّة القانونية لا تتمّ إلاّ إذا اجتمع إدخال البطاقة في جهاز السحب الآلي (ATM) أو أجهزة نقاط البيع (POS) مع إدخال الرقم السرّي الخاصّ بالمستخدم الذي لا يعلم به أحد غيره، كذلك في حال فقدان البطاقة المصرفية أو نسيان الرقم السري أو علم أحد آخر به دون رغبة صاحبه، فيستطيع هذا الأخير تجميد كافّة العمليات التي تتمّ بواسطة هذه البطاقة عن بمجرّد إعلام المصرف بذلك، علمًا أنّ معظم المصارف تولي اهتمامًا كبيرًا بهذا الأمر عن طريق تخصيص خطٍّ ساخن على مدى ٢٤ ساعة طيلة أيّام الأسبوع. فضلاً عن ذلك فإنّ عمليات السحب أو الإيداع التي تتمّ عن طريق البطاقة الممغنطة

---

[١] طارق، حمزة، المرجع السابق، ص.٣٩٧.

[٢] تمّ تعديله بموجب القرار الوسيط رقم ١١٤٤٥ تاريخ ٢٠١٣/٦/٦.

المقترنة بالرقم السرّي يتمّ إثباتها على ثلاثة أنواع من المخرجات على شريط ورقي موجود خلف جهاز السحب على أسطوانة ممغنطة[١].

ورغم ذلك، يعتقد بعض الفقهاء[٢] أنّه في حال استحصال شخص ثالث على البطاقة الممغنطة مع الرقم السرّي دون علم أو رغبة صاحبها، فإنّ التوقيع الإلكتروني في هذه الحالة لا يفيد بهويّة الشخص الموقّع بل بهويّة من يتحمّل نتائج العمليّة التي تمّت بالشكل أعلاه كون المبالغ المسحوبة سوف يتمّ حسمها من حساب صاحب البطاقة.

وفي هذا السياق اعتبرت محكمة التمييز الفرنسية[٣] أنّ إثبات صحّة عمليّة مصرفية يمكن أن يتمّ عن طريق استعمال بطاقات مصرفية مقترنة بتوقيع سرّي طالما أنّ المدين، حامل البطاقة، لم يؤمّن دليلا على حصول خداع أو اختلالٍ وظيفي في النظام المعلوماتي العائد للمصرف، ولنا عودة لهذا القرار لاحقًا من دراستنا.

٥. التوقيع بواسطة إعطاء الامر بالموافقة على اتمام العقدعن طريق استخدام شبكة الانترنت

بعد انتشار التجارة الإلكترونية بشكلٍ هائلٍ في عالمنا اليوم، أنشأت العديد من الشركات مواقعا" الكترونية لها، أو لجأت إلى عرض بضائعها على مواقع عامة مثل eBay، AliExpress وغيرها ,فيتمكن بالتالي الزبائن من التسوق عبر الانترنت. ويتمّ الموافقة على عملية الشراء بمجرد الضغط (click) على مفتاح "OK" أو "accept" أو بما يماثلها. وبمجرّد القيام بهذا الأمر يعتبر تعبيرًا صريحًا عن الإرادة.[٤]

أمّا العقبات التي يواجهها هذا النوع من التوقيع فهو أنّه قد يقوم بعض زوار الانترنت بالضغط على زر "الموافقة" دون أن تكون لهم النيّة في التعاقد، لذا تلجأ معظم الشركات بالطلب من العميل إدخال رقم بطاقة ائتمانه بغية التأكّد من جدّيته.

فضلا" عن التجارة، تقوم العديد من الإدارات الحكومية بإتمام معاملاتها عبر شبكة الانترنت دون الحاجة إلى الحضور شخصيا" , وقد بدأ استعمال هذه الخدمة في لبنان كمعاملات وزارة الاقتصاد مثلا" التي يمكن

---

[١] محمد المرسي، الزهرة، المرجع السابق، ص. ٩٦.

[2] E.CAPRIOLI, Le juge et la preuve électronique, Réflexions sur le projet de loi portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique , texte présenté au colloque de Strasbourg, "Le commerce électronique : vers un nouveau droit", 8-9 octobre 1999,disponible sur le site: www.caprioli-avocats.com, consulté le: 20-05-2022.

[3] CA Montpellier, 17e ch., sect. D, 9 avril 1987, JCP., éd. G., II, n° 20984

[٤] رانيا، صليبا، المرجع السابق، ص. ١١٠.

إجراؤها عبر الموقع الخاصّ بالوزارة[١]، فيتمّ من بعدها إرسال رسالة نصّية لطالب الخدمة فور إنجازها ليتمكّن من استلامها.

٦. التوقيع الرقمي

إنّ التوقيع الرقمي هو أبرز أنواع التوقيع الإلكتروني وأكثرها موثوقيّة وأمانًا وفعاليّة. وبحسب المادة ٣-٣-٢٦ من المواصفات القياسية العالمية (ISO) رقم ٢- ٧٤٩٨، الصادرة عن المنظمة الدولية للمواصفات والمقاييس، فإنّه يقصد بالتوقيع الرقمي بيانات أخرى أو صياغة منظومة بصورة شيفرة (Code)، والذي يسمح للمرسل إليه إثبات مصدرها والتأكّد من سلامة مضمونها وتأمينها ضدّ أي تعديل أو تحريف[٢].

يرتكز التوقيع الرقمي على معادلاتٍ رياضية باستخدام اللوغاريتمات أو الخوارزميات التي تستند على تقنية التشفير. والتشفير نوعان:

أ. تشفير متماثل حيث يتمّ استعمال نفس المفتاح من أجل تشفير المعلومات وفكّ تشفيرها.

ب. تشفير غير متماثل حيث يستعمل مفتاحين مختلفين أحدهما للتشفير والآخر لفكّ التشفير، ولنا عودة للبحث بتفاصيل تقنيّة التشفير في الفصل الثاني من دراستنا.

بعد التوقيع باستعمال مفتاحٍ معيّن لتشفير الرسالة يقوم المرسل إليه إلى فكّ التشفير للحصول على المعلومات الصرفة الأصلية. يستخدم في تقنية التشفير غير المتماثل ما يعرف بالوظيفة التداخلية أو Hash Function وهي آلية تخلق نوعًا من ملخّص للرسالة يكون بحجم أقلّ منها بكثير ويتميّز بكومه وحيدًا لكلّ رسالة، ولا يمكن استعادة الرسالة الأصلية من هذا الملخّص أو حتّى استنتاجها منه[٣] إذ يهدف فقط لإثبات عدم حصول أي تلاعب بمضمون الرسالة.

ويرى البعض[٤] أنّ موثوقية السند الالكتروني ترتبط بشكلٍ وثيقٍ بالتوقيع الرقمي خاصّة في حال تضمّن هذا التوقيع وظيفة الهاش (مثال SHA-256)، التي تسمح من التثبّت من موثوقية الرسالة أو الملف الموقّع.

أمّا بالنسبة للمراحل والإجراءات المتّبعة لإرسال رسالة رقمية موقّعة بالتوقيع الرقمي، فهي التالية:

- بدايةً يحدّد المرسل الرسالة المنوي توقيعها وإرسالها، ثمّ يستعمل الوظيفة التداخلية لإجراء ملخّص للرسالة أعلاه.

---

[١] عبر الرابط التالي: portal.economy.gov.lb

[2] P. Le tourneau – Contrats informatiques et électroniques –Dalloz Reference- 2ème edition,Paris 2002, p. 391.

[٣] وسيم، حجار، المرجع السابق، ص ١٨٩ وما بعدها.

[4] E. Caprioli, Signature électronique et dématerialisation, éditions Lexis Nexis,Paris 2014, P. 77.

- بعدها يقوم المرسل بتشفير الرسالة مستعملا مفتاحه الخاصّ، ثمّ يضيف توقيعه الإلكتروني المتمثّل بالملخّص أعلاه والمفتاح العام، ويرسل بعد ذلك الرسالة المشفّرة والموقّعة بالشكل المذكور إلى المرسل إليه.
- بعد استلامه الرسالة يقوم المرسل إليه بفكّ التشفير مستعملا المفتاح العام العائد للمرسل فيحصل على الملخّص السالف الذكر.
- كذلك يقوم المرسل إليه باختزال (أو تلخيص) نصّ الرسالة الأصلية عن طريق استخدام نفس الدالة الهاشية المستخدمة من قبل المرسل.
- يمكن بعد ذلك للمرسل إليه التثبّت من محتوى الرسالة الأصلية ولم يتمّ التلاعب بمحتواها عن طريق مقارنة قيمة الإختزال في التوقيع الرقمي مع ناتج الإختزال الذي استحصل عليه.

ويشرح الرسم البياني الملحق كيفية عمل التوقيع الرقمي[1].

الباب الثاني: الفرق بين التوقيع التقليدي والتوقيع الإلكتروني

يهدف كلا التوقيعان التقليدي أو العادي والإلكتروني إلى تحقيق الغاية نفسها وهي إثبات هويّة الموقّع ورضاه، إلا أنّ هذا الأمر لا يمنع من توافر عدّة اختلافات بينهما. وهذه الخلافات سنعالجها في الفقرة الأولى أدناه، كما سنتناول في الفقرة الثانية حجيّة التوقيع الالكتروني وموقف القوانين الوضعية واجتهادات المحاكم من منحه قيمةً منوازيةً للتوقيع اليدوي في مجال الإثبات.

الفقرة الأولى: الإختلافات بين التوقيع التقليدي والتوقيع الإلكتروني

يُعتبر التوقيع الالكتروني صورةً رقميةً للتوقيع العادي إلا أنّه لكلّ منهما خصائصه المادية (أولا")، كذلك يختلفان من الناحية العملية والمعنويّة (ثانيًا).

أولاً: الإختلاف من الناحية المادّية

يمكن تلخيص الإختلاف فيما بين التوقيع العادي والإلكتروني من الناحية المادّية بمسألتين الأولى تتعلّق بالشكل الخاصّ لكلّ منهما والثانية بالدعامة المختلفة التي يتمّ تدوينهما عليها:

١. لناحية الشكل

[1] ملحق رقم ١: رسم بياني بعنوان: كيفيّة عمل التوقيع الالكتروني.

إنّ صور التوقيع العادي تقتصر على الإمضاء بشكلٍ أساسي إضافة إلى بصمة الأصابع والختم كما سبق بيانه في الفقرات السابقة من دراستنا،

أمّا التوقيع الإلكتروني فتختلف صوره وأشكاله، لذا فإنّ معظم التشريعات لم تتطلّب صورةً معيّنة لهذا التوقيع بل أجازت أن يتّخذ صورة حروف أو أرقام أو رموز أو إشارات أو حتى أصوات شرط أن يتميّز بطابع التفرّد وبشكل يسمح بتمييز صاحب التوقيع وإثبات هويته وبيان رغبته ورضاه على العمل القانوني وموافقته على مضمونه[١].

٢. لناحية الدعامة

يختلف التوقيعان العادي والإلكتروني عن بعضهما من حيث الوسيط أو الدعامة، فالتوقيع التقليدي يتمّ على دعامة ماديّة ملموسة وهي في الغالب دعامةً ورقية، فتذيّل بالتوقيع لتتحوّل هذه الدعامة إلى مستند صالح للإثبات.

أمّا التوقيع الإلكتروني فيتمّ إنشاؤه إمّا كليًّا أو جزئيًا عن طريق أجهزة الحاسب الآلي. ويتّخذ التوقيع الإلكتروني عدّة صورٍ كما سبق بيانه، فمصداقية التوقيع الإلكتروني لا ترتبط بالركيزة المادّية بحدّ ذاتها، مثل حالة ملف رقمي محفوظ على اسطوانة ممغنطة ثمّ يتمّ نقله إلى القرص الصلب العائد للحاسوب ومنه عبر شبكة الإنترنت، ففي هذه الحالة استمدّ التوقيع مصداقيته من الآلية التقنية التي يعتمد عليها وليس من الركيزة المادّية[٢].

ثانياً: الاختلاف من الناحية العملية والمعنويّة

يختلف التوقيع الإلكتروني عن التوقيع اليدوي التقليدي أيضًا من الناحية العمليّة بحيث يمكن للأوّل تحقيق وظائف يعجز الثاني عن تحقيقها، كذلك يختلفان من الناحية المعنوية إذ يتيح التوقيع العادي إمكانية اختيار الموقّع لشكل توقيعه وهو أمرٌ لا يمكن للتوقيع الالكتروني تحقيقه.

١. لناحية الوظيفة

لقد سبق وعالجنا في إطار دراستنا لأهداف الوقيع العادي أنّه يتمتّع بثلاث وظائف وهي تحديد هويّة صاحب التوقيع، تمييز شخصيته والتعبير عن رضاه بمضمون العمل القانوني.

---

[١] ثروت، عبد الحميد، المرجع السابق، ص ٥١.

[٢] وسيم، الحجار، المرجع السابق، ص. ١٥٠.

أمّا بالنسبة للتوقيع الإلكتروني، فتكمن أهمّيته وتميّزه عن التوقيع العادي بإمكانيّة التثبّت من مضمون السند الإلكتروني وعدم تعرّضه لأيّ تعديلٍ أو حذف، وذلك عن طريق ربط التوقيع بالسند بحيث يقتضي الاستحصال على توقيع جديد من أجل القيام بأي تعديل لاحق[١].

فضلاً عن ذلك يمنح التوقيع الإلكتروني المستند صفة " الأصلي"[٢] وهذه الوظيفة هي ضرورية وأساسية بالنسبة للسند ذي التوقيع الخاصّ، والتوقيع هو الذي يعطي السند صفة الأصل. وفي حالة السند الورقي يمكن تمييز الأصل بشكلٍ سهل إذ يكون في هذه الحالة غير موقّع توقيعًا حيًّا. أمّا بالنسبة للسند الإلكتروني فمتى كان التوقيع مقترنًا بالمستند وأُثبتَت صحّة هذا التوقيع، وحتّى لو تمّ نسخ هذا المستند تُعطى النسخة أيضًا صفة المستند الأصلي[٣].

٢. لناحية حرّية الإختيار

يؤمّن التوقيع العادي للموقّع حرّية اختيار شكل توقيعه وكيفيّة كتابته، أمّا التوقيع الإلكتروني وبما أنّه يتمّ عن طريق خوارزميات حسابية معقّدة تتمّ عن طريق برامج معلوماتية متخصّصة تتطلّب في بعض أشكال التوقيع وأكثرها موثوقية تدخّل شخص ثالث يعرف "بمقدّم خدمات المصادقة " والتي سنتطرّق لاحقًا خلال دراستنا لدورها ومسؤوليتها. وبالتالي فإنّ الإجراءات المذكورة تشكّل قيودًا على حريّة الشخص باحتيار توقيعه أو تغيير شكل هذا التوقيع.

الفقرة الثانية: حجيّة التوقيع الإلكتروني في المرحلة السابقة لإقرار التشريعات المنظّمة له

عارض بعض الفقهاء مساواة التوقيع الإلكتروني بالتوقيع التقليدي متذرّعين بعدّة حجج أبرزها عدم قدرة الموقّع معرفة مضمون الالتزام بصورةٍ أكيدة حتّى يمكن الاحتجاج به بوجهه، كما إنّ التوقيع الإلكتروني ليس صادرًا عن صاحب التوقيع بل عن شخصٍ ثالث ممّا يخلق شكوكًا لدى مستقبل الرسالة حول حضور المرسل الجسدي وراء خط الاتصال الإلكتروني، إضافة إلى أنّه، ونتيجة غموض آلية التوقيع وارتباطها بنظام مغلق، يمكن للموقّع سيء النيّة الزعم بعدم معرفة آلية التوقيع لمحاولة التنصّل من التزاماته[٤].

---

[١] ثروت، عبد الحميد، المرجع السابق، ص. ٥٣.

[2] D.Gobert et E. Montero, La signature dans les contrats et les paiements électroniques : l'approche fonctionnelle Publié au DA/OR, avril 2000, n° 53, P 7.

[٣] مشيمش، ضياء، التوقيع الإلكتروني – دراسة مقارنة، المنشورات الحقوقية صادر، بيروت ٢٠٠٢، ص ١٥٦.

[4] X.Linant de Bellefonds et A. Hollande, Droit de l'informatique et de la Télématique, 2ème édition, Masson, Paris, 1990, P. 143.

في مقابل ذلك، يعتقد البعض أنّ تزوير التوقيع اليدوي هو أسهل بكثير من اكتشاف الرمز السرّي لبطاقة الدفع المصرفية أو مفكّ رموز مفتاح تشفير عمومي أو نقض شهادة إلكترونية صادرة عن مرجعية موثوق بها[١]، وباستطاعته أن يؤمن مزيداً من الثقة والأمن عبر مقدّمي خدمات المصادقة المعترف بهم دوليًا[٢].

كذلك، ولتسليط الضوء على مدى درجة الأمان الذي يوفّره التوقيع الإلكتروني، يعطي البعض[٣] مثلا أنّ مفتاح إعلان الحرب النووية هو عبارة عن رقم يتمّ فكّ رموزه بواسطة الكومبيوتر.

طرحت مسألة إمكانية قبول الإثبات الإلكتروني جدلا واسعًا في الفقه والإجتهاد لا سيّما في المرحلة السابقة لإقرار قوانين وضعيّة تنظّم هذه المسألة بشكل واضح ودقيق، ففيما رفض البعض قبول وسائل الإثبات الإلكترونية، حاول البعض الآخر تليين قواعد الإثبات التقليدية وتطويعها بغية الإعتراف بالتوقيع والمستندات الإلكترونية، وهو ما سنبيّنه أدناه.

أولاً: العقبات التي واجهت الإعتراف بالتوقيع الإلكتروني

شكّلت وسائل الإثبات التقليدية عقبة أمام الاعتراف بالركائز الإلكترونية وحجيتها، ويمكن اختصار هذه العقبات القانونية بما يلي:

١. طبيعة السند التقليدي

إنّ معظم القوانين اللاتينية (كالقانون اللبناني والفرنسي) تفرض شرط الكتابة لإثبات الأعمال القانونية التي تتجاوز نصابًا معينًا، كما تنصّ على عدم إمكانية إقامة الدليل المعاكس على عقدٍ خطي إلا بعقدٍ أو وثيقةٍ بالصيغة الخطّية نفسها.

والمقصود بالصيغة الخطّية وفق المفهوم التقليدي هو السند الأصلي أو العقد ذو التوقيع الخاصّ المتجسّد في مستند ورقي وممهور بتوقيع ناتج عن فعل يدوي للإنسان، وبالتالي فإنّ الكتابة في ظلّ النظام التقليدي تجعلنا غير قادرين على الاعتراف بالمعاملات الإلكترونية على اعتبار أنّها محصورة في المظهر المادي

---

[١] طوني، عيسى، التنظيم القانوني لشبكة الانترنت: دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية، صادر للمنشورات الحقوقية، بيروت ٢٠٠١، ص ٣١٢.

[٢] نادر، شافي، التوقيع الالكتروني،الاعتراف التشريعي به وتعريفه القانوني وشروطه وأنواعه والمصادقة عليه، منشور على الموقع التالي:https://www.lebarmy.gov.lb/ar/content ، تمّ الإطلاع عليه بتاريخ: ٠٥-٠٧-٢٠٢٢.

[٣] محمد المرسي، زهرة، المرجع السابق، ص. ٢٥.

فقط. فضلاً عن ذلك، فإنّ معظم القوانين الوضعية قد اشترطت توفّر الكتابة بغية إثبات الأعمال القانونية كونها تؤمّن المساواة بين الأطراف وتعدّ دليلا مسبقًا للإثبات يتّصف بالثبات[١].

٢. اشتراط التوقيع

إنّ التوقيع ورغم كونه أداةً قانونية تقليدية وشائعة لم يتمّ تعريفه من قبل معظم القوانين التقليدية، فالكلّ يعرف ماهيته، حتى يمكن القول أنّ تبنّي التوقيع من جانب طفل صغير تشكل عنصرًا مهمًّا على تنشئته الاجتماعية وعن عبوره القريب إلى المراهقة، والتوقيع لا يقتصر على كونه علامة من الموقّع الذي يلتزم بعمل قانوني ما، بل إنّ التوقيع هو أيضًا بل هو دليل مرئي يفيد موافقته على التزاماته الواردة في السند الموقّع من قبله[٢].

وقد خلق التطوّر التكنولوجي فجوةً بين الواقع والقانون في ما يختصّ بالتوقيع، فالقانون يتطلّب أن تكون الكتابة موقّعة توقيعًا مكتوبًا بيد الموقّع حتّى تكون لها القوّة الثبوتية الكاملة، بينما يتّجه الواقع إلى معالجة البيانات بالوسائل الإلكترونية التي لا يمكن تطويعها بسهولة مع التوقيع المكتوب[٣].

٣. القوة الثبوتية للمستندات الإلكترونية

إنّ البناء القانوني لقوانين الإثبات التقليدية اقتصر على دعائم مادّية كالورق، فاستند بالتالي على فكرة الكتابة التي لها مدلولٌ مادّي بحت. وقد سعى البعض إلى توسيع مفهوم الكتابة ليشمل الوسائل التقنية الحديثة إلا أنّ هذه المعلومات قد اصطدمت بمشكلة توثيق وتخزين المعلومات الكترونيًا بشكلٍ موازٍ للسندات الصادرة عن طريق الوسائل الورقية التقليدية[٤].

وقد اعتبرت محكمة التمييز اللبنانية في هذا السياق أنّه ليس من عائق قانوني يمنع من اعتماد التسجيل الصوتي كوسيلة إثبات[٥]، كذلك اقرّت محكمة التمييز الفرنسية بصحّة التنازل عن دين مرسل عن طريق الفاكس معتبرةً أنّ سند قبول الرجوع عن دين مهني يمكن أن ينشأ ويحفظ على أي دعامة بما في ذلك الفاكس طالما أنّه ليس من نزاع حول مضمون السند وصدوره عن صاحبه[٦].

---

[١] المعتصم بالله، أدهم، دراسة بعنوان الإثبات الإلكتروني في ضوء قانون المعاملات الإلكترونية رقم ٢٠١٨/٨١، مجلّة الجامعة العربية، ص ٢.

[2] T. Piette-Coudol, Signature electronique, Ed. Litec, Paris 2001, p. 7

[٣] أدهم، المعتصم بالله، المرجع السابق.

[٤] رانيا، صليبا، المرجع السابق، ص. ٩٨.

[٥] محكمة التمييز الجزائية، الغرفة السادسة، قرار رقم ١، تاريخ ١٩٩٧/١/١٤، كساندر ١٩٩٧، عدد ١، ص ٤٠.

[6] Cass, com, 2 décembre 1997, JCP G 1998, P 905.

وتطرح مسألة الإثبات القانوني مشكلة تأمين أمن المعلومات ومنحها الضمانات الكافية كي لا تكون عرضةً للتلاعب من قبل مخترقي نظم المعلوماتية. فعلى سبيل المثال تعرّض لبنان لهجوم في صيف عام ٢٠١٢ طال نظامه المصرفي عن طريق الفيروس"Gauss" الذي مسّ أكثر من ٢٥٠٠ حاسوب في المنطقة، وتحديداً في لبنان[١]، لذا لا بدّ من تأمين وسائل متطوّرة تضمن موثوقية السند الإلكتروني وعدم تعرّض محتواه لأي تلاعب. ويبرز في هذا الإطار دور شخص ثالث أو جهة معتمدة تعرف بمقدّم خدمات المصادقة والتي يدخل في صلب مهامها تثبيت مضمون السند الالكتروني والحؤول دون إمكانية حصول تلاعب بمندرجاته، ولنا عودة لدور هذه السلطات في الفصل الثاني من دراستنا.

٤. مبدأ عدم جواز اصطناع الشخص دليلا" لنفسه

اصطدم الإثبات الإلكتروني بالمبدأ القانوني الذي ينصّ على عدم جواز اصطناع الشخص دليلاً لنفسه، وهذا المبدأ غير منصوص عليه في القوانين الوضعية إنّما يستنتج من قواعد العدالة وروح القوانين، فالكتابة التي يعتدّ بها كدليل إثبات هي تلك التي تصدر عن الخصم وليست ما يصطنعها الشخص ويدوّنها بنفسه ولنفسه[٢].

لذا فإنّ المبدأ المذكور يقف عقبةً في وجه الإثبات الإلكتروني باعتبار أنّ الحاسب الآلي يخضع لإرادة الجهة المستخدمة له الذي يعود إليها إدخال المعلومات التي تريد. كذلك يمكن أن يكون طرفا العقد غير متكافئين من حيث الخبرة في إبرام العقود وتوقيعها بشكلٍ إلكتروني، فيمكن بالتالي للطرف المحترف أن يقوم بتسجيل العقود المبرمة من قبله على ركائز إلكترونية تمكّنه من استرجاعها وقت يشاء بخلاف الطرف غير المحترف الذي يمكن أن يدلي بمواجهة خصمه بالمبدأ القانوني أعلاه[٣].

ثانياً: الإستثناءات القانونية المتعلّقة بالإثبات

نصّت كافّة التشريعات التي تعتمد مبدأ الإثبات المقيّد على بعض الاستثناءات التي يمكن فيه اثبات الأعمال القانونية بكافّة وسائل الإثبات، فيمكن بالتالي اللّجوء إلى شهادة الشهود والقرائن والخبرة.

ويمكن تلخيص هذه الاستثناءات بما يلي:

١. في المعاملات التجارية

---

[١] حسن، شقراني، فيروس في المصارف، الموقع الإلكتروني لجريدة الأخبار، تاريخ ١١ أب ٢٠١٢، عبر الرابط التالي: https://www.al-akhbar.com/Community/73896 تمّ الإطلاع عليه بتاريخ 2022-3-2

[٢] ضياء، مشيمش، المرجع السابق ص ٢٦.

[٣] المعتصم بالله، أدهم، المرجع السابق، ص ٤.

تقوم المعاملات التجارية على أساس السرعة والثقة فيما بين التجّار، وهذا ما يستدعي تبسيط وسائل الإثبات لعدم عرقلة سرعة الإجراءات التي تتطلّبه المعاملات التجارية.

ويسود مبدأ حريّة الإثبات في الأعمال التجارية متى كان طرفيها من التجّار، فيمكن بالتالي لأي فريق في العقد التجاري أن يجابه الإثبات الخطي الذي يدلي به خصمه بوسائل الإثبات الحرّ دون أيّ تفريق في درجات طرق الإثبات المنصوص عليها في القانون المدني. ويتمتّع القاضي في هذه الحالة بسلطة تقديرٍ واسعة فيمكنه مثلا" صرف النظر عن إثباتٍ خطّي لاعتماد وسيلة إثباتٍ أخرى كبيّنة القرائن[١].

أمّا في الحالة التي يكون فيها أحدهما تاجرًا، فإنّ مبدأ حرّية الإثبات يطبّق فقط على من كان التصرّف تجاريًا بالنسبة إليه، وهذا الأمر ينطبق على قسمٍ كبيرٍ من الأعمال التجارية التي تحصل عن طريق الإنترنت حيث يغلب عليها الطابع المختلط إذ يكون البائع وحده تاجرًا ، فيستفيد المشتري بالتالي من مبدأ حرية الإثبات، ويمكنه التمسّك بالمستند الإلكتروني المسجّل على وسيط غير ورقي أو بالنسخة الورقيّة التي يتمّ طباعتها منه[٢].

٢. في التصرّفات القانونية التي لا تزيد قيمتها عن نصاب محدّد

حدّدت معظم التشريعات نصابًا محدّدًا بحيث تخضع كافّة الأعمال القانونية التي تقلّ قيمتها عن هذا النصاب لمبدأ حريّة الإثبات، فالمشرّع اللبناني قد حدّدها بمبلغ خمسمائة ألف ليرة[٣] وقد بلغت ١٥٠٠ يورو في التشريع الفرنسي[٤] وخمسمائة جنيه في القانون المصري[٥] و ١٠٠٠ دينار في القانون التونسي[٦]، ويمكن بالتالي الأخذ بالسند الإلكتروني بغية إثبات الأعمال القانونية التي تقلّ قيمتها عن النصاب المحدّد.

٣. اعتبار المستندات الإلكترونية بدء بيّنة خطّية

نصّت الفقرة الثالثة من المادة ٢٥٧ أ.م.م.[٧] على جواز الإثبات بشهادة الشهود مهما كانت قيمة المدعى به في حال وجدت بداءة بينة خطّية أي كتابة ولو خالية من التوقيع صادرة عن الخصم المحتجّ بها عليه أو عمّن يمثّله تجعل وجود التصرّف المدعى به قريب الاحتمال.

---

[١] الياس، ناصيف، الكامل في قانون التجارة، الجزء الأول، عويدات للطباعة والنشر، بيروت ١٩٩٩، ص ٤٢٦.

[٢] رانيا، صليبا، المرجع السابق ص ٤٥.

[٣] مادة ٢٥٤ أ.م.م

[44] Décret nº 2004-836 du 20 Août 2004.

[٥] مادة ٦١ من قانون الإثبات .

[٦] فصل ٤٧٤ من مجلة الالتزامات والعقود.

[٧] معدّلة وفقا للمرسوم الاشتراعي ٢٠ تاريخ ١٩٨٥/٣/٢٣.

ويقابل هذه المادة نصّ المادة ١٣٤٧ من القانون المدني الفرنسي والمادة ٦٢ من قانون الإثبات المصري، ويتّضح من مراجعة هذه النصوص أنّه للأخذ ببداءة البيّنة الخطّية يقتضي توافر ثلاثة شروط وهي التالية:

- وجود دليلٍ كتابي: ومصطلح الكتابة ينصرف إلى أوسع معانيه إذ يشمل كلّ سند وليس بالضرورة المرتبط بدعامة ورقية[١].
- صدور الدليل عن الخصم المحتجّ بها عليه أو من يمثّله أي الوكيل أو الخلف العام أو الخاصّ.
- أن تجعل البيّنة التصرّف مرجّح الوجود.

وقد عارض بعض الفقهاء مبدأ إعطاء الدليل الإلكتروني صفة بدء البيّنة الخطّية معلّلين ذلك أنّه بحسب مفهوم اللغة الرقمية فإنّ الآلة بشكلها الإلكتروني لا تصدر نسخًا أصليّة يمكن تفريقها عن النسخ المستنسخة عنها[٢] ، اذ تؤلف هذه النسخ تكراراً تاماً للأصل وتكون بدورها قابلة للاستنساخ غير المحدود، وبدء البينة الخطية قد وجد بقصد تسهيل الاثبات في الحالات التي تقتضي العدالة ذلك وبغية جعل نظام الاثبات اكثر مرونة. فلا يمكن بالتالي جعل هذا الأمر مصدراً للالتفاف على قواعد الاثبات وإزالتها تحت ستار التفسير. فالتفسير يهدف إلى اعطاء النصّ ابعاده القانونية وليس إلى تحميله اكثر ممّا يحتمل[٣].

٤. حالة استحالة الحصول على دليل خطّي

نصّت الفقرة ٤ من المادة ٢٥٧ أ.م.م. [٤] على جواز الإثبات بشهادة الشهود في حال استحال على الدائن الحصول على سند خطّي. لم تفرّق المادة أعلاه بين الاستحالة المادية أو المعنوية التي عدّدت بعض حالتها على سبيل المثال لا الحصر، فهي تتحقّق نتيجة ظروف نفسيّة أو أدبية ناتجة عن علاقة القربى أو المودّة كالعلاقة بين الأصول والفروع أو بين الزوجين أو حتّى بين الخطيبين، أو بحسب العرف المتّبع في بعض المهن.

أمّا الاستحالة المادّية فتتمثّل بظروف خارجية استثنائية شأنها حرمان أحد المتعاقدين من الاستحصال على دليل خطّي، كالكوارث الطبيعيّة وغيرها... وبكلّ الأحوال يعود للقاضي أمر تقدير توافر هذه الظروف.

---

[١] ضياء، مشيمش، المرجع السابق، ص ٣٣.

[٢] طوني، عيسى، المرجع السابق، ص١٩٧.

[٣] سامي، منصور، الاثبات الالكتروني في القانون اللبناني: معاناة قاض، العدل عدد ١، ٢٠٠١، ص ١٥٠.

[٤] يقابلها المادة ٦٣ من قانون الإثبات المصري والمادتين ١٣٤٨ و١٩٥٠ من القانون المدني الفرنسي.

وبالنسبة لمدى إمكانية تطبيق المبادئ السالفة الذكر على الوسائط الإلكترونية الحديثة، فبالنسبة للاستحالة المعنوية إنّ طبيعة التعاقد الإلكتروني وميزاته المتمثّلة بالسرعة والفعالية والكلفة تفرض الأخذ بهذه الاستحالة وأوضح مثال على ذلك هو شراء بطاقات السينما عن طريق الإنترنت [١].

وفيما خصّ الإستحالة المادّية، فنجد أنّ الفقه قد انقسم بهذا الخصوص فرأى جانبٌ منه أنّه يمكن الحكم بالاستحالة المادية بالنسبة للسندات الإلكترونية الحديثة التي، وبحكم طبيعتها، تجعل من المستحيل ابرام العقود بصيغة خطّية مكتوبة[٢].

عارض البعض هذه النظرية معتبرين أنّ الاستحالة المادّية لا يمكن أن تنطبق على الوسائل الإلكترونية كون سبب هذه الإستحالة ليس قوّةً قاهرة بل قرارًا إراديًا باستخدام الأساليب المعلوماتية[٣].

٥. حالة فقدان الدليل الكتابي

نصّت الفقرة الخامسة من المادة ٢٥٧ أ.م.م. على جواز الإثبات بشهادة الشهود مهما كانت قيمة المُدّعى به إذا ثبت فقدان السند الخطي بسببٍ أجنبي لا يد للخصم فيه[٤].

وبمقارنة نصّ المادة المذكورة مع نصّ المادة ١٣٤٨ من القانون المدني الفرنسي نجد أنّ النصّ الأخير قد جاء أوضح بهذا الخصوص إذ اشترطت توافر ثلاثة شروطٍ مجتمعة للأخذ بالبيّنة الشخصية كدليل للإثبات، وهذه الأسباب هي التالية:

- فقدان النسخة الأصلية
- مطابقة الصورة للأصل
- ثبات الصورة أي عدم إمكانية العبث بمحتواها بعد نسخها

وقد اعتبرت الهيئة العامة لمحكمة التمييز اللبنانية أنّ لصورة الشيك، بعد ضياع أصله، ولئن لم يكن للصورة الفوتوغرافية قيمة في الإثبات بصورة مستقلة بذاتها، وفق الرأي الراجح، فان القضاء والفقه يتّجهان

---

[١] ضياء، مشيمش، المرجع السابق، ص ٣٨.

[2] F. Chamoux, la loi du 13 juillet 1980, une ouverture sur de nouveaux moyens de preuve, JCP édition, 1981, II, 13491, n 20 et s.

[3] E. Caprioli, Preuve et signature dans le commerce électronique, droit et patrimoine, n° 53 Decembre 1997, p.56 et s.

[٤] يقابلها نصّ الفقرة "ب" من المادة ٦٣ من قانون الإثبات المصري و المادة ١٣٤٨ من القانون المدني الفرنسي.

إلى إعطائها حجّية تفوق حجّية الصورة الخطّية البسيطة وأنّها تعتمد كدليل ثبوتي أمام القضاء، وخلصت إلى اعتبارها دليل إثبات كامل بعد اقترانها برسالة إلكترونية[١].

وكون السند الإلكتروني ليس له نسخًا أصلية، كما سبق بيانه، فيرى البعض[٢] أنّ نسخ المعلومات الإلكترونية على أسطوانات رقمية (CD) يجعلها غير قابلةٍ للتغيير أي إنّها تتمتّع بالثبات، ما يدفع للقول باعتبارها بمثابة صور عن الأصل وبالتالي الاعتراف بها كوسيلة في الإثبات.

٦. الإثبات الإلكتروني على ضوء الاتفاقيات الخاصّة بالإثبات

نظرًا لسرعة التطوّر في المجال الإلكتروني، ونتيجة تردّد المشرّعين بسنّ قوانين تنظّم الإثبات الإلكتروني، لجأ كثيرون إلى إدراج بنود في الاتفاقيات الموقّعة من قبلهم تقرّ بصحّة الإثبات بالوسائل الرقمية، ولعلّ أبرز هذه الاتفاقيات كانت في القطاع المصرفي حيث لجأت معظم المصارف بالتوقيع على اتفاقيات مع زبائنها بغية تمكينهم من الاستحصال على بطاقة ائتمان أو للاستفادة من الخدمات المصرفية الإلكترونية، وسنبحث أدناه بمدى صحّة هذه الاتفاقيات، ومدى إمكانيتها إضفاء الحجية على الوسائل الإلكترونية.

أ. مدى صحّة اتفاقيات الإثبات

إنّ الاتفاقيات أعلاه تستند بداية على مبدأ سلطان الإرادة ، ويستند هذا المبدأ على حرّية الإنسان بالتعاقد وتحديد شروط تعاقده، فالإرادة هي مصدر الموجبات وللأفراد أن يرتّبوا علاقاتهم التعاقدية كما يشاؤون شرط أن يراعوا مقتضى النظام العام[٣]. وكذلك تستند هذه الاتفاقيات على النصوص الوضعية التي كرّست حقّ المتعاقدين بتنظيم علاقاتهم التعاقدية، كنصّ المادة ٢٥٤ أ.م.م والمادة ٦٠ من قانون الإثبات المصري، وعلى مبدأ عدم تعلّق وسائل الإثبات بالانتظام العام، عارض بعض الفقهاء فكرة هذه الاتفاقيات وقد طالب بعضهم باعتبارها باطلة.

وبالفعل فبرأي العلّامة السنهوري" إنّ الاتفاقيات المتعلّقة بكافّة قواعد الإثبات أو بتعيين من الخصوم يتحمّل عبء الإثبات هي باطلة"[٤]، كذلك يرى بعض الفقهاء، تأييدًا لهذه النظرية أنّه ولئن كانت قواعد

---

[١] الهيئة العامة لمحكمة التمييز، قرار رقم (٢٩) تاريخ ٢٠١٧/٤/٢٤، منشور في كساندر ٢٠١٧ ص ٥٦٤.

[٢] ضياء، مشيمش، المرجع السابق، ص ٤٢.

[٣] مصطفى، العوجي، القانون المدني، الجزء الأول، العقد، منشورات الحلبي الحقوقية، بيروت ٢٠٠٩، ص ١١٠.

[٤] عبد الرزاق، السنهوري، الوسيط في شرح القانون المدني، ج ٢، المجلد الأول، دار النهضة العربية، مصر ١٩٨٢، رقم ٥٩.

الإثبات لا تتعلّق بالانتظام العام إلا أنّه لا يجوز للاتّفاق على مخالفتها أن يحرم أحد الطرفين من الحقّ بالإثبات، فهكذا اتفاقيات تعدّ باطلة[١].

إلا أنّ محكمة النّقض المصريّة كان لها رأيًا مغايرًا بهذا الصدد فاعتبرت أنّ قاعدة عدم جواز الاثبات بالبيّنة في الأحوال التي يجب فيها الاثبات بالكتابة ليست من النظام العام فيجوز الاتّفاق صراحةً أو ضمناً على مخالفتها، ولقاضي الموضوع السلطة التقديرية في استخلاص القبول الضمني من سلوك الخصم[٢].

إلا أنّ الرأي الراجح في الفقه والاجتهاد قد أجمع على صحّة الاتفاقيات أعلاه مستندين إلى كون معظم تشريعات الإثبات في غالبية الدول تقضي بإمكانية تعديل قواعد الإثبات ما يعني أنّ هذه القواعد ليست متعلّقة بالانتظام العام.

ب. مدى إمكانية اتفاقيات الإثبات إضفاء الحجية على الوسائل الإلكترونية

تهدف اتفاقيات الإثبات إلى تحقيق المساواة بين المستندات الإلكترونية والمستندات الكتابية بمفهومها التقليدي، وقد نتج عن هذه المساواة قلب عبء الإثبات فصار زبون المصرف مثلا مضطرًا للبحث عن أدلّة تثبت عكس ما يدلي به المصرف.

يتّضح من خلال مراجعة بعض العقود التي تجريها المصارف مع عملائها أنّها لا تكتفي فقط بالنصّ على قبول الإثبات الإلكتروني بل جعلت من النظام الإلكتروني العائد للمصرف الدليل القاطع الوحيد للإثبات، وهذا ما يتبيّن جليًّا من مراجعة البند ٦-١ من نموذج العقد المعتمد من قبل بنك لبنان والمهجر بهذا الخصوص[٣].

وأمام هذا الواقع اعتبر كثيرون أنّ هذه الاتفاقيات تدخل ضمن إطار عقود الإذعان، وعقد الإذعان هو العقد الذي يقبل فيه المعروض عليه، دون مناقشة، بشروط مقررة يضعها الموجب. وعادة ما يتعلق، هذا العقد، بسلعة او حاجة او مرفق ضروري، يكون محل احتكار قانوني او فعلي، او تكون المنافسة محدودة النطاق في شأنه[٤].

إلاّ أنّ الرأي الراجح في الفقه والاجتهاد يفضّل عدم التشدّد في هذا الأمر ويوصي بالابتعاد عن التفسير الضيّق لعقود الإذعان باعتبار أنّ هذه العقود تتعلّق بالسلع أو الخدمات الضرورية التي تكون محلّ احتكار فعلي أو قانوني[٥].

---

[١] محمد المرسي، زهرة، المرجع السابق، ص ٣١ وما بعدها.

[٢] طعن مصري رقم ١٥٧، تاريخ ١٩٧٣/٤/٢٤، مكتب فني ٢٤ ج ٢ ق ١١٧ ص ٦٦٧، منشور في المستشار الإلكتروني.

[٣] ملحق رقم ٢: نموذج العقد المعتمد من قبل بنك لبنان والمهجر المتعلّق بالخدمات الإلكترونية.

[٤] الياس، ناصيف، موسوعة العقود المدنية والتجارية، الجزء الأول، مطبعة نمنم، ١٩٨٦ بيروت، ص ٤١.

[٥] ثروت، عبد الحميد، المرجع السابق، ص ١٠٨.

وقد تصدّت محكمة التمييز الفرنسية لهذه المسألة فاعتبرت في قضية CREDICAS الشهيرة، ففسخت قرار محكمة Sète معلّلة ذلك أنّ الفرقين قد اتّفقا على أنّ بمجرّد استعمال المقترض للبطاقة الممغنطة المصحوب بالرقم السرّي فإنّ ذلك يعني أمرًا موجّهًا إلى المؤسسة المالية بدفع ثمن المشتريات، وأنّ الفريقين قد حدّدا بذلك إجراءات الإثبات، فخلصت إلى اعتبار أنّ الاتفاق المذكور صحيحٌ لتعلّقه بالحقوق التي يملك الأفراد حقّ التصرّف فيها، واعتبرت أنّ محكمة Sète قد خالفت بقرارها المطعون فيه أحكام المادتين ١١٣٤ و ١٤١٣ من القانون المدني الفرنسي[1].

[1] Cass. 1ère civ., 8 nov. 1989, n° 86-16.197, Bull. 1989 I N° 342 p. 230.

المبحث الثاني: حجّية التوقيع الإلكتروني في القوانين الخاصّة وتطبيقاته

يهدف وضع التوقيع على مستندٍ معيّن إلى ترتيب آثارٍ قانونية. فالتوقيع، كما أسلفنا، يمكّن من تحديد هويّة الموقّع وصلاحياته. كذلك يعدّ وضع التوقيع إقرارًا من الموقّع بصحّة مضمون المستند.

وإذا كان الفقه الاجتهاد قد استقرّا على أنّ التوقيع اليدوي يمكنه تحقيق الأهداف أعلاه، فإنّ السؤال الذي يقتضي بحثه هو مدى حجيّة التوقيع الإلكتروني في مجال الإثبات بحسب أحكام التشريعات الدوليّة والمحلّية، وهذا ما سنتطرّق إليه في المبحث الأول.

ونظرًا للتطوّر المُذهل الذي تحقّق في ميدان المعاملات التجارية، فقد تشعّب استعمال التوقيع الإلكتروني الأمر الذي ساهم بتوفير النفقات وبتحقيق سرعة في تنفيذ هذه المعاملات، وهو ما سنبيّنه في المبحث الثاني أدناه.

الباب الأول: حجيّة التوقيع الإلكتروني

نتيجة استخدام التقنيات الحديثة في إبرام العقود برز دور التوقيع الإلكتروني في هذا المجال، وقد أثار التوقيع بشكله المذكور إشكاليّاتٍ عديدة، فتضاربت النظريات لناحية منحه حجيّة موازية لنظيره التقليدي،

وقد تبدّدت هذه الإشكاليات بعد إقرار تشريعاتٍ تنظّم التوقيع الإلكتروني وتضع ضوابط وشروط محدّدة لإنشائه وصحّته كما وتحدّد وسائل لحمايته وتعزيز موثوقيته، كلّ ذلك بغية توفير عنصري الثقة والأمان، ما أدّى إلى الإعتراف بحجيّة التوقيع المذكور في الإثبات ومساواته مع التوقيع العادي أو التقليدي.

وسنبحث أدناه بحجّية التوقيع الإلكتروني في النصوص.

الفقرة الأولى: حجّيّة التوقيع الإلكتروني في النصوص

لم يقتصر الاهتمام بقوننة التوقيع الإلكتروني وتطوير مفهومه على التشريعات المحليّة بل شكّل هذا الموضوع اهتمامًا بالغًا من قبل المنظّمات الدوليّة والإقليمية، وهذا ما سنبحثه أدناه.

أولاً: حجيّة التوقيع الإلكتروني في نصوص المنظمات الدولية

يعود الاهتمام الدولي للاعتراف بالتوقيع الإلكتروني والسندات الإلكترونية للعام ١٩٧٨ حيث نصّت الفقرة ٣ من المادة ١٤ من اتّفاقية هامبورغ المبرمة بتاريخ ١٩٧٨/٣/٣ على أنّ التوقيع على سند الشحن يمكن أيضًا أن يتمّ في شكل رمز (أو شعار)، أو أية وسيلة ميكانيكية أو إلكترونية، بدلاً من المستندات الورقية التقليدية[١].

كذلك، أصدرت لجنة الأمم المتّحدة للقانون التجاري الدولي في دورتها المنعقدة في العام ١٩٨٥ توصيةً للحكومات والمنظّمات الدولية بضرورة أن تعيد النظر بالقواعد التي تعيق استعمال المعلوماتية في الأعمال التجارية الدولية بغية السماح بنقل أو تحويل المستند الالكتروني المُتمثّل بالرسالة الالكترونية.[٢]

وسنحصر بحثنا بقانون الأونسيترال النموذجي والتوجيهات الأوروبية كونهما يشكّلان حجر الأساس الذي استندت عليه معظم الدول لسنّ التشريعات المتعلّقة بالتوقيع الإلكتروني.

١. قانون الأونسيترال النموذجي

حرصًا منها لتفادي أيّ تعارضٍ ممكن أن يحصل بين القوانين الوضعية في مجال التجارة الالكترونية، بذلت لجنة الأمم المتحدة للقانون التجاري الدولي جهودًا كبيرة لتضع في العام ١٩٩٦ مجموعة من القواعد القانونية المتعلقة بالتجارة الالكترونية الدولية، وصاغتها في شكل قانون نموذجي، كما قامت هذه اللجنة في دورتها الخامسة والثمانين المنعقدة بتاريخ ٢٠٠١/١/١٢ بوضع قانون الاونسيترال النموذجي المتعلق بالتوقيع الالكتروني الذي تضمّن اثنتي عشرة مادة[٣].

وقد أعطى هذا القانون الحجيّة المطلقة للتوقيع الإلكتروني الموثوق مساويًا إيّاه بالتوقيع التقليدي. وبالفعل فقد نصّت الفقرة ١ من المادة ٦ من القانون أعلاه على ما يلي:

---

[1] E.Caprioli, EDI et commerce électronique au regard des normes juridiques internationales, Lamy Contrats internationaux, Div. 2, Annexe 100/2-1,Paris, 1996,p. 63.

[2] E.Caprioli et I.Choukri, reflexions et perspectives autour de l'arbitrage international et du commerce electronique: vers une nouvelle gouvernance du contentieux? – p 107, disponible sur le site :

https://www.wgtn.ac.nz/, consulté le: 01-03-2022.

"عندما يشترط القانون وجود توقيع من شخص يستوفي ذلك الشرط بالنسبة إلى رسالة البيانات إذا استخدم توقيع إلكتروني موثوق بالقدر المناسب للغرض الذي أنشئت أو بلغت من اجله رسالة البيانات في ضوء كل الظروف بما في ذلك أي اتفاق ذي صلة"

وبحسب الفقرة ٣ من المادة عينها، يعدّ التوقيع موثوقًا في حال توافرت فيه الشروط التالية:

أ. كانت بيانات إنشاء التوقيع مرتبطة، في السياق الذي تُستخدم فيه، بالموقِّع دون أي شخص آخر؛

ب. كانت بيانات إنشاء التوقيع خاضعة، وقت التوقيع، لسيطرة الموقِّع دون أي شخص آخر؛

ج. كان أي تغيير في التوقيع الالكتروني، يُجرى بعد حدوث التوقيع، قابلا للاكتشاف؛

د. كان الغرض من اشتراط التوقيع قانونا هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع وكان أي تغيير يجرى في تلك المعلومات بعد وقت التوقيع قابلا للاكتشاف.

واللافت أنّ القانون أعلاه لم يضع أيّ قيودٍ على حجيّة التوقيع الإلكتروني وابتعد عن وضع تصنيفاتٍ للتواقيع الإلكترونية بل اكتفى بالإقرار بصحّة كافّة التواقيع التي تلبّي الشروط المنصوص عنها في الفقرة الأولى من المادة ٦ من هذا القانون. علمًا أنّ هذه الشروط لا تحدّ من قدرة أي شخص من إثبات قابلية أو عدم قابلية التعويل على التوقيع الالكتروني بأيّ طريقة أخرى وفق ما جاء في الفقرة ٤ من المادة أعلاه.

٢. حجيّة التوقيع الإلكتروني في التوجيهات الأوروبية

إنّ الجهود المبذولة في سياق تنظيم التجارة الإلكترونية والتوقيع الإلكتروني لم تقتصر فقط على المستوى الدولي، بل اتّجهت تكتلات إقليمية أخرى لتنظيم المعاملات الالكترونية كان أبرزها الاتحاد الأوربي الذي نجح بتاريخ ١٩٩٩/١٢/١٣ بإصدار التوجيه الأوروبي رقم 93/1993 بشأن التوقيع الالكتروني، الذي يتألّف من خمسة عشرة مادّة، عالجت كافّة الإشكالات التي يثيرها التوقيع الإلكتروني إن كان من حيث التعريف أو شروط الموثوقية، فضلا عن جهات التصديق الإلكتروني. وتضمّن هذا التوجيه أربعة ملاحق تتعلّق بالإجراءات والشروط الواجب توافرها من أجل تأمين الأمن التقني للتوقيع الإلكتروني.

وقد نصّت المادة الخامسة من التوجيه الأوروبي رقم ١٩٩٩/٩٣ تاريخ ١٩٩٩/١٢/١٣ على أنّ الدول الأعضاء تسهر على أن تكون التواقيع الإلكترونية المتقدّمة المستندة على شهادة مؤهلة والتي تمّ إنشاؤها عن طريق أجهزة إنشاء توقيع آمن:

أ. أن تستوفي هذه التواقيع المتطلبات القانونية فيما يتعلق بالبيانات الإلكترونية بنفس الطريقة التي يفي بها التوقيع بخط اليد بهذه المتطلبات فيما يتعلّق بالبيانات المكتوبة بخط اليد أو مطبوعة على الورق.

ب. تسهر الدول الأعضاء على الاعتراف بالتوقيع الإلكتروني

ومن خلال مراجعة هذه المادّة، نجد أنّها قد ميّزت بين التوقيع الإلكتروني المؤمّن والتوقيع الإلكتروني العادي أو البسيط، فأقرّت بحجيّة كاملة للنوع الأول، أمّا النوع الثاني فقد أوصت الدول الأول عدم إنكار دوره في الإثبات فتحتاج بالتالي حجّيته لإثبات موثوقيته أمام القضاء.

أمّا بالنسبة لأجهزة إنشاء التوقيع الإلكتروني الآمنة(SSCD) فيمكن تمييز نوعين منها:

- أجهزة محلية على سبيل المثال البطاقات الذكية وما إلى ذلك.
- أجهزة يمكن إدارتها عن بُعد من قبل مزوّد خدمات أجهزة إنشاء توقيع إلكتروني آمنة.

وقد تمّ لاحقًا إلغاء التوجيه السالف الذكر ليحلّ محلّه لائحة eIDAS الصادرة بالتوجيه رقم ٢٠١٤/٩١٠، التي أبقت على المبادئ نفسها أعلاه فيما يتعلّق بحجيّة التوقيع الإلكتروني إذ أوصت جميع الدول الأعضاء عدم رفض التوقيع غير المعزّز ومساواة التوقيع المؤهّل بالتوقيع الخطّي. وبالفعل فقد نصّت المادة ٢٥ من اللائحة أعلاه على أنّ الأثر القانوني وقبول التوقيع الإلكتروني كدليلٍ في الإثبات لا يمكن أن يتمّ رفضهما فقط بسبب أنّ هذا التوقيع يتمّ بشكلٍ الإلكتروني أو لعدم مراعاته لمتطلّبات التوقيع المؤهّل.

كذلك أكّدت الفقرة الثانية من هذه المادة وجوب منح التوقيع الإلكتروني المؤهل نفس الأثر القانوني للتوقيع الخطّي، في حين نصّت الفقرة الثالثة من المادّة عينها على الشروط الواجب توافرها لاعتبار التوقيع مؤهلا فاعتبرت أنّ التوقيع المؤهل الذي يستند على شهادة مؤهلة صادرة عن إحدى الدول الأعضاء يعتبر توقيعًا مؤهلا في كافّة الدول الأعضاء، أمّا المادة ٣٥ من هذه اللائحة فقد نصّت على عدم جواز نزع الأثر القانوني لأي توقيع إلكتروني أو منع الاعتداد به أمام المحاكم لمجرّد أنّه ليس توقيعًا إلكترونيًا متقدمًا أو مؤهلاً.

ثانياً: حجّية التوقيع الإلكتروني في القوانين الوضعية

سعت كافّة التشريعات التي نظّمت التوقيع الإلكتروني إلى تحديد الشروط الواجب توافرها للإعتراف بحجيّة التوقيع الإلكتروني ومساواته بالتوقيع اليدوي، وسنستعرض أدناه موقف القانون الفرنسي (فقرة أولى)، وموقف القانون المصري (فقرة ثانية)، وموقف القانون التونسي (فقرة ثالثة) وموقف القانون اللبناني (فقرة رابعة).

١. حجّية التوقيع الإلكتروني في التشريع الفرنسي

تدخّل المشرّع الفرنسي لإقرار حجيّة المستندات الإلكترونية بداية بشكلٍ جزئي عن طريق بعض النصوص التي عالجت حالات خاصّة مثل القانون ٨٣-٣٥٣ تاريخ ١٩٨٣/٤/٣٠، المتعلّق بإجازة استخدام وسائط إلكترونية بدلا" من الدفاتر التجارية التقليدية، وقد منح القانون الفرنسي الوسائط السالفة الذكر ذات الحجيّة التي تتمتّع بها الدفاتر التقليدية في الإثبات.

ونتيجة التطوّر الذي شهدته فرنسا في المعاملات الإلكترونية، والتزاما منه بالتوجيهات الأوروبية الخاصة بالتوقيع الالكتروني، عمل المشرّع الفرنسي على تعديل نصوص القانون المدني الخاصة بالإثبات، فصدر القانون رقم ٢٣٠-٢٠٠٠ بتاريخ ٢٠٠٠/٠٣/٣ الذي اعترف بحجيّة الكتابة الالكترونية إسوة بالكتابة الورقية، وقد لحظ هذا القانون مسألة الاعتراف بالتوقيع والكتابة الإلكترونية والإقرار بحجيّتهما في الإثبات ووضع ضوابط لضمان صحّتهما.

كذلك، قام المشرّع الفرنسي بتعديل نصّ المادّة ١٣٢٦ من القانون المدني بغية إزالة كلّ تمييز بين التوقيع اليدوي والالكتروني فاستبدل عبارة "التوقيع بخطّ اليد" لتصبح "التوقيع بواسطة الشخص". من ثمّ صدر المرسوم رقم ٢٧٢-٢٠٠١ بتاريخ ٣٠ مارس ٢٠٠١، الذي حدّد الشروط الواجب توافرها في التوقيع الالكتروني، حتى يكون موثوقا به، وميّز هذا المرسوم بين نوعين من التوقيعات الالكترونية:

أ. **التوقيع الالكتروني العادي:** الذي عرّفه بأنه" يعد توقيعا الكترونيا، كل معطى أو بيان ينتج عن استعمال أداةٍ تستجيب للشروط الواردة في البند الأول من الفقرة الأولى من المادة ١٣١٦/٤."

ب. **التوقيع الالكتروني المؤمّن:** وهو التوقيع الذي يجب أن تتوافر فيه الشروط التالية:

- أن يكون خاصًا بالموقّع.
- أن يتمّ إنشاؤه بوسائل يكون بإمكان الموقّع وضعها تحت مراقبته المطلقة.
- أن يؤمّن صلة وثيقة بالعقد الملحق به على نحو أن أي تغيير لاحق يمسّ العقد، يكون قابلا للكشف.

وبناءً لأحكام المادة الأولى[1] من المرسوم رقم ٢٠١٧-١٤١٦ تاريخ ٢٠١٧/٩/٢٨ فإنّ موثوقيّة عمليّة التوقيع الالكتروني مفترضة حتّى إثبات العكس عند توافر الشروط التالية:

[1]"La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en oeuvre une signature électronique sécurisée, établie grâce à un

- أن يكون التوقيع الالكتروني مؤمنا.
- أن يكون هذا التوقيع قد تم إنشاؤه بموجب منظومة آمنة لإحداث التوقيع الالكتروني.
- أن يكون التحقق من هذا التوقيع يقوم على استخدام شهادة الكترونية معتمدة.

وقد قضت محكمة التمييز الفرنسية[1] في هذا السياق أنّه ومن أجل اعتبار التوقيع الالكتروني مشتملا" على آلية آمنة، وعبر إجراءات موثوقة في التعريف تضمن اتّصال العمل القانوني بالتوقيع، يجب أن يكون مقترنًا بشهادة مصادقة الكترونية.

وخلافًا لهذا المبدأ، فقد قضت محكمة استئناف Nîmes[2] بنزاع عُرض أمامها متعلّق بإيجار تمويلي، أنّ التوقيع الالكتروني موضوع النزاع يسمح بتحديد هويّة مدير شركة المستأجر، وخلصت لاعتبار هذا التوقيع موثوقًا حتّى إثبات العكس. ويُعتبر هذا الإجتهاد متعارضًا مع أحكام المرسوم ٢٠١٧-١٤١٦ الذي نصّ أنّ التوقيع المؤهّل وحده الذي يتمتّع بقرينة الموثوقية حتى إثبات عكس هذا الأمر، ويظهر اتّجاهًا للإعتراف بالحجيّة الكاملة لأيّ توقيعٍ إلكتروني مهما كان نوعه.

٢. حجيّة التوقيع الإلكتروني في التشريع المصري

أصدر المشرّع المصري بتاريخ ٢٠٠٤/٤/٢٢ القانون رقم ٢٠٠٤/١٥ المتعلّق بتنظيم التوقيع الالكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، وقد أقرّ هذا القانون في المادة ١٤ منه القانون بحجيّة التوقيع الإلكتروني في الإثبات عند استخدامه في نطاق المعاملات المدنية والتجارية وكذلك الإدارية متى روعي في إنشائه وإتمامه الشروط المنصوص عليها في القانون المذكور والضوابط الفنية والتقنية التي تحدّدها اللائحة التنفيذية.

وقد ساوت المادة ١٥ من القانون المذكور بين حجيّة التوقيع الإلكتروني والتوقيع اليدوي، وبالعودة إلى الشروط الواجب توافرها لصحّة التوقيع الإلكتروني فقد حدّدتها المادة ١٨ من القانون السالف الذكر، وهي التالية:

أ. ارتباط التوقيع الإلكتروني بالموقّع وحده دون غيره

---

dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié."

[1] Cass. Civ. 1ère, 30 sept. 2010, N° 09-685555, BICC N° 734, 15 Janv. 2011.

[2] Cour d'appel de Nîmes CA Nîmes, 1re ch., 14 mars 2019, n° 17/03531, disponible sur le site: https://www.doctrine.fr/d/CA/Nimes/2019/C52D70AD1C86427FE2BCD, consulté le: 18-05-2022.

ب. سيطرة الموقّع وحده دون غيره على الوسيط الإلكتروني
ج. إمكانية كشف أي تعديل أو تبديل في بيانات المحرّر الإلكتروني أو التوقيع الإلكتروني.

أمّا بالنسبة للشروط التقنيّة والفنّية الواجب توافرها في التوقيع الإلكتروني فقد حدّدتها اللائحة التنفيذية للقانون أعلاه الصادرة بموجب قرار وزير الاتصالات وتكنولوجيا المعلومات رقم ١٠٩ تاريخ ٢٠٠٥/٥/٢٥ والتي جرى تعديلها بموجب القرار رقم ٣٦١ تاريخ ٢٠٢٠/٤/٢٣، بعد الأخذ بعين الإعتبار الإحتياجات التي كشف عنها التطبيق العملي لمنظومة إنشاء التوقيع الإلكتروني[١]، وقد استحدثت اللائحة التنفيذية الجديدة البصمة والختم الإلكترونيين فضلا عن إضافتها بعض الشروط التقنية.

وللأخذ بحجيّة التوقيع الالكتروني فقد نصّت المادة ٩ من اللائحة التنفيذية تاريخ ٢٠٢٠/٤/٢٣ على وجوب توافر الشروط التالية:

أ. أن يكون متاحًا فنيًا تحديد وقت وتاريخ إنشاء الكتابة الإلكترونية أو السندات الإلكترونية الرسمية أو العادية وأن تتمّ هذه الإتاحة من خلال نظام حفظ إلكتروني مستقلّ وغير خاضع لسيطرة منشئ هذه الكتابة أو لسيطرة المعني بها.
ب. أن يكون متاحًا فنيًا تحديد مصدر هذه الكتابة أو السندات ودرجة سيطرة منشئها على المصدر وعلى الوسائط المستخدمة في إنشائها.
ج. في حالة إنشاء وصدور الكتابة الالكترونية أو السندات الالكترونية بدون تدخّل بشري، جزئي أو كلّي، فإنّ حجّيتها تكون متحقّقة متى أمكن التحقّق من وقت وتاريخ إنشائها ومن عدم العبث بها.

ويتحقّق الشرط الأول بحسب أحكام المادة ١٠ من اللائحة التنفيذيّة الجديدة عن طريق التثبّت من مدى استناد التوقيع إلى منظومة مؤمّنة وفقًا لأحكام المواد ٢، ٣ و٥ من هذه اللائحة، إضافة إلى وجوب توافر أحد الشرطين التاليين:

أ. ارتباط التوقيع بشهادة تصديق صادرة عن جهة مرخّص لها أو معتمدة.
ب. أن يتمّ التحقّق من صحّة التوقيع من قبل الهيئة (هيئة تنمية صناعة تكنولوجيا المعلومات).

[١] أحمد، شرف الدين، ضوابط حجية المحررات الالكترونية في الإثبات تعليق على تحديثات اللائحة التنفيذية لقانون التوقيع الإلكتروني في ضوء أحكام محكمة النقض، المجلّة الدولية للفقه والقضاء والتشريع المجلد ٢، العدد ١ ،٢٠٢١، ص. ٩٤ – ١٠٣.

ويتحقّق الشرط الثاني من خلال التثبّت أنّ الموقّع هو الحائز والمسيطر على مفتاح التشفير الخاصّ، علمًا أنّ اللائحة الجديدة وبخلاف أحكام اللائحة القديمة بهذا الخصوص، فإنّها لم تشترط التحقّق من مدى توافر هذا الشرط عن طريق أدوات محدّدة.

أمّا بالنسبة للشرط الثالث، فيتمّ عن طريق استخدام نظام التشفير الغير متماثل المعتمد على المفتاحين العام والخاص، ومطابقة شهادة التصديق وبيانات إنشاء التوقيع بأصل الشهادة أو البيانات المذكورين أو بأيّ وسيلة أخرى مع مراعاة الضوابط المنصوص عنها في اللائحة الجديدة لاسيّما في المادة ٥ منها.

وقد استخلصت محكمة النقض المصرية، في سياق بحثها حجيّة المستندات الالكترونية، رغبة المشرّع المصري وحرصه على ربط حجيّة الكتابة الالكترونية بمدى توافر الشروط الفنيّة والتقنية المنصوص عنها في القانون رقم ٢٠٠٤/١٥ ولائحته التنفيذية، فقضت[١] أنّه " لا يكون للمراسلات التي تتمّ عن طريق البريد الالكتروني- عند جحد صورها الضوئية أو إنكارها- أيّ حجيّة إلا بمقدار توافر الشروط المنصوص عليها في قانون نظام التوقيع الالكتروني ولائحته التنفيذية، فإن لم يتمّ التحقّق من تلك الشروط فلا يعتدّ بها."

انتقد بعض الفقهاء موقف المشرّع المصري كونه قد أجاز استعمال التوقيع الإلكتروني ومنحه الحجيّة في كافّة المعاملات المدنية والتجارية والإدارية دون استثناء أيّ معاملات من نطاق الإثبات الإلكتروني، إمّا لأهمّية هذه المعاملات في حياة الشخص، أو لندرتها في العمل أو لتأثيرها في الاقتصاد القومي[٢].

٣. موقف المشرّع التونسي

إنّ المشرّع التونسي هو من أوّل المشرّعين على مستوى الدول العربية الذي اهتمّ بالإعتراف بحجيّة السندات الالكترونية، وقد ظهرت أولى هذه البوادر في الفقرة الثانية من الفصل ٦ من قانون التحكيم التونسي الصادر في ١٩٩٣/٤/٢٦، الذي نصّ على عدم ثبوت اتفاقية التحكيم إلا بكتبٍ معتبرًا في الفقرة الثانية منه أنّ الإتّفاقية تعتبر ثابتة بكتبٍ إذا وردت في وثيقة موقّعة من الأطراف أو تبادل رسائل أو تلكسات أو برقيات أو غيرها من وسائل الاتصال.

---

[١] نقض مصري، طعن رقم ٧٨/١٧٠٥١، تاريخ ٢٠١٩/٣/٢٨، عبر الرابط:
https://ahmedazimelgamel.blogspot.com/2022/11/17051-87-28-3-2019-70-64-482.html ، تمّ الاطلاع عليه بتاريخ ١١-٠٧-٢٠٢٢.

[٢] ثروت، عبد الحميد، المرجع السابق، ص. ١٩٢.

تجلّى هذا الإعتراف فيما بعد في قانون المبادلات التجارية التونسي رقم ٢٠٠٠/٨٣ تاريخ ٢٠٠٠/٨/٩، كذلك فقد أصدر وزير الاتصالات قرارًا[١] بتاريخ ٢٠٠١/٧/١٩ حدّد فيه شروط ومواصفات التوقيع الالكتروني وطريقة إنشائه وحفظه.

وقد ساوى القانون السالف الذكر العقود الإلكترونية بالعقود الكتابية التقليدية فنصّت الفقرة الثانية من المادة الأولى من هذا القانون على ما حرفيته:

" تسري على العقود الالكترونية نظام العقود الكتابية من حيث التعبير عن الإرادة ومفعولها القانوني وصحتها وقابليتها للتنفيذ فيما لا يتعارض وأحكام هذا القانون."

كذلك نصّت الفقرة الأولى من المادة الرابعة من هذا القانون على أنّه يعتمد قانونًا حفظ الوثيقة الالكترونية كما يعتمد حفظ الوثيقة الكتابية. وقد اشترطت المادة الخامسة من القانون المذكور إحداث التوقيع الالكتروني بواسطة منظومة موثوق بها حفظ المعلومات الخاصّة بمصدرها ووجهتها وكذلك تاريخ ومكان إرسالها أو استلامها.

وبالتالي نجد أنّ المشرّع التونسي قد اشترط أن يكون التوقيع موثوقًا حتى يضمن حجّيته. وقد ساوى التوقيع الموثوق بالتوقيع الكتابي التقليدي كما جاء صراحة في نصّ المادة ٤٥٣ من قانون الموجبات والعقود التونسي المعدّلة بموجب القانون رقم ٢٠٠٠/٨٣ أعلاه، والتي نصّت على ما حرفيته:

"يتمثل الإمضاء اليدوي في وضع أمر أو علامة خاصة بخط اليد للعقد نفسه مدمجة بالكتاب المرسوم أو إذا كان إلكترونيا في استعمال منوال موثوق به يتضمن صلة الإمضاء المذكور بالوثيقة الإلكترونية المرتبط به."

٤. حجيّة التوقيع الإلكتروني في القانون اللبناني

سبق وتقدّمت النائب الدكتورة غنوى جلّول باقتراح قانون متعلّق بالمعاملات الالكترونية، كما تقدّم النائب ياسين جابر باقتراح قانون مماثل قضى بتعديل بعض أحكام المواد من قانون أصول المحاكمات اللبنانية، إلاّ أنّ المسودّة الأولى للقانون رقم ٢٠١٨/٨١ قد أُنجزت في العام ٢٠٠٥ من قبل الأستاذين الفرنسيين بيار كتالا وفاليري سيداليان بمشاركة بعض الخبراء اللبنانيين.

لقد أقرّ مجلس الوزراء اللبناني بتاريخ ٢٠١٢/١١/١٧ مشروع القانون أعلاه الذي حمل الرقم ٩٣٤١ وأحالته إلى مجلس النواب، لكنّ المناقشات في اللّجان النيابية قد استغرقت حوالي ستّة أعوامٍ قبل أن يتمّ إقرار هذا القانون. كرّس القانون رقم ٢٠١٨/٨١ مبدأين عصريين في مجال الإثبات الإلكتروني:

---

[١] عبر الرابط التالي: https://www.tuntrust.tn/sites/default/files/reglementationsAR/Arrete_1_ar.pdf ، تمّ الاطلاع عليه بتاريخ: 2022-09-26.

أ. مبدأ الحياد التقني

أقرّ القانون المذكور مفهومًا موسّعًا للكتابة بشكلٍ يمكنه استيعاب التقنيّات والصور الحيثة للكتابة، كما يمكنه استباق أيّ تطوّر تقنيّ في هذا المجال، وهذا المبدأ يعني تحرير مفهوم الكتابة التقليدي من ارتباطه بالوسيلة التقنيّة إن كان لجهة تدوينها او لجهة طبيعة الركيزة المدوّنة عليها[١].

وبذلك يكون القانون أعلاه قد أزال أيّ تمييز يمكن أن يحصل بين أساليب الكتابة، فأصبحت الكتابة بالتالي شاملة لتلك التقليدية الورقية وللكتابة الالكترونية وحتّى أيّ شكل من الكتابة يمكن أن يطرأ لاحقًا نتيجة التطوّر التقني، وهذا المبدأ كرّسه قانون الأنسيترال النموذجي في المادة الخامسة منه. فضلا" عن ذلك فقد أقرّ القانون ٢٠١٨/٨١ بالعنصر المعنوي إذ جاء في المادة الأولى منه في إطار تعريفه للكتابة الالكترونية إذ نصّ على ما حرفيته:

"الكتابة :(L'écrit /Writing) هي تدوين أحرفٍ أو أرقامٍ أو اشكالٍ أو رموزٍ او بياناتٍ أو تسجيلها شرط ان تكون قابلةً للقراءة وان يكون لها معنى مفهوم، وذلك أيًّا كانت الدعامة المستعملة (ورقية او الكترونية) وطرق نقل المعلومات."

ب. مبدأ التكافؤ الوظيفي

كرّس القانون أعلاه مبدا التكافؤ الوظيفي الذي يهدف لتحقيق المساواة بين السندات الورقيّة التقليدية والسندات الالكترونية من ناحية قبولها كدليلٍ كامل في الإثبات، ومنحها بالتالي الحجيّة وذلك متى توافرت فيها الشروط المنصوص عنها في هذا القانون. وقد نصّت المادة ٤ من القانون رقم ٢٠١٨/٨١ على إعطاء الكتابة والتوقيع الالكتروني ذات المفاعيل القانونية التي تتمتع بها الكتابة والتوقيع على دعامة ورقية، شرط توافر:

- إمكانيّة تحديد الشخص الصادرة عنه
- ان تنظّم وتحفظ بطريقةٍ ضمن سلامتها

فأصبحت الكتابة الالكترونية، استنادًا لهذا النصّ، منتجةً لكافّة الآثار القانونية في الإثبات مثلها مثل الكتابة التقليدية، وذلك شرط إمكانيتها تحديد هوية صاحبها وتمتّعها بالموثوقية للاعتداد بها كدليل في الاثبات.

[١] المعتصم بالله، أدهم، المرجع السابق ص ٩.

إلا أنّ المشرّع اللبناني لم يقضِ بوجوب إهمال الكتابة التي لا تتوافر فيهما الشرطين المذكورين وفي حال عدم توافر هذين الشرطين بل نصّ على إمكانية اعتبارها بدء بيّنة خطّية. أمّا المادة ٩ من القانون أعلاه فقد اشترطت في فقرتها الأولى أن يصدر التوقيع الالكتروني عن طريق استعمال وسيلة آمنة تعرّف عن الموقع، وتشكل ضمانة على علاقة التوقيع بالعمل القانوني الذي يرتبط به.

كما حدّدت في فقرتها الثانية ماهيّة التوقيع المقصود في المادة ٤ السالفة الذكر فاعتبرت أنّ هذا التوقيع يقتضي أن يقترن بإجراءات الحماية المصادق عليها من قبل مقدّم خدمات المصادقة المعتمد وفق أحكام الفصل الرابع، فيكون بالتالي مساويًا للتوقيع اليدوي حتّى إثبات العكس، إلا أنّ هذه المادة لم تنصّ على كيفيّة وشروط إثبات العكس.

ويرى البعض[١] أنّ المشترع وإن لم يلحظ وسائل إثبات عكس التوقيع الإلكتروني المصادق عليه، فهو قد تبنّى ضمنًا الأحكام العامّة التي ترعى قواعد الإثبات التي نصّ عليها قانون أصول المحاكمات المدنية وكيفيّة إثبات عكس ما يتضمّنه السند الخطّي.

كذلك عالج القانون السالف الذكر قاعدة تعدّد النسخ المنصوص عنها في المادة ١٥٢ أ.م.م.، والتي أثارت في السابق جدلا" فقهيًا. وبالفعل، فقد نصّت المادّة العاشرة من القانون أعلاه على اعتبار قاعدة تعدّد النسخ مستوفاة عند تنظيم السند العادي وفق شروط الموثوقية المنصوص عليها في هذا القانون، وعندما تسمح الآلية المستعملة لكل طرف بالحصول على نسخة عن السند او الوصول اليها، وشروط الموثوقية المقصودة تتمّ باستعمال وسائل آمنة مصحوبةً بتصديق مقدّم خدمات المصادقة.

ويُلاحظ أنّ المادّة المذكورة قد اكتفت بتمكين أيّ طرف من أطراف السند أو العمل القانوني الوصول إليه وإن يكُن بالوسائل الالكترونية دون أن تشترط استخراجه على دعامةٍ ورقيةٍ أو حتّى الكترونية. أمّا في حالة التعارض بين الدليل الالكتروني والدليل الورقي فقد منحت المادة ١١ من القانون ٢٠١٨/٨١ القاضي الناظر بالنزاع سلطة تقديرية لتحديد السند أو الدليل الأكثر مصداقية بصرف النظر عن دعامته، دون تقييده بشروطٍ أو معايير محدّدة للترجيح بين السندات المذكورة التي تختلف طبيعة دعامتها، وسلطة القاضي هذه لا تخضع لرقابة محكمة التمييز[٢]. وقد ميّز المشرّع اللبناني في القانون ٢٠١٨/٨١ بين نوعين من التوقيع الإلكتروني:

[١] هاني، الحبال، قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي، دون دار نشر، بيروت ،٢٠١٩، ص. ١٣.

[٢] المعتصم بالله، أدهم، المرجع السابق، ص. ١٠.

أ. التوقيع الإلكتروني المصادق عليه من قبل مقدّم خدمات غير معتمد

نصّت المادة ١٨ من القانون رقم ٢٠١٨/٨١ على أنّه إذا تمّ انشاء توقيع الكتروني او تنظيم كتابة الكترونية وتأريخها وحفظها وفق إجراءات مصادقة يقدّمها مقدّم خدمات مصادقة غير معتمد، يعود للقاضي حق تقدير قوتها الثبوتية، ما لم يتّفق الفرقاء على خلاف ذلك.

ونجد أنّ المشرّع اللبناني قد أعطى الحرّية للفرقاء رغم اختيار مقدّم خدمات غير معتمد أن يمنحوا قوّة ثبوتية مطلقة للتوقيع الإلكتروني في حال اتّفاقهم على ذلك، وهذا ما يتجانس مع نصّ المادتين ١٤ و١٥ من هذا القانون حيث نصّت الأولى أنّ الكتابة الالكترونية حرّة، ولا يُلزم أحدٌ باللّجوء الى وسائل حماية ما لم ينصّ القانون على خلاف ذلك.

أمّا الثانية فاعتبرت أنّ وسائل الحماية التي تطبق على الكتابات والتواقيع الالكترونية، والتي يؤمنها مقدم خدمات المصادقة، تهدف الى تعزيز موثوقيتها.

ومقدّم الخدمات غير المعتمد المذكور أعلاه هو الذي لم يستحصل على شهادة اعتماد من المجلس الوطني للإعتماد Collibac، وفق الإجراءات المنصوص عليها في المادة ٢٠ وما بعدها من القانون المذكور، فمقدّمي الخدمات العالميين ربما لا يكون لهم مصلحة أو حاجة لخضوع لرقابة سوق داخلي وتكبّد نفقات هم بغنًى عنها، نظرًا لحجم محفظتهم على المستوى العالمي.

ويرى البعض[١] أنّ الشهادة المذكورة، وإن لم تصدر عن مقدم خدمات معتمد، فيمكن أن يكون لها القوّة الثبوتية كتلك الصادرة عن مقدّم خدمات معتمد، في حال تثبّت القضاء أنّ التوقيع الملحق بالشهادة المذكورة يمكّن من تحديد الشخص الصادر عنه واستعمال وسيلة آمنة تعرّف بالموقّع وتنظيم وحفظ التوقيع بطريقة تضمن سلامته.

أمّا بالنسبة لأبرز الشروط والضمانات الواجب على القضاء التثبّت منها فهي:

- مدى اعتماد إجراءات الحماية ومعايير الأمان اللازمة للحؤول دون أيّ تعرّض للبيانات أو استعمالها بشكلٍ غير مشروع.
- احترام موجبات السرّية والموثوقية والإستعمال لأهدافٍ مشروعة.

ب. التوقيع الإلكتروني المصادق عليه من قبل مقدّم خدمات

نصّت المادة ١٧ من القانون رقم ٢٠١٨/٨١ على تمتّع التوقيع المصادق عليه وفق اجراءات يقدّمها مقدم خدمات مصادقة معتمد بقرينة الموثوقية حتى اثبات العكس،

[١] شربل، قارح، قانون الإنترنت، الجزء الثامن، المنشورات الحقوقية صادر، بيروت، ٢٠١٩، ص. ١٣١.

وقد أعطى المشرّع اللبناني بالتالي التواقيع الإلكترونية الملحقة بشهادات إلكترونية صادرة عن مقدّمي خدمات معتمدين من قبل المجلس اللبناني للاعتماد COLLIBAC قوّةً ثبوتيةً كاملة.

الفقرة الثانية: شروط صحّة التوقيع الإلكتروني وخصائصه

تعتبر الغاية الأساسية من التوقيع الإلكتروني إضفاء قوّة ثبوتية على الأعمال القانونية. ومن أجل تحقيق هذه الغاية يقتضي توافر شروطٍ محدّدة بغية تعزيز هذا التوقيع وتوفير الثقة فيه.

كذلك نجد أنّ التوقيع الالكتروني يتمتّع بسِماتٍ وخصائص منفردة تميّزه عن التوقيع اليدوي التقليدي.

وسنبيّن أدناه الشروط الواجب توافرها في التوقيع الالكتروني (أولا")، وخصائص هذا التوقيع التي تميّزه عن التوقيع اليدوي التقليدي(ثانيًا).

أولاً: شروط صحّة الوقيع الإلكتروني

اشترطت معظم التشريعات للأخذ بالتوقيع الإلكتروني كدليلٍ كاملٍ في الإثبات أن تتوافر فيه عدّة شروط يمكن اختصارها بما يلي:

١. ارتباط التوقيع بشخص صاحبه

إنّ هذا الشرط يتماشى مع مفهوم التوقيع التقليدي الذي يعتبر علامةً مميّزةً وخاصّةً بشخص الموقّع تميّزه عن غيره، كما سبق بيانه، ويهدف هذا الشرط لضمان عدم استخدام التوقيع الإلكتروني من قبل شخصٍ آخر غير صاحبه.

من شأن توافر هذا الشرط أن يثبت نيّة الموقّع بالالتزام بمضمون العمل القانوني الموقَّع عليه من قبله، وفي الحالة التي يكون فيها التوقيع موثّقًا، ولنا عودة للحديث عن التوثيق في الفصل الثاني من دراستنا، فمن شأن هذا الأمر أن يؤكّد على ارتباط التوقيع بشخص صاحبه بشكل لا لبس فيه، كذلك في حالة استعمال التوقيع البيومتري (كالتوقيع ببصمة الإصبع أو قرنية العين) الذي لا يمكن أن ينسب لغير صاحبه نظرًا لكونه سماتٍ فريدة خاصة بالموقّع.

٢. إمكانية تحديد هويّة الشخص الصادر عنه

إنّ الغاية الأهمّ من التوقيع هي تحديد هويّة الموقّع، وفي حالة التوقيع التقليدي إنّ هذا الشرط هو بديهيّ فالإمضاء والختم والبصمة كلّها تدلّ على صاحبها وتعرّف عنه، أمّا في حالة التوقيع الالكتروني، حتى وإن لم يشتمل على اسم الموقّع إلا أنّ الإجراءات التقنيّة المتّبعة تكفي لتحديد هويّة الموقّع، خاصّة

مع التطوّر التقني الذي شهده ميدان التوقيع الإلكتروني أصبح بإمكانه تأمين هذه الوظيفة خاصّة عند استعمال تقنيّة التشفير المزدوج الذي يسمح بتحديد هويّة الموقّع بشكلٍ آمنٍ وفعّال باعتبار أنّ المفاتيح السرّية تُحفظ بشكلٍ يجعل من إمكانيّة الغشّ جدّ ضئيلة إن لم نقل منعدمة [١].

تكمن أهميّة تحديد الهويّة، للدلالة من جهةٍ على سلطة الموقّع لإبرام العمل القانوني، ومن جهةٍ أخرى يثبت رضى الموقّع عن مضمون هذا العمل القانوني.

٣. توافر إجراءات تقنية تسمح بالسيطرة على التوقيع

إنّ المقصود بهذا الشرط هو استئثار الموقّع بفكّ رموز توقيعه أو معرفته وحده الرمز السرّي في حالة اعتماد هذا النوع من التواقيع.

وقد أكّدت محكمة استئناف Besançon على وجوب توافر هذا الشرط في حكمها الصّادر بتاريخ ٢٠ تشرين الأوّل من العام ٢٠٠٠ [٢]، حيث اعتبرت هذه المحكمة بوجوب خضوع وسائل التوقيع الالكتروني لسيطرة الموقّع دون غيره بغية اعتبار التوقيع المذكور حجّة على الموقّع.

٤. توافر إجراءات تقنيّة تسمح باكتشاف أيّ تعديل يطرأ عليه أو على مضمون المستند

إنّ هذا الشرط يتمتّع بأهميّةٍ بالغة كونه يميّز التوقيع الإلكتروني عن التوقيع العادي، فالتوقيع العادي لا يمكنه أن يثبت بشكلٍ جازم عدم حصول تزوير في المستند أو في التوقيع، أمّا التوقيع الإلكتروني فيمكنه تحقيق هذه الغاية بحسب التقنيّات المستعملة لتأمين ارتباط السند بالتوقيع.

ومن أبرز هذه التقنيات هو استعمال التوقيع الرقمي المُرتكز على تقنيّة التشفير المزدوج، والذي يؤمّن التدقيق بصحّة مضمون السند عن طريق ما يُعرف بالهاش أو التقطيع اللامعكوس والذي يخلق ملخّصًا رقميًّا عن الرسالة[٣] يسمح بعد فكّه بالتثبّت من عدم حصول تلاعب بمحتويات هذا السند.

ثانياً: خصائص التوقيع الالكتروني

يتميّز التوقيع الإلكتروني بعدّة خصائص أبرزها السرعة والسرّية وإمكانية تحديد توقيت حصول التوقيع على المستند.

١. السرعة والمرونة

---

[١] ضياء، مشيمش، المرجع السابق، ص. ١٥٠.

[٢] تمّت الإشارة إليه في الصفحة ١٦ من هذه الدراسة.

[3] T. Piette-coudol, op. cit, p. 17.

إنّ أبرز الأمثلة على السرعة والمرونة التي يؤمّنها التوقيع الإلكتروني هي في المعاملات المصرفيّة، فقد أدّى استعمال هذا التوقيع إلى تحقيق تطوّر هائل في هذا القطاع موفّرًا على عملاء المصرف الوقت وعناء المعاملات المصرفيّة الورقيّة. وبمقارنةٍ بسيطةٍ بين الإجراءات التقليدية المعتمدة سابقًا في المصارف لتحويل الأموال وسحبها وإيداعها يمكننا أن نلمس الفارق الكبير الذي أحدثه استعمال التوقيع الإلكتروني والبطاقات الممغنطة في هذا المجال.

٢. تأمين السرّية

منذ استعمال وسائل الاتصالات عن بعد أصبحت السرّية والموثوقية هدفًا أساسيًا وحاجة بغاية الأهمّية يأمل مستخدمي هذه الوسائل تحقيقها. حتّى في يومنا هذا نجد أنّ تطبيقات التواصل الاجتماعي تسعى بشكل دائم لتطوير أنظمتها بغية تأمين ميزة السرّية، فتطبيق واتساب، المملوك من شركة Meta، والذي يستخدمه حوالي ملياري شخص حول العالم[١]، بدأ منذ شهر نيسان ٢٠١٦ إلى حماية سرّية المراسلات الحاصلة عن طريقه معتمدًا على تقنية التشفير[٢]، بغية جذب أكبر عدد من المستخدمين الذي يسعون، كما أسلفنا، لتأمين سرّية رسائلهم.

والتوقيع الإلكتروني من شأنه أن يؤمّن سريّة المراسلات خاصّة متى استعمل التوقيع الرقمي المستند على التشفير غير المتماثل والذي يعتبر أحد أهمّ أنواع التوقيع الإلكتروني وأكثرها أمانًا وموثوقيّة.

٣. تحديد تاريخ التوقيع

إنّ إثبات تاريخ التوقيع الإلكتروني هو نظامٌ يقوم على ربط التاريخ بعملٍ أو واقعةٍ قانونية، ومن الناحية التقنيّة يرتكز على تقنيّة التشفير. وتكمن أهميّة هذه العملية على ضمان موثوقية العمل القانوني وصحّة تاريخ التوقيع [٣].

وبحسب الفقرة الأولى من المادة ٤١ من التوجيه الأوروبي تاريخ ٢٠١٤/٩١٠ فإنّ الأثر القانوني وقبول الختم الزمني الإلكتروني في الإثبات لا يمكن أن يتمّ رفضه فقط تحت ذريعة حصوله بالطريقة الإلكترونية

---

[١] عبر الرابط التالي: https://backlinko.com/whatsapp-users ، تمّ الاطّلاع عليه بتاريخ: ١٠-٠٨-٢٠٢٢

[٢] عبر الرابط التالي: https://faq.whatsapp.com/820124435853543 تمّ الاطّلاع عليه بتاريخ: ١٠-٠٨-٢٠٢٢

[3] Caprioli, Eric De l'authentification à la signature électronique : quel cadre juridique pour la confiance dans les communications électroniques internationales p. 34

Disponible sur le web : https://www.caprioli-avocats.com/fr/, conculté le 21-3-2022

أو لعدم مراعاته متطلّبات الختم الزمني المعتمد. وبحسب الفقرة الثانية من المادة عينها فإنّ الختم الزمني المؤمّن يتمتّع بحجيّة صحّة التاريخ والتوقيت التي يحدّدها وكذلك موثوقية البيانات المتعلّقة بهذا التاريخ وهذا التوقيت.

وقد عرّفت المادة ١٣ من اللائحة التنفيذية الجديدة للقانون المصري رقم ٢٠٠٤/١٥، الصادرة بتاريخ ٢٠٢٠/٤/٢٣، البصمة الزمنية الالكترونية بأنّها:

"ما يوضع على محرّر إلكتروني ويتّخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها والتي تربط تلك البيانات بوقتٍ محدّد لإثبات وجود هذا المحرّر الإلكتروني في ذلك الوقت."

يحدّد التوقيع الإلكتروني لحظة إرسال الرسالة ويتمّ ذلك بواسطة سلطة إصدار الشهادة، بحيث تحدّد التاريخ دون التعرّف على محتوى العقد أو صفات الأشخاص[١]. وتكمن أهميّة إثبات تاريخ التوقيع لحماية المستند من التزوير كما من إمكانيّة التذرّع زورًا بأنّه قد حصل بتاريخ سابق أو لاحق لتاريخه الفعلي وما ينتج عن ذلك من إشكاليّات قانونية وتؤثّر على صحّة المستند الإلكتروني.

[١] ضياء، مشيمش، المرجع السابق، ص. ١٤٧.

الباب الثاني: تطبيقات التوقيع الإلكتروني

تتنوّع تطبيقات التوقيع الالكتروني في ميدان التجارة الالكترونية، فقد أدّى انتشار التقنيات الحديثة في المعاملات ووسائل الدفع والإيفاء إلى ظهور وسائل جديدة في هذا المجال ترتكز بمعظمها على التوقيع الالكتروني.

وسنبحث أدناه تطبيقات التوقيع الالكتروني في البطاقات المصرفية والنقود الالكترونية (فقرة أولى)، ودور التوقيع الالكتروني في السندات الالكترونية والحكومة الالكترونية (فقرة ثانية).

الفقرة الأولى: التوقيع الإلكتروني في البطاقات المصرفية والنقود الالكترونية

تلعبُ البطاقات المصرفية والنقود الالكترونية دورًا بارزًا في إطار التجارة الالكترونية وأجهزة الدفع التي تشكّل بدورها أهميةً قصوى في تلبية حاجات الإنسان اليومية. وسنحاول أدناه تسليط الضوء على أنواع البطاقات المصرفية ودور الإلكتروني في عمليّة الدفع (أولا")، وعلى ماهية النقود الالكترونية وأنظمتها (ثانيًا).

أولا": في البطاقات المصرفية

بدأ استخدام البطاقة المصرفية في منتصف القرن السابق، وذلك بهدف الدعاية والمنافسة لتسهيل عمليّة البيع بالثمن المؤجّل ليس إلاّ وكانت العلاقة آنذاك ثنائية بين المُصدر والحامل. وقد كانت بطاقة شركة دينارز كلوب (Diners Club)البداية الحقيقية لما يُعرف اليوم باسم البطاقة المصرفية[1]. فقد كانت فكرة الشركة ان تدفع عن المشتري قيمة البضاعة او الخدمة (وذلك مقابل عمولة بسيطة)، وبعدها ترسل للمشتري المبلغ المستحق بعد مدّة محدّدة فيقوم بدفعها. ودخلت المصارف حيّز المنافسة، حين قام بنك اوف اميركا (Bank of America) بتقديم فكرة البطاقة ولكن مع بعض التطوّر والتسهيلات[1].

في العام ١٩٦٦ كانت باكورة البطاقات المصرفية في أوروبا عندما أصدر "مصرف باركليز" "Barclay's Bank" بالإشتراك مع " بنك أوف أميركا" "Bank of America " بطاقة مصرفية سمّيت "بطاقة باركليز" "Barclay's card" وفي نفس السنة أطلقت مؤسسة "ستليم" "Cetelem" الفرنسية بالإتفاق والتعاون مع متاجر " غاليري لافاييت" "Galleries Lafayette" بطاقة حملت اسميهما. وبعد ذلك بعام واحد، أصدر تجمّعٌ

[1] أنس، العلبي، النظام القانوني لبطاقات الاعتماد، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٥، ص. ٣٤.

يضمّ أقوى المصارف الفرنسية بطاقة حملت إسم البطاقة الزرقاء "Carte Bleu"، أتُبِع بإطلاق بطاقة "انتركارت" "Intercarte"من المصارف الشعبيّة[1].

أمّا في لبنان فقد صدرت في أوائل التسعينات بطاقتان محليّتان يقتصر استعمالهما على السوق المحلّي فقط، الأولى عن شركة "كاشلس كارد ش.م.ل." "Cashless card S.A.L." سمّيت "Cashless Card" والثانية عن "الشركة اللبنانية للبطاقات المصرفية ش.م.ل." "Lebanese Interbank Card S.A.L" سمّيت بطاقة"LINK"[2].

ويمكن تعريف البطاقة المصرفية أنّها بطاقة بلاستيكية ذات خصائص معيّنة صادرة عن مؤسسة مالية أو مصرفية تستخدم كوسيلة دفع أو إيفاء بدلاً من النقود ويستطيع حاملها أن يستفيد بواسطتها من الخدمات المالية إضافة إلى الإئتمان الممنوح بموجبها من المصرف الذي أصدرها[3].

تحمل البطاقة بيانات جوهريّة أبرزها: إسم وشعار المنظمة الدولية، اسم وشعار المصرف المصدر، رقم البطاقة، اسم صاحبها، وتاريخ الصلاحية. وللبطاقة شريط ممغنط مسجّل عليه بيانات غير ظاهرة كالرقم السرّي والحدّ الأقصى للسحب والمعلومات الضرورية لاستعمالها على آلات نقاط البيع (POS) والصّراف الآلي.

إنّ خصائص وأهداف الخدمات المصرفيّة الالكترونية هي التي جعلت المصارف تسارع للّجوء اليها، لأنّها توفّر للزبائن اليسر والسهولة والسرعة والكلفة المتدنية حين إجراء الخدمات المصرفية ممّا يزيد من حجم عملاء المصارف. فمستقبل المصارف لا يعتمد على خدمة الزبائن فقط، بل وايضا على مواكبة البيئة الالكترونية الحديثة التي تتيح للعملاء أو الزبائن إجراء معظم عمليّاتهم المصرفيّة من خلال الانترنت أو الهاتف الخلوي أو الصرّاف الآلي(ATM) وغيرها، ولكن مع المحافظة على جوّ الثّقة والامان والسلامة والذي يعتبر من أهمّ الركائز للقطاع المصرفي بشكل عام.

وقد شهدت وسائل الدفع تطورا بارزًا وباتت المعاملات المالية تتمّ باستخدام الحواسيب وشبكة الانترنت وتقنيات الاتصالات الحديثة وقد نتج عن ذلك توفير في الوقت وتحجيم النفقات المادية والبشرية بعد أن صار بإمكان الحاسوب تلقّي الأوامر الصادرة عن الحامل إمّا عبر الموزعات أو الكوّات الآلية (D.A.B.,G.A.B)

---

[1] خليل، الدحداح، بطاقة الإعتماد، بدون دار نشر، بيروت، ١٩٩٨، ص. ٩.

[2] وائل، الدبيسي، البطاقات المصرفية أنظمة وعقود، منشورات صادر ص. ٢٤.

[3] أنطوان، الناشف؛ وخليل، الهندي، العمليات المصرفية والسوق المالية، مؤسسة حديثة للكتاب، الجزء الأول، لبنان، ١٩٩٨ ص. ١٥٩.

إمّا عبر الأجهزة الموجودة في نقاط البيع (T.P.E.,T.P.V) أو عبر أجهزة خاصة مستحدثة كجهاز المينيتل المستعمل في فرنسا[1].

١. أنواع البطاقات المصرفية

باتت البطاقات المصرفية في عالمنا اليوم من الضروريات، فهي طريقة آمنة الى حدّ ما ومضمونة. تُصدر البنوك والمؤسسات المالية المرخّص لها البطاقات المصرفية لعملائها من أجل تيسير احتياجاتهم ممّا أدّى الى التنافس بين المصارف لتقديم أفضل خدمة للزبائن، فعملوا على استحداث انواع بطاقات جديدة من حيث الخدمات التي يمكن تقديمها. أمّا أبرز أنواع البطاقات المصرفية فهي:

أ. البطاقة المصرفية المسبقة الدفع (Prepaid Card)

إنّها أبسط انواع البطاقات، يشتريها الزبون ويدفع ثمنها مسبقًا حتّى لو لم يكن لديه أي حساب في المصرف مُصدر البطاقة. وهناك نوعان متمايزان من هذه البطاقة:

(١) البطاقة المسبقة الدفع القابلة للتجديد: ويمكن لحاملها إعادة تمويلها بعد إنتهاء قيمتها ويظل محتفظا" بها لاستعمالها بعد إعادة تمويلها.

(٢) البطاقة المسبقة الدفع غير القابلة للتجديد: وفي هذا النوع تتلف البطاقة بمجرد إنتهاء القيمة المخزنة فيها والنوع الأكثر شيوعا" من هذه البطاقات هي تلك المستعملة للتبضع عبر شبكة الإنترنت، ويكون الرقم السري في هذا النوع من البطاقات مخفيا"، يمكن إظهاره بواسطة الحكّ ومن ثم إستعماله على الشبكة الدولية او للعمليات عبر البريد أو عبر الهاتف. ولا يمكن استعمالها للسحب النقدي عبر الصرّافات الآلية ولا في نقاط البيع.

ب. البطاقة الدائنة أو القيد المباشر (Debit Card)

هذا النوع من البطاقات هو الأوسع انتشارا في العالم لأنّ مخاطرها قليلة نسبيًا أو يمكن أن تكون معدومة إلّا في حالة الخطأ. فهي بطاقة تصدر عن المصرف لمصلحة الزبون الذي يكون له حسابًا مصرفيًا. يقدّم الزبون بطاقته الى التاجر لدفع ثمن مشترياته، فيمرّر التاجر البطاقة عبر جهازٍ موصولٍ مباشرةً بمركز البطاقات. فإذا كان حساب الزبون يكفي لايفاء قيمة المشتريات، يتمّ حسم المبلغ آليًا وتُضاف القيمة الى التاجر مباشرة. وإذا كان الرصيد لا يسمح بالوفاء، فيتمّ الغاء العملية.

[1] خليل، الدحداح، المرجع السابق ص. ٨١.

هذا النوع من البطاقات لا ينطوي على ائتمان فعلي لذلك يرى البعض[1] أنّه من غير الدقّة أن تسمّى مثل هذه البطاقات ببطاقة إعتماد، وهذا ما درج عليه الإصطلاح الإنكليزي إذ يدعو هذه البطاقة Debit Card أي بطاقة الدين. ولكنّ تسمية هذه البطاقة هذه البطاقة في اللغة العربية ببطاقة إعتماد ليس من قبيل الخطأ لأنّ الحامل قد يستفيد من اعتماد يفتحه له المصدر أحيانًا، إذ إنّ بعض مصدري هذه البطاقات وزيادة في الثّقة الممنوحة لعملائهم يتيحون للحامل سحب أموال، بواسطة البطاقة وبحدودٍ معيّنة، تفوق تلك المودعة في حسابه بواسطة البطاقة وبحدودٍ معيّنة، تفوق تلك المودعة في حسابه بواسطة البطاقة وحتّى حدّ معيّن.

إلاّ أنّ المصرف لا يقوم بهذا التصرّف إلاّ ليقينه الكامل بالوضع المالي المتين لعميله ولثقته بأنّ عميله إن تعرّض لمثل هذه المخاطر فإنّه سوف يلتزم بإعادة الأموال المسحوبة.

ج. بطاقة الائتمان (Credit Card)

هي وسيلة اعتماد لحاملها حيث يفتح المصرف المصدر اعتمادًا لزبونه إمّا بسقفٍ محدّد أو غير محدّد. يقوم الزبون بجميع مشترياته ويجري السحوبات النقدية من خلال الصرّاف الآلي وذلك خلال مدّةٍ اعتمادية محدّدة. ويقوم المصرف المصدر بمحاسبة الزبون في نهاية هذه المدة بفاتورة واحدة. ويمكن تقسيم هذه البطاقة، استنادًا إلى محاسبة العميل في نهاية المدّة الإعتمادية، إلى نوعين:

(١) بطاقة الاعتماد العادية: في هذا النوع من البطاقات يقوم الحامل بدفع كامل قيمة الفاتورة عند المحاسبة في نهاية الفترة الاعتمادية، لذلك فإنّ التكاليف المتوجّبة عليه تقتصر على بدلات الاشتراك والعمولة التي تترتّب على مجمل الفاتورة ولا يفرض المصدر فوائد إلاّ على التأخّر في السداد.

(٢) بطاقة الاعتماد القرضية: في هذا النوع من البطاقات يكون العميل مخيّرًا بين دفع قيمة الفاتورة المرسلة إليه في نهاية الفترة الاعتمادية وبين دفع جزء منها أو الحدّ الأدنى منها وفق ما يحدّده المصدر في عقده مع الحامل. ويتمّ تدوير الجزء المتبقّي من الفاتورة إلى الفترات الاعتمادية التالية ويتحقق على تلك المبالغ فائدة بنسبة محددة (تصل احيانا" إلى ١٧ %)، وهذه الميزة تعرف باسم (الاعتماد المتجدد أو الاعتماد المدور Revolving credit) لأنّ الاعتماد يتجدّد باستمرار. تحقّق هذه الفائدة ربحًا مجزيًا للمصدر يُضاف إلى مجمل التكاليف المفروضة على الحامل من بدلات وعمولات.

[1] أنس، العلبي، المرجع السابق، ص. ٥٣.

(٣) بطاقات الاعتماد المضمونة (Secured Credit Card): والتي تصدرها المصارف لبعض الزبائن نظرا لكونهم غير مؤهّلين للحصول على البطاقة الائتمانية، فيطلب المصرف من الزبون ايداع مبلغ مالي لديه يبقيه بمثابة ضمانةٍ مقابل عمليات البطاقة. فإذا استخدم الزبون البطاقة ولم يقم بتسديد المبلغ المتوجب عليه للمصرف في الوقت المحدد، يقوم المصرف بتجميد البطاقة ويسدّد الدين المطلوب على الزبون من الضمانة المودعة لديه.

٢- دور التوقيع الإلكتروني في عمليّة الدفع

عمليًّا يقوم المصرف بتسليم العميل بطاقة بلاستيكية أو ما يعرف ببطاقة السحب الآلي بالإضافة إلى رمزٍ سرّي يكون في العادة مؤلّفًا من أربعة أرقام يمكن للعميل اختياره، وبعد ذلك تتّبع الإجراءات التالية:

- يقوم العميل بإدخال البطاقة المذكورة في مكانٍ مخصّصٍ لها في الصرّاف الآلي أو في أجهزة الدفع المتوفّرة لدى نقاط البيع.
- يقوم العميل بعد ذلك بإدخال الرقم السرّي، ما يعدّ تعبيرًا عن اتّجاه إرادته للإتمام العمليّة التي يقوم بها، إذ يعتبر هذا الرمز السرّي توقيعًا إلكترونيًا كما أثبتنا سابقًا في دراستنا.
- يحدّد العميل العملية المصرفية التي يرغب بالقيام بها كسحب الأموال أو إيداعها أو إيداع الشيكات وغيرها من العمليّات.

ثانيًا: النقود الإلكترونية

عرّفت الفقرة ٢ من المادة ٢[1] من التوجيه الأوروبي رقم ٢٠٠٩/١١٠ تاريخ ٢٠٠٩/٩/١٦ النقود الإلكترونية بأنّها:" قيمة نقدية مخزّنة في شكل إلكتروني، بما في ذلك مغناطيسي ، تمثّل دينًا على المُصدر، والصادرة مقابل إيداع أموال بهدف تنفيذ عمليات نقدية، محدّدة في البند ٥[2] من المادة ٤ من التوجيه الأوروبي رقم ٢٠٠٧/٦٤، ومقبولة من قبل شخص طبيعي أو معنوي غير مصدر هذه النقود الإلكترونية."

---

[1] «monnaie électronique»: une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement telles que définies à l'article 4, point 5), de la directive 2007/64/CE et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique;

[2] «opération de paiement»: une action, initiée par le payeur ou le bénéficiaire, consistant à verser, transférer ou retirer des fonds, indépendamment de toute obligation sous-jacente entre le payeur et le bénéficiaire;

علمًا أنّ البند ٥ من المادة ٤ من التوجيه الأوروبي رقم ٢٠٠٧/٦٤ قد عرّفت العمليات النقدية بأنّها: إجراء يقوم به الدافع أو المستفيد، ويتألّف من دفع الأموال أو تحويلها أو سحبها، بشكلٍ مستقلّ عن أي التزام أساسي بين الدافع والمستفيد.

وقد تبنّى المشرّع الفرنسي التعريف نفسه الوارد في التوجيه الأوروبي أعلاه في المادة L315-1 من قانون النقد والتسليف الفرنسي[١]. كذلك عرّفتها المادة الأولى من القانون اللبناني رقم ٢٠١٨/٨١ بأنّها وحداتٌ تسمّى وحدات نقدٍ الكتروني يمكن حفظها على دعامة الكترونية.

ترتكز العملة الالكترونية على برنامج حاسبٍ آليّ مؤلّف من سلسلة أرقامٍ متتابعة تديرها خوارزميات معقّدة. ويهدف هذا البرنامج من جهة إلى معالجة القيمة النقديّة التي تمثّلها هذه العملة الرقميّة، ومن جهةٍ أخرى إلى مصادقة الجهة المصدرة للعملة أعلاه، ويتمّ كلّ ذلك باستخدام تقنيات التشفير لضمان الأمان[٢].

وهناك العديد من أنظمة النقود الإلكترونية أمّا أبرزها:

أ. نظام Cyber Coin: تمّ تصميم هذا النظام من قبل شركة Cyber Cash في العام ١٩٩٤ في ولاية فيرجينيا في الولايات المتّحدة الأميركية، ويتميّز هذا النظام بارتباطه بنظام مركزي يعطي وحدة النقد الإلكتروني قيمتها[٣].

يدفع العميل مقدمًا قيمة النقود الإلكترونية، وهذه النقود لا تُختزن في الذاكرة الصلبة Hard Disk العائد لحاسبه الشخصي إنّما يتمّ تحويلها إلى محفظة مركزية عائدة للنظام المذكور موجودة في Cyber Cash Bank، لا يحتاج العميل إلى فتح حساب لدى المصرف المذكور إنّما يقتصر الأمر على تحويل قيمة مشترياته من محفظته المودعة لدى المصرف المذكور، كذلك الأمر بالنسبة للتاجر فهو ليس مضطرًا لفتح حساب لدى المصرف أعلاه إذ يمكنه إمّا التعامل بالنقود المدفوعة إليه عن طريق عمليّة شراء وتحويل يق.وم بها، أو يمكنه طلب تحويلها إلى حسابه المصرفي المفتوح لدى مصرف آخر لقاء عمولة معيّنة.

---

[1] La monnaie électronique est une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement définies à l'article L. 133-3 et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique.

[٢] طوني، عيسى، المرجع السابق، ص. ٣٠٣.

[3] R.Razali, The Overview of E-cash: Implementation and Security Issues, https://www.giac.org, acceced 01-10-2022.

يمتاز هذا النظام بمحدوديّة المخاطر نظرًا لكون العملة الإلكترونية غير مخزّنة في الحاسب الآلي العائد للمستخدم إنّما يتمّ دائمًا الرجوع إلى المصرف لإجراء عملية تبادل هذه العملة[١].

ب. نظام شركة Digicash، وقد تمّ اعتماد هذا النظام من قبل مصرف Mark Twain في الولايات المتّحدة الأميركية الذي يعتبر أوّل مصرف في العالم يقبل هذا النوع من النقود.

وبحسب هذا النظام يقتضي أن يكون لكلّ من التاجر والزبون حسابين مصرفيين أحدهما بالعملة العاديّة والآخر بالعملة الإلكترونية، وبعد قيام الزبون بتسديد ثمن مشترياته بالعملة الإلكترونية، يتحقّق التاجر من صلاحية هذه العملة ويقوم من بعدها إمّا بقيدها في حسابه الفتوح لدى المصرف المذكور بالعملة الإلكترونية أو يقوم بتحويلها إلى حسابه الآخر المفتوح بالعملة العادية[٢].

ج. نظام شركة Mondex، تمّ تصميم هذا النظام من قبل Tim Jones و Graham Higgins في بريطانيا، ويرتكز هذا النظام على البطاقة ذات الشريحة (Carte à Puce)[٣] . ويتمّ تحويل الأموال فيما بين بطاقتين مماثلتين الأولى تكون بحوزة البائع والثانية بحوزة المشتري، ولا يستلزم ذلك تدخّلا من قبل المصرف.

لا يحتاج هذا النظام للمقاصّة، ولا يحتاج أيّ طرفٍ ثالث لتسوية المعاملات بين المستخدمين، ومن شأن ذلك أن يؤدّي إلى زيادة السرعة في التعامل وتبسيط إجراءات الاستخدام.

الفقرة الثانية: دور التوقيع الإلكتروني في السندات الإلكترونية والحكومة الإلكترونية

نتج عن دخول المعلوماتية عالم الأعمال التجارية ظهور سندات تجارية ذات دعامةٍ الكترونية.

ومن جهة ثانية فقد ساهمت تقنيات المعلوماتية بشكلٍ كبير في تسهيل معاملات المواطنين اليوميّة وتقليص النفقات والحدّ من الفساد الأمر الذي يُعرف بالحكومة الإلكترونية،

---

[١] أحمد، موسى، النقود الإلكترونية وتأثيرها على دور المصارف المركزيّة في إدارة السياسة النقدية، الجديد في أعمال المصارف من الوجهتين القانونية والسياسية، أعمال المؤتمر العلمي السنوي لكليّة الحقوق بجامعة بيروت العربية، منشورات الحلبي الحقوقية، الجزء الأول، الطبعة الأولى، بيروت،٢٠٠٢، ص. ١٥٧.

[٢] طوني، عيسى، المرجع السابق، ص ٣٠٤.

[3] Overview ~ What Is Mondex?, https://web.mit.edu/ecom/Spring1997/gr13/overview.html, acceced: 09-08-2022.

وسنتطرّق أدناه لأبرز أنواع السندات الإلكترونية (أولا")، وإلى الحكومة الإلكترونية (ثانيًا).

أولا": في السندات الالكترونية

يُعدّ الشيك وسند الشحن الإلكترونيين من أبرز تطبيقات التوقيع الالكتروني في مجال السندات الرقمية لذا سنحصر بحثنا بهذين النوعين مسلّطين الضوء على ماهيّة كلٍّ منهما وأهمّيتهما في مجال التجارة الالكترونية.

١. الشيك الإلكتروني

يُعتبر الشيك الإلكتروني بمثابة نسخة الكترونية عن الشيك الورقي التقليدي، ونظرًا لأهميّة هذا الشيك في ميدان التعامل التجاري قامت عدّة مصارف بإصدار شيكات إلكترونية وأبرز هذه المصارف بوسطن بنك والبنك الفدرالي الأميركي.

وقد عرّفه البعض بأنّه "عبارة عن وثيقة إلكترونية، تُرسَل عن طريق البريد الإلكتروني وتكون موقّعة وموثّقة إلكترونيًا، يتمّ تبادلها بين الساحب والمستفيد من خلال وسيط إلكتروني يتأكّد من صحّة الرصيد وبواسطة أحد المصارف مباشرةً[١] ".

تتشابه إلى حدٍّ ما، طريقة تحرير الشيك الإلكتروني بالشيك الورقي، إنّما تتمّ عن طريق اتّباع الإجراءات التالية:

أ. يقوم العميل مسبقًا بفتح حسابٍ إلكتروني لدى مصرفٍ معيّن.

ب. يرسل العميل الشيك الموقّع إلكترونيًا عن طريق البريد الإلكتروني.

ج. يقوم البائع أو المسحوب لأمره الشيك بإيداعه لدى خادم (Server) مخصّص لهذه العمليّة.

د. يتمّ تحصيل قيمة الشيك بعد التثبّت من صحّة التوقيع الإلكتروني.[٢]

يتمّ الاستعانة بعمليّة التشفير، التي لنا عودة إليها في الفصل الثاني من دراستنا، وذلك بهدف ضمان عمليّة تسوية الدين بالإيفاء[٣]. ومن أبرز أنظمة الشيك الإلكتروني نذكر نظام NetCheque، وقد تمّ تطويره من قبل باحثين في جامعة كارولينا الجنوبية في الولايات المتّحدة الأميركية[٤]، ويقتضي أن يقوم البائع والزبون بإنشاء حسابٍ لكلّ منهما ضمن النظام المذكور، ويقوم الزبون بتحميل برنامج على الحاسب الآلي

---

[١] شريفة، هنية، الشيك الإلكتروني كوسيلة وفاء حديثة، مجلّة الحقوق والعلوم الإنسانية، العدد ٢٠، المجلّد الأول، ص. ١١٦.

[2] T.Verbiest et E. WERY, Le droit de l'internet et de la société de l'information, Ed. larcier,Belgique 2001, P. 313.

[٣] طارق، حمزة، المرجع السابق، ص ٧١.

[4] https://Gost.isi.edu/info/netcheque/demo.html , acceced: 01-09-2022.

العائد إليه، ويلعب البرنامج المذكور دورًا مماثلاً لدفتر الشيكات الورقي، ومن بعدها يقوم الزبون بإرسال الشيك الإلكتروني الموقّع من قبله بطريقة مشفّرة إلى البائع،

يقوم نظام الدفع NetCheque بالتأكّد من مدى صحّة الشيك الإلكتروني ومن بعدها يعطي الموافقة للتاجر ليقوم بإرسال البضائع للمشتري.

ومن أبرز الأنظمة أيضًا نظام Echeck وهذا النظام قد تمّ تجربته من قبل وزارة الخزانة الأميركية في العام ٢٠٠٠، بهدف وضع حدّ لعمليّات الاحتيال، يعمل بشكل مشابه لنظام الشيك الورقي العادي حيث يتمّ تعبئة نفس البيانات المطلوبة لإصدار الشيك الورقي، إنّما يكون الاختلاف بكيفيّة تسليم الشيك التي تتمّ إلكترونيًا، يستعمل التوقيع الرقمي المؤمّن خلال هذه العمليّة، ما يجعل من هذا النظام فعّالا وآمنًا.

من أبرز مزايا الشيك الإلكتروني هو إمكانية التأكّد من مدى توافر رصيد لدى ساحب الشيك، وهو ما يميّزه عن الشيك الورقي العادي ويساهم في الحدّ من عمليّات الإحتيال وإصدار الشيكات دون مؤونة.

ففي تونس مثلا"، فقد كشف البنك المركزي عن رفض أكثر من مليوني شيك ورقي تبلغ قيمتها ١.٤ مليار دينار (أي حوالي ٤٤١.٤٣٢.٦٠٠ دولار أميركي)، من جملة ١٢ مليون شيك (بقيمة ٥٦ مليار دينار)[١]، ونجد أنّ المشرّع التونسي يسعى بشكلٍ دؤوب لمواكبة التطوّر الحاصل في وسائل الدفع الإلكترونية وقد تمّ تقديم اقتراح قانون حمل الرقم ٢٠٢٠/٤٥ يهدف إلى تعديل النصوص المتعلّقة بالشيك الورقي التقليدي.

أمّا في مصر فقد أطلق البنك المركزي مؤخّرًا نظام مقاصّة للشيكات الإلكترونية متعدّد العملات للمساعدة بتطوير التجارة الدولية، ووفق إحصائيات البنك المذكور فقد تمّ تنفيذ عملياتٍ مالية طبقًا للنظام أعلاه تزيد قيمتها عن ٢ تريليون جينيه مصري.

٢. سند الشحن الإلكتروني

عرّفت الفقرة السابعة من المادة الأولى من اتفاقية الأمم المتّحدة للنقل البحري للبضائع بالبحر لسنة ١٩٧٨، المعروفة باتّفاقية هامبورغ، سند الشحن بأنّه "وثيقة تثبت انعقاد عقد نقلٍ وتلقي الناقل للبضائع أو

[١] تونس، رفض مليوني شيك بدون رصيد، ٢٦ ديسمبر ٢٠٢٢، عبر الرابط التالي: https://tunisie-telegraph.com، تمّ الاطلاع عليه بتاريخ: ٠٢-١٠-٢٠٢٢.

شحنه لها ويتعهّد الناقل بموجبها بتسليم البضائع مقابل استرداد الوثيقة وينشأ هذا التعهّد عن وجود نصّ في الوثيقة يقضي بتسليم البضائع لأمر شخص مسمّى أو تحت الإذن لحاملها".

وقد عرّفه الفقه[١] بأنّه " العقد الذي بمقتضاه يلتزم أحد الأشخاص، ويسمّى الناقل البحري، بتغيير مكان بضائع تُعهد إليه بحرًا إمّا لمصلحة المتعاقد معه، ويسمّى الشاحن وإمّا لمصلحة شخصٍ آخر هو المرسل إليه، وذلك مقابل أجرة". فيما اعتبره البعض بمثابة "سندٍ ممثلٍ للبضاعة المشحونة ويثبت عقد اللنقل البحري[٢]".

وقد قُضي أنّ سند الشحن يحدّد إلتزامات وحقوق أطرافه وعلى أساسه يتمّ تحديد الصفة بالدعوى كما أنّه يمثّل البضاعة ذاتها، ويعطي المستفيد منه حسب الأصول جميع النتائج الناجمة منه[٣].

وبالتالي يمكننا القول أنّ سند الشحن البحري يعتبر بمثابة الضمان القانوني بين الشاحن والناقل لإيصال البضائع إلى المرسل إليه. ونتيجة التطوّر في وسائل الإتّصال ظهر مفهوم سند الشحن الإلكتروني الذي تبنّته اللّجنة البحريّة الدوليّة في العام ١٩٩٠ سعيًا منها لوضع نظامٍ حديثٍ لسند الشحن يعتمد فقط على الوسائل الإلكترونية.

لاقت هذه المساعي انتقاداتٍ واسعة في البداية ما لبثت أن تبدّدت شيئًا فشيئًا، فبرز في شهر أيلول من العام ١٩٩٩ نظام عُرف بـِ BOLERO [٤]وهذا النظام يختصّ بإصدار سندات الشحن الالكترونية، ويرتكز على نظام التشفير بهدف حماية البيانات والتواقيع.

يتمّ التوقيع الإلكتروني في سند الشحن الإلكتروني عن طريق التشفير بالمفتاح الخاصّ الذي يُعتبر بمثابة سند الشحن الورقي، وفي حال رغب صاحب البضائع بتحويلها لشخص آخر عليه إعلام الشاحن ليصدر مفتاحًا خاصًّا جديدًا يُسلَّم لصاحب البضائع الجديد.

تكمن أهميّة سند الشحن الإلكتروني بتوفير الوقت والنفقات، وقد برزت أهميّته نتيجة انتشار فيروس كورونا حيث علقت العديد من حاويات البضائع في مرافئ متعدّدة حول العالم نتيجة عدم تمكّن صاحب

---

[١] هاني، دويدار، النقل البحري والجوي، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، ٢٠٠٨، ص. ١٦٣.

[١] بسّام، المهتار، معاهدة بروكسل وتعديلاتها، منشورات الحلبي الحقوقية ط ١ لسنة ٢٠٠٦، ص. ٣٣.

[٣] استئناف بيروت، قرار تاريخ ١٩٧٠/١١/٢١، منشور في مجلّة العدل لسنة ١٩٧٠، الجزء الثاني، ص ٣٢٠.

[٤] هو اختصار لعبارة:Bill Of Lading Electronic Registry Organisation

البضائع من استلام أصل سند الشحن يغية تمكينه من استلام بضائعه[1]، وبحسب منظمة DSCA[2] فإنّه وفي حال استبدال نصف سندات الشحن الورقية عالميًا يمكن توفير مبلغ وقدرة أربعة مليار دولار سنويًا[3].

ثانيًا: الحكومة الإلكترونية

نتيجة اجتياح الوسائل الرقمية الحديثة عالم الإدارة، ظهرت مفاهيم ومصطلحات جديدة أبرزها الحكومة الإلكترونية، والتي تهدف إلى السماح للمواطنين بإنجاز معاملاتهم الرسميّة إلكترونيًا دون الحاجة للحضور إلى الدوائر الرسميّة للدولة،

وهذا ما يساهم بتوفير النفقات على المواطن والدولة معًا، كذلك يساعد بالحدّ من الفساد ويساعد بإنجاز المعاملات بسرعة كبيرة،

في لبنان، ونظرًا للأهمّية البالغة التي تقدّمها الحكومة الإلكترونية حيث أنّ غيابها يكبّد خسائر بحوالي ١.٢ مليار دولار أميركي سنوياً حسب تقدير الشركة اللبنانية « Cedar Institute for Economic and Social Affairs»[4]، فقد سعت الحكومة اللبنانية في العام ٢٠١٨ للعمل على إطلاق مشاريع تساهم بالوصول إلى الحكومة الإلكترونية، وقد طوّر مكتب وزارة الدولة لشؤون التنمية الإدارية OMSAR[5] استراتيجية التحوّل الرقمي التي تُرجمت بحوالي ٨٠ مشروعًا تمّ اقتراحها لتقوم بالتالي كافّة المؤسسات والإدارات العامة بدمج خدماته الإلكترونية، إلا أنّ هذه الاسترتيجية لم تقرّ للأسف في مجلس الوزراءز. علمًا أنّه وبحسب إحصائيات

---

[1] Hariesh Monaadiar, The beginning of the end for the paper Bill of Lading, 25 May 2020, https://www.shippingandfreightresource.com, acceced: 10-08-2022.

[2] Digital Container Shipping Association.

[3] عبر الرابط التالي: ww.inodocs.com/blog/electronic-bill-o/f-lading-export-process، تمّ الإطلاع عليه بتاريخ: ١٠-٠٨-٢٠٢٢.

[4] محمد، جعفر، الحكومية الإلكترونية في لبنان: واقع وتحدّيات، الموقع الإلكتروني لجريدة الأخبار، عبر الرابط التالي: https://al-akhbar.com/Opinion/234668، تمّ الإطلاع عليه بتاريخ: ١٠-٠٨-٢٠٢٢.

[5] التحوّل الرقمي، مكتب وزير الدولة لشؤون التنمية الإدارية، عبر الرابط التالي: https://omsar.gov.lb/Digital-Transformation?lang=ar-lb، تمّ الإطلاع عليه بتاريخ ١٠-٠٨-٢٠٢٢..

الأمم المتّحدة يحتلّ لبنان في العام ٢٠٢٢ المرتية ١٢٢ من أصل ١٩٣ دولة، في حين أنّه كان يحتلّ في العام ٢٠٠٣ المرتبة ٦٩ عالميًا[١].

واستعمال التوقيع الإلكتروني في الحكومة الإلكترونية يتمّ في المعاملات التي يتطلّب إنجازها توقيع صاحبها، فيحلّ بذلك مكان التوقيع التقليدي.

[١] عبر الرابط التالي: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/94-Lebanon، (تمّ الإطلاع عليه بتاريخ: ١١-٠٨-٢٠٢٢)

الفصل الثاني

وسائل حماية التوقيع الإلكتروني التقنية والقانونية

بالرغم ممّا تقدّمه الثورة الرقمية من تطوّرٍ وتقدّم لا سيّما على صعيد المعاملات التجارية، إلاّ أنّ هذا الأمر يطرح في المقابل إشكاليّات تتعلّق بفقدان الأمان والإستقرار،

وقد برز في هذا المجال دور التشفيرالذي اعتبر منذ القدم من أبرز الوسائل التي حقّقت نجاحًا باهرًا في مجال تأمين السرّية والحماية في تبادل الرسائل، وقد أصبح مع الوقت معياراً للعديد من الأجهزة الحسّاسة وأنظمة الكمبيوتر، وتمّ تطويره تحت مُسمّى علم الترميز الكمّي، بهدف رفع مستوى الحماية وتوفير الأمان. ويعدّ التشفير من أبرز وسائل حماية التوقيع الإلكتروني، لا بل إنّه يدخل في صلب تصميم أحد أهمّ أنواعه وهو التوقيع الرقمي.

كذلك، فقد واجه التوقيع الإلكتروني مشكلةً أساسية تتمثّل بكيفيّة التحقّق من صحّة المفتاح العام ومعرفة هويّة صاحبه وصلاحياته، خاصّةً في إطار معاملاتٍ تتمّ بين أطرافٍ لا تعرف بعضها البعض ولم يحصل سابقًا أيّ تعامل تجاري فيما بينهم. ووهذه المشكلة تدخل ضمن إطار الأمان الذي تفتقده الصفقات المبرمة عن طريق الإنترنت وغيره من وسائل الإتّصال الحديثة. لذا فقد ظهرت الحاجة لطرفٍ ثالث يمارس دور الوسيط في المعاملات الإلكترونية، ويضطلع بتأكيد هويّة المتعاقدين، وهو ما يعرف بالتوثيق الإلكتروني والذي يقوم به مقدّم خدمات المصادقة.

ونظرًا لدوره الطليعي على صعيد أمن البيانات الرقمية، فقد سعت التشريعات لتنظيم آلية التشفير كي لا تتحوّل الفائدة المرجوّة منه إلى سلبيات تهدّد أمن الدول وتلحق الضرر بالمواطنين، كذلك فقد تضمّنت القوانين المنظّمة للتوقيع الإلكتروني نصوصًا متعلّقة بمقدّم خدمات المصادقة ومسؤوليته.

كذلك تضمّنت هذه التشريعات نصوصًا جزائية تهدف إلى صون التوقيع الإلكتروني وزجر اتلجرائم التي يمكن أن تطاله.

وسنتطرّق أدناه في المبحث الأول أدناه إلى التشفير والتوثيق وأثرهما في حماية التوقيع الإلكتروني، كذلك سنستعرض في المبحث الثاني مسؤولية مقدّمي خدمات المصادقة والحماية الجزائية للتّوقيع الإلكتروني.

المبحث الأول: التشفير والتوثيق وأثرهما في حماية التّوقيع الإلكتروني

استعمل التشفير لإخفاء معلومات سرّية تابعة لدولة معيّنة، وتوسّع إستعماله ليطال النطاق الدبلوماسي بين الدول لحماية معلومات سرية تحافظ على أمن واستقرار الدولة الداخلي والخارجي، وبالتالي كان يحظّر استعماله من قبل الاشخاص العاديين اذ انه محصورٌ بالدولة وحدها.

ونتيجة ظهور مفهوم العولمة وتطور شبكة الانترنت، الذي أدّى إلى توسّع استعمال تقنية التشفير لتخرج من مجموعة المحظورات، بحيث كان استعمالها مقتصرًا على الغايات العسكرية والدبلوماسية والسياسية، فأصبحت معمّمة تهدف للتّمكن من إتمام وتوفير سرّية وأمن الصفقات، والتعامل التجاري بين الأفراد ككلّ، فقد سعت العديد من الدّول لتنظيم التشفير وقوننته، كما سنبيّن أدناه.

الباب الأول: ماهيّة التشفير

يُعرف التشفير، عموماً، على أنّه علم كتابة الأكواد وشفرات الإتّصال الآمن، وأحد أهمّ العناصر التي يتمّ الإستناد إليها في عصر التطوّر التّكنولوجي، لا سيّما في صناعة البلوكشين والعملات الرقميّة الحديثة والعقود الذكيّة. إلاّ أنّها ليست وليدة المرحلة، بل نتيجة لتاريخ طويل منذ العصور القديمة حيث استخدمها النّاس لتشفير نقل المعلومات بطريقة آمنة.

الفقرة الأولى: مفهوم التشفير

يُطلق على التشفير تسمية CRYPTOLOGIE بالفرنسية، وهو مصطلح من أصل يوناني ويعني علم الإخفاء"Kryptos " تعني مخفي و "Logos" تعني علم[1] . وتعدّ شيفرة "أتباش" واحدة من اقدم الشيفرات التي تعتمد مبدأ استبدال الأحرف بأخرى، وقد استخدمت هذه الشيفرة قبل الميلاد بـ ٥٠٠ سنة وكانت تعتمد على اللغة العبرية لانها شفرة يهودية، ويعتقد انها استخدمت في بعض آيات التوراة.

[1]J. Stern, le maître du secret, Propos recueillis Bertrand Levergeois, Dans Humanisme 2006/4 (N° 275), pages 85 à 89, https://www.cairn.info/revue-humanisme-2006-4-page-85.htm, consulté le: 21-09-2022.

أولاً: التطوّر التّاريخي للتشفير

يعتبر التشفير كعلمٍ راسخ، له أثره التاريخي لأكثر من ألفَي عام، تمّ استخدامه بشكل رئيسي من قبل الحكومات والمؤسّسات العسكرية. ويعتبر كتاب "فاكّو الشفرات" لديفيد كان، الذي نُشر عا ١٩٦٧، بمثابة المرجع الأساسي لعلم التشفير، فقد وُصف حينها بأنّه "أول كتاب شامل يروي تاريخ الإتّصالات العسكرية"[١].

استمرّ التشفير إلى ما قبل سبعينات القرن العشرين فنًّا غامضًا، لا يفهمه أو يمارسه إلاّ القلّة من الأفراد العاملين في الحكومات والمؤسّسات العسكرية. إلاّ أنّه اليوم بات علماً ومجالاً أكاديميًا، يُدرّس في العديد من الجامعات، ويُستخدم في نطاقٍ واسعٍ، ويعود ذلك للعديد من الأسباب لعلّ أبرزها هو ظهور الإنترنت كوسيلة إتّصال بين الحكومات والمواطنين، وبين الشركات وعملائها، وحتى بين الأفراد أنفسهم. بالإضافة إلى بروز التّجارة الإلكترونية التي ازدادت انتشارًا مؤخرًا، وتُشكّل السريّة إحدى مصادر القلق التي قد تعيق الإعتماد عليها بشكل كامل.

إنّ تقنيّات التشفير، المستخدمة اليوم، ليست حديثة، فهي نتيجةٌ لتاريخٍ طويلٍ للغاية من التطوّر، يعود لحوالي أربعة آلاف سنة، وقد تمّ استعمالها من قبل الفراعنة والرومان وغيرهم من الحضارات القديمة. فالمستند الأقدم الذي تمكّن العلماء من فك شيفرته، هو وصفة قديمة لإعداد الفخّار تعود إلى القرن السادس قبل المسيح، وقد تمّ اكتشافها في العراق، وقد هدف التشفير حينها لحماية المعلومات الحسّاسة[٢].

واستخدم التشفير لاحقاً لحماية المعلومات العسكرية المهمة، بحيث اعتمدت مدينة سبارتا في دولة اليونان تشفير الرسائل من خلال نظام "سكيتال" الذي يعتمد على كتابة الرسالة على الرقّ فوق أسطوانة ذات حجم معيّن، بشكل يجعل الرسالة غير قابلة للتّفكيك ما لم يتمّ لفّها حول اسطوانة مشابهة من قبل المستلم وإلا تصبح الرسالة غير مقروءة[٣].

---

[١] فريد، بايير؛ شون، ميرفي، علم التشفير (مقدّمة قصير جداً)، ترجمة: محمد، سعد طنطاوي، مراجعة: هاني فتحي سليمان، مراجعة علمية: حاتم بهيج، مؤسسة هنداوي للتعليم والثقافة، الطبعة الأولى، مصر، ٢٠١٦، ص. ١٠.

[٢] تاريخ علم التشفير، تم النشر بتاريخ ١٤-١-٢٠١٩، عبر الرابط التالي:
https://academy.binance.com/ar/articles/history-of-cryptography، تمّ الاطلاع عليه بتاريخ: ١٢-٠٩-٢٠٢٢.

[3] J. Stern, La science du secret, Ed. Odile Jacob,Paris,1998, p. 23 .

إلاّ أنّ التشفير الأكثر تقدّماً تمّ إستخدامه من قبل الرومان، المعروف بشيفرة قيصر، وهي أبرز الشيفرات أيضًا التي عرفها العالم القديم، سمّيت كذلك تيمّنًا بيوليوس قيصر الذي استخدمها للتواصل مع قادته العسكريين، وتعتمد هذه الشيفرة على أسلوب استبدال الأحرف في الأبجدية اللاتينية، بحيث تصبح غير مقروءة للشخص الثالث. ومثال عملي على ذلك عبارة TREATY IMPOSSIBLE تصبح بعد تشفيرها: wuhdwb lpsrvvleoh، ويلاحظ بالتالي أن كافّة الأحرف في النصّ الأصلي أو النصّ الواضح قد تمّ استبدالها مع الإبقاء على الفاصل بين الكلمتين الأمر الذي يؤدّي إلى إمكانية فكّ هذه الشيفرة بسهولة[١].

إزدادت أهميّة التشفير في العصور الوسطى، واستمرّت طريقة قيصر المعيار في التشفير. بدأ تحليل الشفرات كعلمٍ يتمّ من خلاله فكّ الشفرات وحلّها. وقد طوّر كيندي، عالم الرياضيّات العربي، بتطوير تقنيّةٍ تعرف بإسم تحليل التردّد حوالي العام ٨٠٠ ميلادي، ما جعل شيفرة الإستبدال عرضة لفكّ التشفير، الأمر الذي دفع باتّجاه ضرورة تقدّم لتشفير إلى أبعد من ذلك لكي يبقى مفيداً.

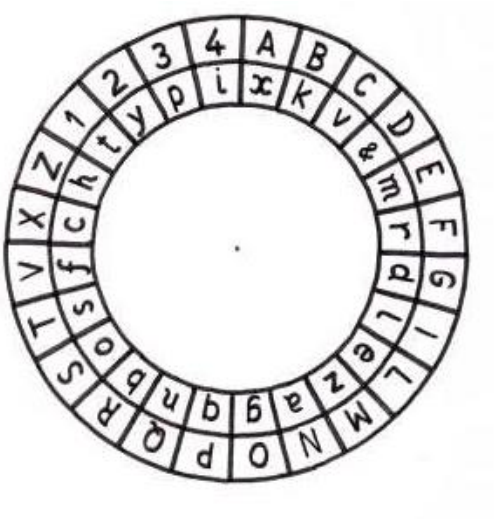
في العام ١٤٧٧ابتكر العالم الإيطالي ليون باتيستا ألبرتي، نظام تشفيرٍ يرتكز على استبدال الأحرف عن طريق قرصين، أحدهما ثابت والآخر متحرّك، فيختار مرسل الرسالة المرجع أو نقط الإنطلاق التي يريد والتي تختلف بحسب دوران القرص المتحرّك، وعلى متلقي الرسالة معرفة الأساس المعتمد من قبل المرسل لكي يتمكّن من فك شيفرتها.

وكمثال عملي، على ذلك نجد أنّه في الصورة أدناه، التي تمثّل تقنية ألبرتي، فقد تمّ اختيار (t=1) كنقطة انطلاق للتشفير فيكون بالتالي (i=4)، أمّا في حال تمّ اختيار(f=1) كنقطة انطلاق فيكون (t=4)، وهكذا دواليك. وقد اعتبرت طريقة التشفير هذه، طريقة متقدّمة ومتطوّرة جدًّا في ذاك العصر، نظراً لقدرتها على إنتاج أكثر من ٤٤٤٤ تركيبة مختلفة[٢].

---

[١] خضر، الطيطي، أساسيات أمن المعلومات والحاسوب، دار الحامد للنشر والتوزيع، الأردن، ٢٠١٠، ص. ١٩٥.

[2] M.Fabrice, Histoire de la cryptologie, P.6, disponible sur le site: https://repo.zenksecurity.com/Cryptographie%20.%20Algorithmes%20.%20Steganographie/Histoire%20de%20la%20cryptologie%20%20Introduction.pdf, consulté le: 22-09-2022.



ومع تطوّر وسائل الإتّصال وبروز التلغراف وغيرها، ابتكر صمويل موريس في العام ١٨٤٠، شيفرةً صوتية يتمّ تصويرها كتابة باستعمال النقاط والخطوط والفراغات، وقد تمّ إرسال أوّل رسالة مشفّرة عند اختراع التلغراف عام ١٨٤٤ بين مدينتي بلتمور ونيويورك. وكمثال عملي على كيفية عمل شيفرة موريس نأخذ عبارة ELECTRONIC SIGNATURE فتصبح بعد تشفيرها على الشكل التالي:

. .–.. . –.–. – .–. ––– –. .. –.–. / ... .. ––. –. .– – ..– .–. . [1]

وقد برز استعمال شيفرة موريس في الحرب العالمية الثانية، من خلال استعمال أنوار الطائرات والدبابات وحتى المشاة، وكان لها دورٌ فعّال في حسم العديد من المعارك. كذلك برزت شيفرة Enigma التي ابتكرها الألمان وعملوا على تطويرها لتخدم الغايات العسكرية منذ العام ١٩٢٦، وهي عبارة عن آلة مؤلفة من ٢٦ دوّار في الواجهة الأمامية و٢٦ آخرين في الواجهة الخلفية للآلة، ويمكن اختيار ثلاثة من أصل خمسة دوارات لربط الدوارات أعلاه الكائنة في الواجهتين الأمامية والخلفية للآلة بها، ويمكن لهذه الآلة إعطاء أكثر من مليون تشفيرة مختلفة، وقد نجح الإنكليز بفكّ شيفرة هذه الآلة في العام ١٩٤٠ عن طريق مشروع بلتشي بارك[٢].

مع إنتشار الحواسيب، بات التشفير أكثر تقدّماً، وأصبح تشفير رياضي ١٢٨ بت أقوى ممّا كان عليه في العصور القديمة والعصور الوسطى، وبات معياراً للعديد من الأجهزة الحسّاسة وأنظمة الكمبيوتر. وبدأ العلماء

[1] https://md5decrypt.net , acceced:21-09-2022.

[2] https://bletchleypark.org.uk/our-story/enigmas-of-bletchley-park/ , acceced:21-09-2022.

منذ العام ١٩٩٠ يطوّرون شكلاً جديداً تماماً من التشفير، يُطلق عليه علم الترميز الكمّي، يهدف لرفع مستوى الحماية الذي يوفّره التشفير الحديث.

وحالياً، جرى الإعتماد بشكل كبير على تقنيات التشفير وتطويرها، لجعل إنشاء العملات الرقمية شيئاً ممكناً، وهي تستفيد من تقنيات التشفير المتطوّرة مثل: دالة الهاش وتشفير المفتاح العام التواقيع الرقمية، وهي تقنيات تستخدم، في المقام الأول، لضمان أمن البيانات المخزّنة على البلوكشين والمصادقة على المعاملات.

على الرغم من أنّ أنظمة التشفير المستخدمة في بلوكشين والعملات الرقمية، تعتبر الأكثر تقدماً في علم التشفير، إلاّ أنّها تبقى جزءًا من تقليدٍ يمتدّ عبر التاريخ، عرف فيه التشفير شوطاً طويلاً من التطوّر من الـ ٤٠٠٠ سنة الماضية حتى يومنا هذا، وليس من المرجّح أن يتوقّف عن التقدّم في أيّ وقتٍ قريب.[١]

ثانياً: تعريف التشفير

عرّف قاموس داللوز التشفير بأنّه "مجموعة تقنيات معدّلة لبيانات معلوماتية بهدف حماية عملية إرسال واستقبال المعلومات التي تحملها. وتتمّ هذه العملية عن طريق رموزٍ سريّة (تسمّى "مفاتيح" أو "اتفاقيات سريّة") بحيث يصبح مرقّم أو مشفّر غير مفهوم بالنسبة للأشخاص الثالثين.[٢] كذلك عرّفه بعض الفقهاء بأنّه "عملية تحويلٍ معلومة مفهومة إلى معلومة غير مفهومة عن طريق بروتوكولات سرّية قابلة للإنعكاس"[٣].

أمّا على مستوى القوانين الوضعية فقد عرّفت الفقرة الأولى من المادة ٢٨ [٤]من القانون الفرنسي رقم ٩٠/١١٧٠ تاريخ ١٩٩٠/١٢/٢٩ التشفير بأنّه "جميع التقديمات التي ترمي بفضل اتفاقيات سرّية إلى تحويل

---

[١] تاريخ علم التشفير، تم النشر بتاريخ ١٤-١-٢٠١٩، عبر الرابط التالي:
https://academy.binance.com/ar/articles/history-of-cryptography، تمّ الاطلاع عليه بتاريخ: ١٢-٠٩-٢٠٢٢.

[2] Dictionnaire Du Web, 1ère édition, Éd.Dalloz, Paris 2001, P. 66.

[3] V. Sedaillan, Droit de l'internet, Éd. Net press, collection AUI, Paris 1997, P.171.

[4] Art. 28: "I. On entend par prestations de cryptologie toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet."

معلوماتٍ أو إشاراتٍ مفهومة إلى معلوماتٍ وإشاراتٍ غير مفهومة، أو القيام بالعمليّة المعاكسة، وذلك بفضل استخدام معدّات أو برامج مصمّمة لهذه الغاية".

كذلك عرّفت الفقرة ٩ من المادة ١ من اللائحة التنفيذية للقانون المصري رقم ٢٠٠٤/١١٥ الصادرة بتاريخ ٢٠٠٥/٥/١٥ بأنّه: "منظومة تقنية حسابية تستخدم مفاتيح خاصّة لمعالجة وتحويل البيانات والمعلومات المقروءة الكترونيًا، بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فكّ الشفرة".

أمّا المشرّع التونسي فقد عرّف التشفير في الفقرة ٥ من الفصل ٢ من الباب الأول من قانون المبادلات والتجارة الإلكترونية رقم ٢٠٠٠/٨٣ بأنّه "استعمال رموز أو إشارات غير متداولة، تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قبل الغير، أو استعمال رموز أو إشارات لا يمكن وصول المعلومات بدونها."

يستنتج ممّا ورد أعلاه أنّ معظم التعريفات قد ركّزت على هدف ودور التشفير دون التركيز على الوسائل التي تعتبر من العمليّات التقنية الدقيقة. باستثناء المشرّع المصري الذي يتبيّن لنا من خلال مراجعة التعريف أعلاه أنّه قد أوضح الطريقة المستخدمة في التشفير من خلال ذكره لمفتاح أو مفاتيح فكّ الشفرة أي وبمعنى آخر المفتاح العمومي الذي لنا عودة إلى تعريفه وشرح كيفيّة عمله عند تناولنا مسألة تقنيّات التشفير.

وسنبحث أدناه بوسائل التشفير المستعملة حديثا"، مبيّنين أهمّيتها لناحية تأمين سرية وحماية المعاملات والمعلومات التي يتم تبادلها على شبكة الانترنت، والتي لا تنحصر فقط بسلامة التبادل الالكتروني على الشبكة الرقمية بل تتخطاها لتوفر أيضًا إحدى دعامات الاثبات المعلوماتي، باعتبار انها تتثبّت من مضمون النصوص المتبادلة، من مرسلها، من التوقيع الالكتروني عليها، أي التحقق من خلوها من أيّة عيوبٍ لدى تبادلها ضمن شبكة الانترنت.

فلدى توافر هذه المقوّمات الأساسية يمكننا عندها التوسّع في إتمام المعاملات وتبادل المعلومات الشخصية والسريّة على الشبكة، كالدفع بطريقة آمنة عبر وضع معلومات عن البطاقات المصرفية دون الحؤول لتسريب وقرصنة هذه المعلومات، اتمام الصفقات، تبادل العقود وغيرها من المعاملات.

ثالثاً: تقنيات التشفير ووظيفته

يرتكز التشفير، عموماً، على العديد من التقنيات المُستخدمة، والتي تهدف الى تحقيق العديد من الوظائف، إلا أنّ ما يهمّنا هو شرح الوظيفة المتمثّلة بإثبات هوية المرسل وموثوقية الرسالة.

١. تقنيّات التشفير

عرف التشفير العديد من التقنيّات، إلّا أنّ أبرزها يتمثّل في التشفير المتماثل، والتشفير غير المتماثل، والتشفير باستعمال المفتاح العام والظرف الرقمي.

أ. تقنية التشفير المتماثل

تستخدم هذه التقنية المفتاح الخصوصي بحيث يستخدم هذا المفتاح أو الرمز السرّي ذاته في تشفير الرسائل وفي فكّ تشفيرها، أي وبمعنًى آخر إنّ هذا النظام يعمل بواسطة مفتاح واحد يمتلكه كلّ من مرسل ومتلقّي الرسالة.

والنظام الأكثر شهرة بالنسبة لهذه التقنية هو نظام DES (بالإنجليزية: Data Encryption Standard) المصمّم من قبل هورست فستل Horst Feistel والذي قامت شركة IBM بتطويره في العام ١٩٧٦، وقد اعتمد كمعيارٍ للتشفير من قبل الإدارة الأميركية في العام ١٩٧٧. يعمل هذا النظام عن طريق تغيير تسلسل الأحرف واستبدالها بأحرفٍ أخرى بحيث يكون مفتاح التشفير عبارة عن أرقامٍ جزافية ذات طول محدّد تنتجها برامج معلوماتية بالإستناد إلى نواة معيّنة مثل ساعة وتاريخ إنتاج المفتاح[١].

وعمليًا، فهو عبارة عن خوارزمية لتشفير كتل البيانات عن طريق استخدام المفتاح المتماثل، وهو كود تشفير بطول (٦٤ بت) ويستخدم منه فقط (٥٦ بت) لعمليّة التشفير، أمّا أوّل (٨ بت) فتستخدم للتدقيق في الأخطاء، وتحتوي الخوارزمية على ١٦ دورة تتكرّر فيها عملية استبدال الأحرف والتبديل بين أماكنها حتى تنتج النص المشفّر.

لاقت هذه التقنية انتقاداتٍ كثيرة نظرًا لأضرار متلقي الرسائل المشفّرة من اقتناء عددٍ كبيرٍ من المفاتيح الخصوصية، فضلا عن أنّ استعمال المفتاح نفسه من قبل المرسل والمرسل إليه من شأنه أن يضعف حجّية

[١] وسيم الحجار، المرجع السابق، ص. ٢٠٢.

المستند الرقمي نظرًا للخطر من تسريب هذا المفتاح لأشخاصٍ ثالثين بشكلٍ غير مشروع ولعدم إمكانية تحديد حدوث التسريب أو هويّة المسرّب[١].

كذلك فإنّ هذه التقنية لا تشكّل مصدر أمانٍ نظرًا لحجم المفتاح (٥٦ بت) الذي يعتبر صغيرًا في ظلّ التطوّر الذي يشهده عالمنا اليوم في ميدان الإتصالات والتكنولوجيا، وقد تمّ سحب نظام DESكمعيار من قبل المعهد الوطني للمعايير والتكنولوجيا (NIST) بعد أن تمّ كسر هذا التشفير في العام ٢٠٠٨، وتمّ استبداله بمعيار التشفير المطوّر (Advanced Encryption Standard) ويشار له بالإختصار (AES) في أغلب الإستخدامات[٢]، ويعتمد هذا النظام على تقنية تشفير الكتل (Block Cipher)، أي إنّها تعمل على تقسيم النص إلى كتلٍ بحجم ٦٤ بت وأحيانًا ١٢٨ بت ويتمّ تشفير كلّ كتلة من هذه الكتل على حدة.

بعد تقسيم النصّ إلى كتل، وفي حال لم يبلغ حجم الكتلة الأخيرة نفس حجم باقي الكتل يتمّ استخدام مفهوم الحشو (Padding)، وهو يعمل على إضافة بايتات إضافية للكتلة الناقصة بحيث تصبح جميع كتل النصّ بالحجم ذاته. كذلك فقد تمّ انتقاد تقنية التشفير بالكتل بكونها بطيئة ويكون من السهل فكّ شيفرتها في حالة تكرار بعض الكلمات في النصّ الأصلي، الأمر الذي يتطلّب في هذه الحالة مزيدًا من العمل التقني واستعمال ما يُعرف بِـ feedback modes ومن أبرز أساليب هذه التقنية هو Cipher block chaining والمعروف باختصار CBC[٣]،

وهناك أيضًا نوع آخر من التشفير المتماثل وهو التشفير المتدفّق (Stream Cipher) والذي يتميّز عن نظام التشفير بالكتل بكونه أسرع وأسهل في كتابة تشفيراته كذلك يمكنه تفادي مشكلة تكرار الكلمات في النصّ التي سبق الإشارة إليها أعلاه كونه يقوم بتشفير كلّ بتّ على حدة، وشيفرات التدفّق لا تسمح باستخدام المفتاح سوى مرّةٍ واحدة بخلاف نظام تشفير الكتل الذي يسمح باستخدامه عدّة مرّات، ومن أبرز أنواع شيفرات التدفق نظام RC4.

---

[١] طوني، عيسى، المرجع السابق، ص. ٢٠٢.

[2] https://www.lri.fr/~fmartignon/documenti/systemesecurite/4-DES.pdf

[٣] وجدي، عصام عبد الرحيم، مقدمة في علم التشفير بالطرق الكلاسيكية، بدون دار نشر، ٢٠٠٧، ص. ١٠٠ إلى ١٠٣ (تمّ تحميله بصيغة PDF عبر الرابط التالي: https://down.ketabpedia.com/files/bnr/bnr14599-1.pdf ، تمّ الإطلاع عليه بتاريخ ١١-١٠-٢٠٢٢.

ب. التشفير غير المتماثل

يقوم هذا النظام على استخدام مفتاحين مختلفين أحدهما يسمّى بالمفتاح العام، الذي يمكن للجميع معرفته والآخر بالمفتاح الخاص، وهو مفتاح سرّي لا يعرفه إلا مرسل الرسالة، يتمّ تشفير الرسالة باستعمال المفتاح العام وإرسالها إلى المستخدم الذي يملك المفتاح الخاص وبالتالي يكون وحده القادر على فكّ الرسائل والتفرّد بقراءتها مستخدمًا المفتاح الخاص.

وكان العالمان Diffe و Hellman أول من عمل على وضع مشروع هذه التقنية، وقد تمّ إطلاق أوّل نظام تشفيري بالمفتاح العمومي من قبل ثلاثة باحثين في من جامعة MIT الأميركية وهم Ronald rivest و Adi Shamirو Leonard Adeleman وقد سمّي هذا النظام RSA تيّمنًا بهم إذ حمل أول حرف من شهرة كلّ واحد منهم.

وفي العام ١٩٨٥، قام العالمان Neal Koblitz من جامعة واشنطن و Victor Miller من مركز بحوث شركة IBM، بالبحث في أحد فروع علم الرياضيات المعروف بالمنحنى الإهليجي أو Elliptic Curve فتوصّلوا إلى إمكانيّة استعمال هذا الفرع في تشفير المفتاح العام، وقد بدأ هذا النوع من الخوارزميات بالظهور فعليًا في بداية تسعينيات القرن الماضي، والذي يعتبر أسهل وأكثر فعالية من أنظمة التشفير الأخرى ويعدّ من أنسب الأنظمة التي يمكن استعمالها في الاتصالات المتحرّكة كأنظمة الهواتف النقّالة[١].

ارتكزت معظم أنظمة التشفير المعروفة حاليًا وكذلك برامج الدفع الإلكتروني الآمن عن بعد مثل Netscape و Digicashعلى نظام التشفير RSA السالف الذكر وعلى غيره من الأنظمة المشابهة، ولعلّ أبرز برنامج في هذا المجال والذي أجمع معظم العلماء على شبه استحالة اختراقه هو نظام Pretty Good Privacy المصمّم من قبل الأميركي فيل زيمرمان في العام ١٩٩١.

يوفّر نظام التشفير غير المتماثل إيجابيات على المستويين العملي والقانوني، فهو من جهة يسهّل على المستخدم عملية إرسال الرسائل الذي يتمّ باستعمال مفتاحٍ واحد كذلك يضمن أمن الرسائل المتبادلة وموثوقيتها

[١] أحمد، خضور – منظومة تقنية لتأمين أمن تبادل المعلومات– مجلة جامعة دمشق للعلوم الهندسية– المجلد الرابع والثلاثون– العدد الثاني– ٢٠١٨– منشور على الرابط التالي:
معاينة منظومة تقنية لتأمين أمن تبادل المعلومات(damascusuniversity.edu.sy) تمّ الإطلاع عليه بتاريخ ١٢-٠٩-٢٠٢٢).

فيحول دون إمكانية من يحمل المفتاح الخصوصي إنكار إرساله الرسائل طالما أنّه يملك وحده المفتاح المستخدم[١].

وتبقى الصعوبة الوحيدة في هذا المجال هو مسألة ضمان أنّ المفتاح العمومي عائد فعليا إلى المستخدم الحائز على المفتاح الخصوصي، وهنا يبرز دور مقدّم خدمات المصادقة لحلّ هذه الإشكالية، ولنا عودة لشرح دور هذه السلطات ومسؤوليتها في الباب الثاني أدناه.

ج. التشفير باستعمال المفتاح العام والظرف الرقمي

تجمع هذه التقنية بين طريقتي التشفير المذكورتين أعلاه، وتقدّم بعض الحلول للصعوبات التي تعتري كلاً منهما، فيقوم المرسل في هذه الحالة بالاستحصال على المفتاح العام للمرسل إليه وهذا المفتاح يكون بطبيعة الحال معروفًا للجميع كما أسلفنا أعلاه، ثمّ يقوم وبشكلٍ عشوائي بإنشاء مفتاحٍ متماثل يتمّ استخدامه في عمليّة تشفير البيانات، ويستخدم المرسل المفتاح العام لتشفير المفتاح المتماثل، من بعدها يقوم المرسل بإرسال المفتاح المشفّر والرسالة إلى المرسل إليه الذي يقوم بدوره باستعمال مفتاحه الخاصّ لفكّ تشفير المفتاح المشفّر بعدها يقوم بفك تشفير الرسالة..،

وبهذه الطريقة يمكن حلّ مشكلة توزيع المفاتيح التي تعتري تقنية التشفير المتلازم من جهة ، ومن جهة أخرى يمكن توفير السرعة التي تفتقدها تقنية التشفير غير المتلازم، إذ إنّه وبالتشفير المتناظر يمكننا تشفير ٥٠ ميغا بايت في الثانية في حين أنّه وبالتشفير غير المتناظر يمكن فقط تشفير بين ٢٠ و ٢٠٠ كيلو بايت في الثانية الواحدة[٢]. وسنتطرّق أدناه إلى المساعي المبذولة من الدول لتنظيم التشفير وقوننته.

٢. وظيفة التشفير في اثبات هوية المرسل وموثوقية الرسالة

يساعد التشفير في إثبات هويّة مرسل الرسالة كما والتأكّد ممّا إذا كانت قد طرأ على الرسالة أي تعديل ناتج عن عملية قرصنةٍ طالتها، ويتمّ هذا الأمر عن طريق اتّباع الخطوات التالية من المرسل والمرسل إليه:

---

[١] طوني، عيسى، المرجع السابق، صفحة ٢٠٤.

[2] What is a digital envelope? , www.security.nknu.edu.tw/crypto/faq/html/2-2-4.html , acceced: 29-09-2022.

يقوم المرسل بداية بكتابة الرسالة التي يريد ويقوم بإدخالها في أحد التطبيقات[1] التي تهدف إلى استخراج الناتج من الرسالة أو ما يُعرف بال hash ثمّ يقوم المرسل بتشفير الهاش عن طريق المفتاح الخاص به ويرسلها بعد ذلك إلى المرسل إليه الذي يقوم بدوره بفكّ التشفير عن طريق المفتاح العام للمرسل، في حال نجاحه بهذا الأمر يكون قد تثبّت من هويّة المرسل، كذلك يقوم بتطبيق الدالة الهاشية التي طبّقها المرسل على الرسالة وفي حال تساوت مع الهاش يتثبّت بالتالي من عدم حصول أي تغيير بمحتوى الرسالة أثناء إرسالها.

الفقرة الثانية: التشفير في القوانين الوضعية

يشكّل التشفير وسيلة فعّالة لتأمين سريّة الرسائل وموثوقيتها إلا أنّ استعماله خارج هذه الأهداف يمكن أن يشكّل خطرًا على أمن الدول. وهذا الأمر تنبّهت له الدول منذ عدّة سنوات، فقد تناولت قمّة مجموعة الدول الصناعية السبع "G7"، المنعقدة في تمّوز ١٩٩٦، والمتعلّقة بمكافحة الإرهاب، هذه المسألة مقترحة أن يتمّ تسريع الإستشارات المتعلّقة بالوصول القانوني للحكومات إلى البيانات المشفّرة بغية مكافحة الإرهاب مع المحافظة على الطابع الخصوصي للإتصالات الشرعيّة[2].

ويرى البعض[3] في هذا السياق أنّ القيود الموضوعة من الدول وعدم وحدة المعايير فيما بينهالا تأتلف مع طبيعة التعاملات التجارية وتشكّل عقبةً بوجه التشفير،

وسنعالج أدناه موقف القانون الفرنسي من التشفير (أولاً)، وموقف التشريعات العربية منه (ثانيًا) والقانون اللبناني (ثالثًا).

أولاً: موقف القانون الفرنسي

صنّف المرسوم الصادر بتاريخ ١٩٣٩/٤/١٨ التشفير ضمن فئات الأسلحة الحربية، وقد ظلّ التشفير في فرنسا محصورًا بالغايات الدبلوماسية والعسكرية والحكومية لغاية العام ١٩٩٠، حين أصدر المشرّع الفرنسي

---

[1] مثال MD5 و SHA-1

[2] Marie- Christine Piatu, Les Libertes individuelles à l'epreuve des NTIC- Editions Presses Universitaires de Lyon – Pul- 2001, p. 132.

[3] Vincent Grautrais- Le contrat electronique international- Editions Bruylant, Bruxelles, 2002, p. 123.

القانون رقم ٩٠/١١٧٠ المذكور أعلاه بهدف تشريع التشفير، وذلك بناءً لضغوط مورست من قبل المستخدمين الذين اعتبروا منع التشفير يشكل تعدّيًا على حرّيتهم الشخصية ويعرقل عجلة التبادل عن طريق الأنظمة المعلوماتية ولا سيّما التجارة الإلكترونية.

وقد صدر لاحقًا بتاريخ ١٩٩٢/١٢/٢٩ المرسوم التطبيقي رقم ٩٢/١٣٥٨٠ الذي حدّد دقائق تطبيق القانون السالف الذكر رقم ٩٠/١١٧٠ واضعًا أصولاً وشروطًا حازمة لعمليّة التشفير. إلا أنّ هذا القانون، وعلى الرغم من كونه شرّع استعمال وسائل التشفير للغايات المدنية والتجارية، إلا أنّه أبقاها خاضعة لرقابة أجهزة الدولة وموافقتها المسبقة، فكانت الملفات تدرس من قبل الخدمة المركزية لأمن أنظمة المعلومات SCSSI وهو جهازٌ مرتبطٌ بالأمانة العامة للدفاع الوطني SGDN.

وبناءً على توصية المجلس الأوروبي الصادرة في ١١ أيلول ١٩٩٥ والمتعلّقة بحماية الأشخاص الطبيعيين لناحية معالجة البيانات ذات الطابع الشخصي وحرّية حركة هذه البيانات[1]، أصدر المشرّع الفرنسي قانونًا بتاريخ ١٩٩٦/٧/٢٦ ونشرت مراسيمه التطبيقية في شباط وآذار ١٩٩٨، وقد حاول القانون المذكور تليين القيود المفروضة بموجب القانون الصادر عام ١٩٩٠، إلا أنه لم يسلم من انتقادات الأخصائيين في هذا المجال كون كلفته باهظة وهو قاس مقارنة مع تشريعات دول أخرى، كما واجه هذا القانون انتقادات لناحية حجم التشفير الذي ظلّ محصورًا بـ 40 BITS [2].

وقد عدّل هذا القانون نصّ المادة ٢٨ من قانون عام ١٩٩٠ ، كما تضمّن تبسيطًا لشكليات الترخيص المسبق، وفرّق بين استعمال برامج ووسائل التشفير داخل الأراضي الفرنسية الذي أصبح حرًّا شرط استيفائه لشروط محدّدة وبين تصدير هذه البرامج أو استيرادها الذي ظلّ خاضعًا لنظام الإجازة المسبقة والتصاريح. كذلك نصّ على حريّة استعمال وسائل التشفير إذا كانت وسيلة التشفير لا تهدف إلى تحقيق وظيفة السريّة أي

[1] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,JO n° L 281 du 23/11/1995 p. 0031 – 0050, disponible sur le site:https://eur-lex.europa.eu/, consulté le: 17-09-2022.

[2] C. Feral Schuhl, cyberdroit – le droit à l'épreuve de l'internet, 5ème edition, éd. Dalloz, Paris 2009-2010, P. 657.

في الحالة التي تهدف فيها فقط للتأكّد من هوية الفرقاء أو مراقبة موثوقية الرسالة. أمّا إذا كانت وسيلة التشفير تؤمّن وظيفة السريّة فيقتضي ألّا يتجاوز حجم التشفير ٤٠ بت.

وفي حال تراوح حجم التشفير بين ٤٠ بت و١٢٨ بت يُشترط أن تكون وسيلة أو برنامج التشفير قد استحصل على موافقة مسبقة أو في حال كانت هذه الوسيلة أو البرنامج مخصّصان حصرًا لاستعمال شخصٍ طبيعي. أمّا في حال تجاوز حجم التشفير حجم ١٢٨ بت يقتضي أن تكون مفاتيح التشفير وفكّ التشفير بعهدة شخصٍ ثالثٍ موثوق به (Tiers de confiance) أو بالإنكليزية TTP (Trusted third party)، والذي حدّد المرسوم رقم ١٠٢ – ٩٨ تاريخ ٢٤ شباط ١٩٩٨ شروط تعيينه[1]، علمًا أنّ الشخص الثالث الموثوق يختلف عن مقدّم خدمات المصادقة على التوقيع الإلكتروني التي سنتطرّق إليه في الفصل من دراستنا، وقد حدّد المرسوم أعلاه الشروط الواجب توافرها في الشخص الموثوق به وهي التالية:

أ. استخدام ستّة أشخاص مؤهلين من الدولة على الأقلّ، على أن يكون اثنان منهما على جهوزية تامّة طوال الأربع والعشرين ساعة من كلّ يوم.
ب. اعتماد بنية تحتيّة ذات درجة عالية من الأمان، تحدّد في دفتر الشروط.
ج. التقيّد بالموجبات المختصّة بالعقد المبرم بينه وبين مستعمل تقنية التشفير وبموجب السرّية وبمسك سجلات إلزامية.

في العام ١٩٩٩ بدأت عمليّة تحرير وسائل التشفير لضمان سريّة الرسائل المتبادلة بشكلٍ تدريجي وتامّ، وقد بدأت الرحلة الأولى في آذار ١٩٩٩ حيث صدر المرسومان رقم ٩٩/١٩٩ و٩٩/٢٠٠ كذلك صدر قرار بتاريخ ١٩٩٩/٣/١٧، وهذه النصوص قد استجابت بشكل سريع للانتقادات التي تعرّضت إليها النصوص الصادرة عام ١٩٩٨ بهذا الخصوص والتي سبق وأشرنا إليها أعلاه، ففي مرحلة الأولى، وبموجب هذه النصوص تمّ تحرير استعمال وسائل التشفير لغاية ١٢٨ بت.

وفي ٢٠٠١/٧/١١ صدر القانون رقم ٢٠٠١/٦١٦ الذي عدّل نصّ المادة ٢٨ المذكورة أعلاه مرّة جديدة كذلك تمّ تعديل المراسيم التطبيقية المتعلّقة بالتشفير بموجب المرسوم رقم ٦٩٣ تاريخ ٢٠٠١/٧/٣١، وقد نصّ القانون ٢٠٠١/٦١٦ على حريّة استعمال وسائل التشقير غير المتعلّقة بتأمين سريّة المعلومات كذلك الوسائل المتعلّقة بالسرّية إذا كانت تتمّ إدارة مفاتيح التشفير وفق إجراءات محدّدة ومن قبل هيئة معتمدة رسميًا. من جهةٍ

[1] C. Feral Schuhl op. cit p. 698.

أخرى اعتبر قانون العام ٢٠٠١ أنّ استيراد وتوريد وسائل التشفير إلى بلد خارج الإتحاد الأوروبي يخضع لترخيص مسبق من رئيس مجلس الوزراء.

ثانياً: التشفير في القوانين العربية

أشارت العديد القوانين العربية إلى التشفير، والتي هدفت عموماً لحماية وتنيظم خدمات الإتصالات، لاسيّما في ظل تنامي التطوّر التكنولوجي، فعمدت إلى بناء بُنى تحتية تنسجم وتساير التقدّم، سنستعرض منها موقف كل من القانونين المصري، والتونسي.

١. موقف القانون المصري

نصّت المادة الثانية من قانون ١٥- ٢٠٠٤ على إنشاء هيئة تنمية صناعة تكنولوجيا المعلومات تحت وصاية الوزير المختصّ في القطاع، وقد أوكل إلى هذه الهيئة مهام تنمية وتنظيم خدمات الاتصالات وتكنولوجيا المعلومات وزيادة فرص تصدير هذه الخدمات وذلك وفق ما جاء في المادة الثالثة من القانون عينه.

وقد أصدر وزير الاتصالات المصري الدكتور طارق كامل قرارًا بتاريخ ٢٠٠٥/٥/١٥ تحت الرقم ١٠٩ التي عرّفت التشفير كما سبق بيانه أعلاه كذلك عرّفت تقنية شفرة المفتاح العام والخاص، المفتاح الشفري العام، المفتاح الشفري الخاصّ والمفتاح الشفري الجذري في الفقرات ١٠ لغاية ١٣ من المادة ١ من القرار أعلاه. وتمّ تعديل اللائحة التنفيذية السالفة الذكر بموجب القرار رقم ٣٦١ تاريخ ٢٠٢٠/٤/١٩ الصادر عن وزير الاتصالات وتكنولوجيا المعلومات المصري الدكتور عمرو سميح طلعت لتتلاءم مع التطوّر في قطاع الاتصالات والمعلوماتية، وسنأتي على ذكر التعديلات الحاصلة بموجب هذه اللائحة في الفقرات اللاحقة من دراستنا.

من جهةٍ أخرى نصّت المادة ٦ من الفصل الرابع من مشروع قانون التجارة الإلكترونية المصري على ما يلي: "تحدّد اللائحة التنفيذية القواعد والضوابط الخاصّة بتشفير المحرّرات الإلكترونية والتوقيع الإلكتروني وبطاقات الإئتمان وغير ذلك من البيانات التي يتمّ تحريرها أو نقلها أو تخزينها على وسائط الكترونية"، وقد نصّت المادة ٧ من المشروع من الفصل الرابع من مشروع القانون عينه على ما حرفيته:

" تحدّد اللائحة التنفيذية أنواع وبرامج التشفير المسموح باستيرادها أو تصنيعها محليًّا دون ترخيص مسبق من الوزارة المختصّة كما تحدّد إجراءات ترخيص ما عدا ذلك من أجهزة وبرامج التشفير".

كذلك نصّت المادة ٢٢ من قانون مكافحة جرائم تقنية المعلومات المصري الصادر في ١٤ آب ٢٠١٨ على تجريم إستخدام خدمات التشفير إذ نصّت على ما يلي:

"يعاقب بالحبس مدة لا تقل عن سنتين وغرامة بين ٣٠٠ – ٥٠٠ ألف جنيه كل مَن حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدر أو تداول أي جهاز أو معدات أو برامج أو أكواد مرور أو شفرات أو أي بيانات مماثلة، بدون تصريح من الجهاز [١] أو مسوغ من الواقع أو القانون، وثبت أن ذلك السلوك كان بغرض استخدام أي منها في ارتكاب أية جريمة من المنصوص عليها في هذا القانون أو إخفاء أثرها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء".

كما نصّت المادة ٦٤ من قانون تنظيم الاتصالات رقم ١٠ تاريخ ٢٠٠٣/٢/١٧ على وجوب الاستحصال موافقة كتابية من الجهاز القومي لتنظيم الاتصالات والجيش وسلطات الأمن القومي من أجل استخدام أجهزة التشفير.

من خلال مراجعة النصوص السالفة الذكر نجد أنّ المشترع المصري قد أولى أهميّةً كبيرةً للتشفير، كذلك سعى لتخطي عقبة جمود القوانين مواكبةً للتطوّر السريع في مجال الاتصالات والتكنولوجيا عن طريق إنشاء هيئة تنمية صناعة تكنولوجيا المعلومات وأولاها المهامّ المذكورة أعلاه، وهذا ما عزّز مكانة مصر في ميدان تكنولوجيا المعلومات.

٢. موقف القانون التونسي

أنشأ المشرّع التونسي بموجب الفصل الثامن من القانون رقم ٢٠٠٠/٨٣ المتعلّق بالمبادلات والتجارة الإلكترونية "الوكالة الوطنية للمصادقة الإلكترونية" وهي مؤسسة عمومية لا تكتسي صبغة إدارية وتتمتّع بالشخصية المعنوية وبالاستقلال المالي وتتولّى هذه المؤسسة منح التراخيص لمزوّدي خدمات التجارة الإلكترونية على كامل تراب الجمهورية التونسية وتحديد مواصفات منظومة إحداث الإمضاء والتدقيق وتخضع لإشراف الوزارة المكلّفة بالقطاع وفق ما جاء في الفصل التاسع من القانون عينه، علمًا أنّ منظومة إحداث الإمضاء المذكورة هي "مجموعة وحيدة من عناصر التشفير الشخصية أو مجموعة من المعدّات المهيأة خصيصًا لإحداث إمضاء إلكتروني.

[١] الجهاز القومي للإتصالات

أمّا منظومة التدقيق في الإمضاء فهي "مجموعة من عناصر التشفير العمومية أو مجموعة من المعدّات التي تمكّن من التدقيق في الإمضاء الإلكتروني"، كما جاء في الفصل ٢ من القانون رقم ٢٠٠٠/٨٣، كذلك نصّ الفصل ٣ من القانون السالف الذكر على إخضاع استعمال التشفير في المبادلات والتجارة الالكترونية عبر الشبكات العمومية للاتصالات إلى التراتيب الجاري بها العمل في ميدان الخدمات ذات القيمة المضافة للاتصالات.

وقد جاء في الفصل ١١ من الأمر رقم ٥٠١ /١٩٩٧ تاريخ ١٩٩٧/٣/١٤ المتعلّق بالخدمات ذات القيمة المضافة من أن "مزوّد الخدمة يسعى إلى الحصول على ترخيصٍ من الوزير المكلّف بالمواصلات لبث المعلومة المشفّرة وترتبط شروط الحلول على رخصة الاستغلال الشفرة بقرار من وزير المكلف بالاتصالات."

ومن الناحية الجزائية تعاقب المادة ٨٧ من القانون رقم ٢٠٠١/١ تاريخ ٢٠٠١/١/١٥ " بالسجن لمدة تتراوح بين ستة أشهر وخمس سنوات وبخطية من ألف إلى خمسة آلاف دينار أو بإحدى هاتين العقوبتين، كلّ من استعمل أو صنع أو استورد أو صدر أو حاز لأجل البيع أو التوزيع مجانا أو بمقابل أو عرض للبيع أو باع وسائل أو خدمات التشفير أو أدخل تغييرا عليها أو أتلفها دون مراعاة أحكام الأمر المنصوص عليه بالفصل ٩ من هذه المجلة،" وقد نصّ الفصل ٩ المذكور على ما حرفيته: "تضبط بمقتضى أمر شروط وإجراءات استعمال وسائل أو خدمات التشفير عبر شبكات الاتصالات وكذلك شروط تعاطي الأنشطة ذات العلاقة."

من خلال مراجعتنا هذه النصوص يتبيّن أنّ المشرّع التونسي قد أخضع تنظيم برامج وتقنيات التشفير لسلطة التصديق التي أولاها إلى الوكالة الوطنية للمصادقة الإلكترونية من جهة وإلى رقابة الوزارة المكلّفة بالقطاع من جهةٍ أخرى.

ثالثاً: موقف القانون اللبناني

رغم أهميّته، لم ينظّم المشرّع اللبناني التشفير في أيّ من قوانينه الوضعية، بل تمّ ذكر هذا المصطلح بشكل عابر في بعض القوانين كنصّ المادتين ١٩٧ و١٩٨ من المرسوم الإشتراعي رقم ١٢٦ تاريخ ١٩٥٩/٦/١٢ المعدّل، والمتعلّق بتنظيم الأصول الإدارية والمالية في المديرية العامة للبريد والبرق حيث سمحت بقبول برقيات محرّرة بعبارات رمزية.

كما ورد مصطلح التشفير بشكلٍ عابر، في بعض النصوص مثال القرار الصادر عن حاكم مصرف لبنان رقم ١١٤٤٥ تاريخ ٢٠١٣/٦/٦، إلا أنّ هذه النصوص لا يمكن أن تطبق على وسائل وأدوات التشفير، والملفت أنّ قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي رقم ٢٠١٨/٨١ قد خلا من تعريف التشفير ولم يأت حتى على ذكره.

على الرغم الخطورة التي يشّكلها التشفير من جهة، وكونه وسيلة فعّالة لضمان أمن وموثوقية الرسائل من جهة أخرى،

وتجدر الإشارة إلى أنّ القرارات القضائية الصادرة في لبنان قد أبرزت الخطورة التي تمثّلها تقنيات التشفير نظرًا لاستخدامه كوسيلة تواصلٍ بين العصابات الإجرامية، الأمر الذي يوجب تدخّل المشرّع لقوننته.

وبالفعل يتبيّن من خلال مراجعة القرار الإتهامي الصادر عن المحقق العدلي الصادر بتاريخ ١٠ تموز من العام ٢٠٠٠ في الأحداث الإرهابية التي حصلت في منطقة الضنية– شمال لبنان حيث جاء فيه ما حرفيته:

"وخلال شهر شباط من العام ١٩٩٩ زار قاسم ضاهر إيهاب البنا في منزله في بيروت ومعه برنامج تشفير على الكومبيوتر يسمى PGP ودرّبه عليه ثمّ طلب منه بناء على طلب أبو عائشة أن يسلّم هذا البرنامج لعصبة الأنصار في مخيم عين الحلوة كي يصبح في إمكان أبو عائشة أن يتبادل الرسائل المشفرة معهم عبر الإنترنت....[١]".

وفضلاً عن الحماية التي يؤمّنها التشفير للتوقيع الالكتروني، برز في هذا المجال دور التوثيق التي يؤمّنه مقدّم خدمات المصادقة، وهو ما سنتطرّق إليه بالتفصيل أدناه.

[١] منشور في جريدة النهار في عددها الصادر بتاريخ ١١ تموز ٢٠٠٠– أشار إليه طوني عيسى في المرجع السابق صفحة ٢٢٥.

الباب الثاني: التوثيق الإلكتروني كوسيلة لحماية التوقيع الالكتروني

يُعتبر التثبّت من هويّة الموقّع الهدف الأساسي والرئيسي في أيّ نوع من أنواع التواقيع، لكن يقتضي تدارك طبيعة المكوّن التقني الذي يسمح بتحقيق هذا الهدف. وعلى الرغم من أنّ التوقيع الرقمي المستند إلى تقنية التشفير غير المتماثل يسمح بالتثبّت من هويّة المرسل كما سبق بيانه في الباب الأول أعلاه، لكن كيف يمكن التأكّد بشكل جازم وحاسم من كون الشخص المنسوب إليه التوقيع هو فعلاً نفسه الموقّع؟

فالمفتاحين العام والخاص لا يرتبطان ماديًا بشخصٍ معيّن، كونهما عبارة عن زوجٍ من البيانات الإلكترونية. وهنا يأتي دور طرف ثالث محايدٍ ومستقلّ عن الحائز على المفتاح الخصوصي، وبين الحائزين على المفتاح العمومي، ويسمّى هذا الطرف الثالث بمقدّم خدمات المصادقة أو الشخص الثالث المصادق.

الفقرة الأولى: مقدّم خدمات المصادقة

تأتي أهميّة خدمات المصادقة، من كونها تمنح التّوقيع قوّة إثبات له ذات مرتبة ومفاعيل التوقيع الخطي، فالتّصديق أو التوثيق الإلكتروني، وسيلة آمنة هدفها التحقّق من صحّة التوقيع أو المحرّر، وصحّة نسبته لشخص محدّد، ويحدث ذلك عن طريق جهةٍ محدّدة تسمّى مقدّم خدمات التّصديق أو التّووثيق الإلكتروني.

أولاً: التعريف الفقهي

عرّف بعض الفقهاء مقدّم خدمات المصادقة بأنّه "محترف يتولّى مهمّة استقبال المفتاح العمومي للموقّع والتأكّد من توافقها مع الهويّة المعلنة من قبله، ومن ثمّ إنشاء شهادة المصادقة ونشرها"[١]

وبرأي البعض الآخر إنّ الشخص الثالث المصادق هو "هيئة أو جهة عامّة أو خاصّة تصدر شهادات إلكترونية هي كناية عن سجل معلوماتي يحتوي على مجموعة من المعلومات التعريفية منها إسم المستخدم طالب الشهادة وإسم سلطة المصادقة المانحة لها وتاريخ صلاحية الشهادة الممنوحة[٢]".

١. تعريف مقدّم خدمات المصادقة في النّصوص الدوليّة

[1] T. Piette-Coudol, op. Cit, p. 41.

[٢] طوني، عيسى، المرجع السابق، ص. ٢٠٥.

يمكن تعريف التصديق الإلكتروني على أنّه: "وسيلةٌ فنّيّة آمنة للتحقّق من صحّة التّوقيع أو المحرّر الإلكتروني، حيث يتمّ نسبته إلى شخصٍ أو كيانٍ معيّن عبر جهةٍ موثوق بها أو طرفٍ محايد، يُطلق عليه إسم مقدّم خدمات التّصديق أو التّوثيق الإلكتروني"[١].

أمّا مقدّم خدمات المصادقة، فهو شخصٌ من أشخاص القانون العام أو الخاص، يُصدر شهادات مصادقة بعد وضع قيد التطبيق، إجراءات الحماية التي تؤمّن الوظائف المحدّدة في المادة ١٥ من هذا القانون أو إحداها.

أ. تعريف التوجيه الأوروبي

بحسب التوجيه الأوروبي تاريخ ١٩٩٩/١٢/١٣ المتعلّق بالتواقيع الإلكترونية يُقصد بمقدّم خدمات المصادقة "كلّ هيئة أو شخص طبيعي أو معنوي يسلّم شهادات أو يقدّم خدمات أخرى تتعلّق بالتواقيع الإلكترونية"، أمّا التوجيه الأوروبي رقم ٢٠١٤/٩١٠ تاريخ 23/7/2014 فعرّفّ مقدّم الخدمات في الفقرة ١٩ من المادة ٣ منه بأنّه "كلّ شخص طبيعي أو معنوي يقدّم خدمة أو أكثر متعلّقة بالثقة سواء كان موصوفًا أو لم يكن".

ب. تعريف قانون الأنسيترال النموذجي

بحسب قانون الأونسترال النموذجي المتعلّق بالتواقيع الإلكترونية فقد نصّ في الفقرة "هـ" من المادة ٢ منه أن مقدّم خدمات التصديق يعني "شخص يصدر شهادات ويمكنه تزويد خدمات أخرى ذات صلة بالتواقيع الإلكترونية".

٢. تعريف مقدّم خدمات المصادقة في النصوص الوضعية

تضمّنت القوانين الوضعية للدول تعريفاتٍ مختلفة لمقدّم خدمات المصادقة مسترشدةً بالقوانين الدولية السالفة الذكر.

أ. تعريف القانون الفرنسي

[١] سمير، دحماني، التصديق الإلكتروني كوسيلة أمان لآليات الدّفع الإلكرتوني عبر الإنترنت، مجلّة الدراسات القانونية المقارنة، المجلد ٠٤، العدد ١، الجزائر، ٢٠١٨، ص. ٣٧.

تبنّى المشرّع الفرنسي تعريف مقدّم الخدمات الوارد في التوجيهات الأوروبية المشار إليها أعلاه وذلك في الفقرة ١١ من المادة ١ من المرسوم التطبيقي رقم ٢٠٠١/٢٧٢ تاريخ ٢٠٠١/٣/٣٠ والمتعلّق بتطبيق المادة ١٣٦٧ من القانون المدني الفرنسي التي حلّت محلّ المادة ١٣١٦ فقرة ٤.

ب. تعريف القانون المصري

عرّف المشرّع المصري مقدّم خدمات المصادقة في الفقرة ٦ من المادة ١ من اللّائحة التنفيذيّة تاريخ ٢٠٢٠/٤/٢٣ بأنّه: "الجهات المرخّص لها بإصدار شهادة التصديق الإلكتروني وتقديم خدماتٍ تتعلّق بالتوقيع الإلكتروني".

ج. تعريف القانون اللبناني

عرّف المشرّع اللبناني مقدّم خدمات المصادقة في الفقرة ٤ من القانون رقم ٢٠١٨/٨١ أنّه "شخصٌ من أشخاص القانون العام أو الخاصّ يُصدر شهادات مصادقة بعد وضع قيد التطبيق إجراءات الحماية التي تؤمّن الوظائف المحدّدة في المادة ١٥[١] من هذا القانون أو إحداها".

ومن المُلاحظ أنّ معظم التعريفات أعلاه تُجمع على إمكانيّة أن يكون مقدّم الخدمات شخصًا طبيعيًا أو معنويًا رغم شبه استحالة أن يكون شخصًا طبيعيًا نظرًا للمتطلبات الفنّية واللوجستية الكبيرة التي يتطلّبها هذا الأمر، كذلك نجد أنّ معظم التشريعات قد أولت مقدّم خدمات المصادقة صلاحية تقديم خدمات أخرى ذات صلة بالتوقيع الإلكتروني.

[١] نصّت المادة ١٥ من القانون رقم ٢٠١٨/٨١ على ما يلي:"تهدف وسائل الحماية التي تطبق على الكتابات والتواقيع الالكترونية الى تعزيز موثوقيتها.
تكون وظيفة وسائل الحماية التحقق من هوية واضع السند و/أو اعطاء تاريخ صحيح له و/أو ضمان سلامة بنوده وتأمين حفظه.
يؤمن هذه الوظائف او كل منها مقدم خدمات مصادقة او عدة مقدمين، يسلمون عند انجازها شهادة مصادقة الى صاحبة الصفة.
يمكن ان تؤمن هذه الوظائف او كل منها بواسطة تقنيات أخرى.

ثانياً: الشروط الواجب توافرها في مقدّم خدمات المصادقة

نصّت معظم القانونين الوضعيّة على وجوب توافر شروطٍ معيّنة في مقدّمي خدمات المصادقة، وسنبيّن أدناه الشروط المفروضة في القانون الفرنسي والمصري واللبناني.

١. الشروط المفروضة في التشريع الفرنسي

طرحت مسألة صلاحية شهادات المصادقة الصادرة في الخارج إشكالية في دول الإتّحاد الأوروبي الذي سعى من خلال التوجيه ٢٠١٤/٩١٠ الصادر عن البرلمان الأوروبي إلى توحيد المعايير المطبّقة من قبل الدول الأعضاء في هذا الإتّحاد. وبغية اعتماد مقدّم خدمات المصادقة يقتضي أن يتوافق طلبه مع الشروط المحدّدة في نظام الأمن العام (RGS) والشروط المفروضة من قبل الوكالة الوطنية لأمن المعلومات (ANSSI)،

ومن الشروط الواجب توافرها بطالب الإعتماد تلك المنصوص عنها في المادة ٦ من المرسوم رقم ٢٧٢ تاريخ ٢٠٠١/٣/٣٠ ، المعدّلة بموجب المرسوم رقم ٢٠١٧-١٤١٦ تاريخ ٢٠١٧/٩/٢٨:

- أن يستخدم طاقمًا تتوفّر لديه الخبرة والمعرفة والمؤهلات المطلوبة لتقديم خدمات التصديق
- تطبيق إجراءات الأمان واستخدام أنظمة لتحقيق الأمان التقني
- وإقامة الدليل على موثوقية الخدمات التي يقدّمها

يُمنح الإعتماد لمدّة سنتين ويتمّ إعادة التدقيق مجددًا بمدى توافق طالب الإعتماد مع الشروط أعلاه بغية تجديد طلبه.

وبحسب المادة ٩ من الفصل الثاني من الدليل الصادر عن الوكالة الوطنية لأمن المعلومات(ANSSI) في فرنسا بتاريخ ٢٠١٧/١/١٢ تحت الرقم 271/ANSSI/SDE [1] المتعلّق بعمليّة تصديق الخدمات، فإنّ الإعتراض على القرار عدم منح الإعتماد أو سحب الإعتماد أمام الوكالة نفسها أو يمكن الطعن به أمام المحكمة الإدارية في باريس، علمًا أنّ مهلة الطعن أو الإعتراض هي شهرين من تاريخ صدور القرار.

[1] https://www.ssi.gouv.fr/uploads/2014/11/qual_serv_process-processus-de-qualification-d-un-service.pdf, consulté le: 27-09-2022.

٢. الشروط المفروضة في التشريع المصري

اشترطت المادة ١٩ من قانون التوقيع الإلكتروني المصري وجوب استحصال مقدّم خدمات التصديق على ترخيصٍ مسبق من "هيئة تنمية صناعة تكنولوجيا المعلومات"، والهدف من ذلك أن تعزيز رقابة السلطة المسبقة على طالب الإعتماد والتثبّت من مدى استيفائه للشروط المطلوبة لأداء مهامه.

وقد اشترط القانون المصري في المادة ١٣ من اللائحة التنفيذية لقانون ٢٠٠٤/١٥ الصادرة بتاريخ ٢٠٢٠/٤/١٩ بعض الشروط الواجب توافرها بطالب الإعتماد، ومن أبرزها:

- نظام تأمين للمعلومات وحماية خصوصيتها بمستوى حماية لا يقلّ عن المعيارين ISO/IEC 27001 و ISO 27002 الصادرين عن المنظمة الدولية للمعايير[١].
- نظام حفظ بيانات إنشاء التوقيع الإلكتروني وشهادات التصديق الإلكتروني طوال المدّة التي حدّدتها الهيئة في الترخيص، وتبعًا لنوع الشهادة المصدرة، وذلك فيما عدا مفاتيح الشفرة الخاصّة التي تصدرها للموقّع فلا يتمّ حفظها إلا بناءً على طلب من الموقّع وبموجب عقدٍ مستقلّ يتمّ إبرامه بين المرخّص له والموقّع ووفقًا للقواعد الفنّية والتقنية لحفظ هذه المفاتيح التي يضعها مجلس إدارة الهيئة.[٢]
- نظام لإيقاف الشهادة في حال ثبوت العبث ببيانات الشهادة أو انتهاء مدّتها، سرقة أو فقدان المفتاح الشفري الخاص أو حتى الشكّ بذلك وعدم التزام حامل المصدّر له الشهادة ببنود العقد[٣].

كذلك فرض المشرّع المصري في المادة ١٥ من اللائحة التنفيذية أعلاه على طالب الترخيص بتقديم الضمانات والتأمينات التي يحدّدها مجلس إدارة الهيئة لتغطية أي أضرار ناتجة عن إخلاله بموجباته.

وبحسب موقع هيئة تنمية صناعة تكنولوجيا المعلومات ITIDA إنّ عدد الشركات التي تقدم خدمات المصادقة على التوقيع الإلكتروني المعتمدة من قبل الهيئة في مصر هي أربع شركات بالإضافة إلي سلطة التصديق الإلكتروني الحكومية بوزارة المالية والتي تقدم خدمات التوقيع الالكتروني داخل الجهات الحكومية وبين بعضها البعض[٤].

---

[١] فقرة "أ" من المادة ١٣ من اللائحة التنفيذية تاريخ ٢٠٢٠/٤/١٩.

[٢] فقرة "ز" من اللائحة التنفيذية عينها.

[٣] فقرة "ط" من اللائحة التنفيذية أعلاه.

[4] https://itida.gov.eg/Arabic/Pages/E-Signature.aspx.

٣. في التشريع اللبناني

حدّد القانون رقم ٢٠١٨/٨١ الشروط الواجب توافرها بمقدّم خدمات المصادقة، وميّز بمقدّم الخدمات المعتمد وغير المعتمد. فاعتبر في المادة ١٧ منه أنّ التوقيع المصادق عليه من مقدّم خدمات معتمد، يعتبر متمتّعًا بقرينة الموثوقيّة. أمّا التوقيع المصادق عليه من مقدّم خدمات غير معتمد، وبحسب أحكام المادة ١٨ من القانون عينه، فإنّه يعود للقاضي تقدير قوّته الثبوتية، ما لم يتّفق الفرقاء على خلاف ذلك.

وبهذا يكون المشرّع اللّبناني قد أعطى الحرّية للفرقاء بتنظيم علاقاتهم التعاقدية من دون إلزامهم بوسائل الحماية المنصوص عليها في القانون أعلاه.

أمّا بالنسبة لوسائل الحماية التي تطبق على الكتابات والتواقيع الالكترونية، فقد نصّت المادة ١٥ من القانون رقم ٢٠١٨/٨١ على أنّ هذه الوسائل تهدف الى تعزيز موثوقيتها، وتكون وظيفتها التحقّق من هويّة واضع السند و/أو اعطاء تاريخٍ صحيحٍ له و/أو ضمان سلامة بنوده وتأمين حفظه. ويؤمن هذه الوظائف أو كلٌّ منها مقدّم خدمات مصادقة او عدّة مقدمين، يسلّمون عند انجازها شهادة مصادقة الى صاحبة الصفة.

وقد جاء في المادة ١٦ من القانون عينه أنّ تقديم خدمات المصادقة لا يخضع الى ترخيص مسبق، مع مراعاة أحكام المادة ١٣٣ من القانون عينه التي حصرت بمصرف لبنان، فيما يتعلق بالعمليات المالية والمصرفية إعطاء:

أ. شهادات المصادقة العائدة للتواقيع الالكترونية للمصارف وللمؤسسات الخاضعة لرقابته ولرقابة هيئة الاسواق المالية وللمؤسسات وللادارات وللهيئات التي يتعامل معها وفقاً للقوانين التي ترعى عملياته

ب. شهادات الاعتماد للمصارف وللمؤسسات الخاضعة لرقابته ولرقابة هيئة الاسواق المالية، بصفتها مقدّم خدمات مصادقة للتواقيع الالكترونية لزبائنها.

إلا انّ هذه المادة قد أجازت لمقدم خدمات المصادقة الذي يستوفي الشروط، الاستحصال على شهادة اعتماد، يصدرها المجلس اللبناني للاعتماد (COLIBAC) المُنشأ بموجب القانون رقم ٢٠٠٤/٥٧٢، وهذا المجلس يتمتّع بالشخصية المعنوية وبالإستقلال المالي والإداري ويرتبط مباشرة بوزارة الصناعة التي تمارس سلطة

الوصاية عليه، ولا يخضع لسلطة مجلس الخدمة المدنية ولا لرقابة ديوان المحاسبة وفق ما جاء في المادة الثالثة من القانون ٢٠٠٤/٥٧٢ المذكور أعلاه.

وتجدر الإشارة إلى أنّه وبعد مرور حوالي ١٨ سنة على إقرار القانون ٥٧٢ السالف الذكر أقر مجلس الوزراء في جلسته المنعقدة بتاريخ ٢٠٢٢/٤/٦ مشروع المرسوم الذي قدّمته وزارة الصناعة والرامي إلى تنظيم المجلس اللبناني للاعتماد Colibac ،وقد صرّح وزير الصناعة جورج بوشكيان أنّ هذا المرسوم هو الأخير المتبقي من سلسلة المراسيم التطبيقية التنظيمية لقانون إنشاء المجلس اللبناني للاعتماد"[1].

علمًا أنّ المادة ٢٨ من القانون أعلاه قد أجازت أيضًا لمقدّم خدمات مصادقة مقيم خارج الاراضي اللبنانية ان يطلب من المجلس منحه شهادة الاعتماد إذا استوفى الشروط المطلوبة.

وبالعودة للشروط الواجب توافرها في مقدّم خدمات المصادقة بحسب أحكام القانون ٢٠١٨/٨١، فقد أعطت المادة ٢١ من القانون ٢٠١٨/٨١ المجلس اللبناني للاعتماد صلاحية وضع دفتر شروط يحدّد فيه الشروط والموجبات المفروضة في اجراءات الحماية التي يعرضها مقدّم خدمات المصادقة طالب الاعتماد، كما يحدّد العناصر اللازمة لإتمام عملية التقييم بصورة صحيحة، لا سيّما العناصر ذات الطابع الاداري والتقني والمالي التي يجب ان ترفق بطلب الاعتماد.

وقد ترك المشرّع اللبناني المجال مفتوحًا أمام المجلس من اجل تحديد مواصفات دفتر الشروط التقنية لتتلاءم مع التطوّر التقني والتكنولوجي دون أن تحصره بنصوصٍ جامدة، فنصّت الفقرة الثانية من المادة ٢١ أعلاه على أن يأخذ المجلس في الاعتبار المعايير والمقاييس الدولية في مجال التوقيع الالكتروني وغيرها من المنتجات او الخدمات او البرامج (software) المرتبطة بالتواقيع والكتابات الالكترونية، واشترطت على المجلس اعادة النظر في دفتر الشروط سنوياً على الاقل وكلما دعت الحاجة، على ضوء التطور التقني.

ولم يكتف قانون ٢٠١٨/٨١ بإلزام طالبي الإعتماد الذين يتقدّمون بطلبات اعتمادهم أو تجديد اعتمادهم للمجلس أن يتقيّدوا بالشروط ويستوفوا المواصفات المحدّدة في دفتر الشروط السالف الذكر بل فرض شروطًا ومعايير من الواجب الأخذ بها عند إصدار شهادة اعتماد أو تجديدها، حدّدتها المادة ٢٢ من هذا القانون. وتؤخذ في الاعتبار أيضًا لتقدير مدى موثوقية وسائل الحماية التي يقدمها مقدم خدمات المصادقة غير المعتمد، وهي التالية:

[1] http://industry.gov.lb/Media/News , acceced: 25-07-2022.

أ. البنى التحتيّة والتدابير التقنيّة لحماية الكتابة الالكترونية والاجراءات التنظيميّة والموارد البشريّة التي يضعها مقدم خدمات المصادقة قيد التطبيق، والتي يجب ان تكون مطابقة للمعايير الدوليّة.

ب. انتظام عمليّات التدقيق ومداها للتحقق من مطابقة خدمات مقدم خدمات المصادقة على الاعلانات والسياسات الصادرة عنه.

ج. توافر الضمانات المالية لمزاولة نشاط مقدم الخدمات.

د. وجود عقد تأمين يضمن التبعات المالية لمسؤوليته المدنية.

هـ. ضمانات الحياد والاستقلال والنزاهة لدى مقدم خدمات المصادقة.

و. الاعتماد او التقييم المُجرى سابقاً لنوعية وسائل الحماية والتي يجب ان تراعي المعايير الدولية من قبل هيئة مختصة إذا كان مقدم خدمات المصادقة مقيمًا في الخارج.

وبحسب أحكام المادتين ٢٣ و٢٤ من القانون ٢٠١٨/٨١، يتمّ دراسة طلب الإعتماد المقدّم من طالب الإعتماد من قبل المجلس وعلى نفقة طالب الاعتماد وينظم المجلس تقريراً يبلّغه من مقدم خدمات المصادقة لتمكينه من ابداء ملاحظاته، وعلى ضوء ذلك يصدر المجلس في مهلة شهرين قراراً معللاً بتوافر او بعدم توافر الشروط المطلوبة، وإذا انقضت المهلة المحددة في الفقرة الأولى دون أن يتخذ المجلس اي قرار، يعتبر انقضاء المهلة قراراً ضمنياً بالرفض.

علمًا أنّه وبحسب أحكام المادة ٢٠ من القانون ذاته، فإنّ القرارات الصادرة عن المجلس أعلاه المتعلقة بتطبيق هذا القانون تقبل الطعن امام مجلس شورى الدولة، وقد انتقد بعض الفقهاء هذا الأمر[١]، يتنافى في الواقع مع طبيعة الإنترنت وسرعة التجارة الإلكترونية التي تفرض أن يُصار البتّ بالملفات من قبل محاكم متخصّصة تتميّز بسرعة إصدار أحكامها.

الفقرة الثانية: موجبات أطراف المصادقة وأبرز مهامّ مقدّم الخدمات

بهدف الوصول إلى الغاية المنشودة من التوثيق، والتي تتمثّل بتوفير الأمان والإستقرار في المعاملات التجارية الالكترونية، أوجدت التشريعات مجموعة موجباتٍ، يُفترض على أطراف المصادقة إنفاذها، كذلك حدّدت مهام مقدّم خدمات المصادقة، وهذا ما سنتطرّق إليه أدناه.

[١] شربل، القارح، المرجع السابق، ص. ١١٠.

أولاً: موجبات مقدّم خدمات المصادقة

إنّ أبرز الموجبات الملقاة على عاتق مقدّم خدمات المصادقة، والتي أجمعت عليها معظم القوانين الوضعية، هي التالية:

١. التحقّق من صحّة البيانات المصادق عليها من قبله

إنّ هذا الموجب هو من أبرز الموجبات الملقاة على عاتق مقدّم خدمات المصادقة باعتبار أنّه يرتبط بصميم الغاية التي أنشأ التوقيع الإلكتروني من أجلها، وقد نصّت المادة ١٥ من القانون ٢٠١٨/٨١ صراحة على أنّ من وظائف مقدّم خدمات المصادقة التحقّق من هويّة واضع السند و/أو إعطاء تاريخ صحيح له و/أو ضمان سلامة بنوده وتأمين حفظه.

كذلك نصّت على المبادئ نفسها البند "م" من الفقرة الثانية المادة ٦ من القانون الفرنسي رقم ٢٠٠١-٢٧٢ والمادة ٢٤ من التوجيه الأوروبي رقم ٢٠١٤/٩١٠ التي أسهبت بشرح وسائل التثبّت من هويّة طالب الإعتماد مميّزة في فقرتها الأولى بين أربع حالات:

أ. حضور طالب الإعتماد شخصيًا أو حضور ممثله في حال كان شخصًا معنويًا.
ب. عن بعد عن طريق وسائل اتصال الكترونية تضمن نسبة أمان عالية.
ج. عن طريق شهادة توقيع الكتروني مؤهلة أو ختم مستوفٍ لشروط الأمان
د. اللجوء إلى وسائل التثبت من الهوية المعتمدة على المستوى الوطني والتي تؤمّن موثوقية حضور طالب الإعتماد شخصيًا.

٢. موجب المحافظة على سرّية البيانات المسلّمة إليه

إنّ مقدّم خدمات التصديق ملزمٌ حكمًا بسريّة كافّة البيانات والمعلومات المسلّمة إليه أو أخذ علمًا بها بحكم عمله، ويتوجب عليه بالتالي عدم إفشاء هذه المعلومات تحت طائلة ملاحقته وإلزامه بالتعويض. وقد كرّس البند "ط" من الفقرة الثانية المادة ٦ من القانون الفرنسي رقم ٢٠٠١-٢٧٢ هذا المبدأ، كذلك فعلت المادة ٢١ من القانون المصري رقم ٢٠٠٤/١٥.

أمّا بالنسبة للقانون اللبناني رقم ٢٠١٨/٨١ فقد نصّت المادة ١٩ من منه على إخضاع مقدم خدمات المصادقة المعتمد وغير المعتمد على حدّ سواء لموجب السرّية المهنية، إلا أنّ الفقرة الثانية من المادة عينها قد أجازت رفع السرّية المهنية بقرارٍ صادرٍ عن المرجع القضائي المختصّ في معرض النزاع الموجب لرفع تلك السرّية دون تحديد ماهيّة هذا النزاع.

يرى البعض[1] أنّ رفع السرّية المهنية، لا يفترض أن يتمّ إلا بمعرض نزاعٍ يتمحور موضوعه حول البيانات المتعلّقة بالسند الإلكتروني والتوقيع الإلكتروني وليس غيرها، أو في معرض النظر بأيّ فعل يمكن أن يشكّل جنحة أو جناية يتوقّف أمر مدى التحقّق من مدى توافر عناصرها على الدخول إلى خصوصيّة بعض البيانات المؤتمن عليها مقدّم خدمات المصادقة.

٣. موجب تعليق شهادة التصديق أو إلغائها

يمكن أن يطرأ بعد إصدار الشهادة أسبابًا جدّيةً توجب تعليق العمل بشهادة التصديق أو حتّى إلغاءها كما في حال اكتشاف مقدّم الخدمات مثلا أنّ الشهادة التي أصدرها قد استندت على معلومات خاطئة أو إنّ الشهادة تستعمل لأهداف غير مشروعة.

وقد نصّت الفقرة ٥ من المادة ٢٨ من التوجيه الأوروبي رقم ٢٠١٤/٩١٠ على إمكانية الدول الأعضاء وضع قواعد بغية تعليق شهادة التصديق. كذلك نصّ البند الأول من هذه الفقرة على أنّ الشهادة تفقد مصداقيتها طيلة مدّة التعليق، ونصّ البند الثاني من الفقرة عينها على وجوب تحديد مدّة تعليق الشهادة بوضوح، في حين نصّت الفقرة ٤ من المادة ٢٨ أعلاه على فقدان صلاحية الشهادة وعلى عدم إمكانية إعادتها إلى حالاتها السابقة وذلك في حال إلغاء هذه الشهادة، علمًا أنّ المشرّع الفرنسي قد تبنّى التوجيه أعلاه بموجب المرسوم رقم ٢٠١٧/١٤١٦.

وقد تناول القانون التونسي رقم ٢٠٠٠/٨٣ هذه المسألة بشكلٍ مفصّل في الفصل ١٩ منه التي نصّت على إمكانية تعليق العمل بشهادة التصديق بناءً على طلب من صاحبها أو عند توافر الحالات التالية:

أ. تسليم الشهادة بالاعتماد على معلومات مغلوطة أو مزيفة.

ب. انتهاك منظومة إحداث الإمضاء.

ج. استعمال الشهادة بغرض التدليس.

د. تغيّر المعلومات المضمنة بالشهادة.

وقد أوجبت المادّة المذكورة على مزوّد خدمات التصديق إبلاغ صاحب الشهادة حالاً بالتعليق وسببه، كذلك نصّت على إمكانية رفع التعليق في حال ثبُت صحّة المعلومات المدوّنة في الشهادة واستعمالها بصفةٍ شرعيّة.

أمّا المشرّع المصري فاشترط على مقدّم الخدمات فق الفقرة "ط" من المادة ١٣ من اللّائحة التنفيذيّة تاريخ ٢٠٢٠/٤/١٩ أن يتوافر لديه نظام لإيقاف الشهادة في حال ثبوت توافر إحدى الحالات التالية:

[1] هاني، الحبّال، المرجع السابق، ص. ١٩.

أ. العبث ببيانات الشهادة أو انتهاء مدّة صلاحيتها.
ب. سرقة أو فقد المفتاح الشفري الخاصّ أو أداة التوقيع الإلكتروني أو عند الشكّ في حدوث ذلك.
ج. عدم التزام الشخص المصدر له شهادة التصديق الإلكتروني ببنود العقد المبرم مع المرخّص له.

وقد نصّت هذه المادة على خضوع نظام إيقاف الشهادات للقواعد التي يضعها مجلس إدارة الهيئة (هيئة تنمية صناعة تكنولوجيا المعلومات).

ورغم الأهميّة البالغة التي تطرحها مسألة إلغاء شهادات التصديق أو تعليقها، نجد أنّ المشرّع اللبناني لم يتناول هذا الأمر في القانون ٢٠١٨/٨١ المتعلّق بالمعاملات الإلكترونية، علمًا أنّ اقتراح القانون المقدّم من النائبة غنوة جلّول بتاريخ ٢٠٠١/١٠/٩، المذكور في الفصل الأول من دراستنا، قد تناول هذا الأمر.

٤. موجب إعلام سلطة المصادقة

يتوجّب على مقدّم الخدمات إعلام سلطات المصادقة بأيّ تغيير يطال الشروط التي منح على أساسها ترخيصه أو في حال رغب بالتوقّف عن تقديم خدماته، وقد نصّ الفصل ٢٤ من القانون التونسي رقم ٢٠٠٠/٨٣ على وجوب إعلام الوكالة الوطنية للمصادقة الإلكترونية عن رغبته بإيقاف نشاطه قبل ثلاثة أشهر على الأقلّ.

أمّا بالنسبة للمشرّع اللبناني فقد أوجبت المادة ٢٦ من القانون رقم ٢٠١٨/٨١ على مقدم خدمات المصادقة المعتمد أن يبلغ خطياً المجلس (COLIBAC)، بواسطة كتاب يسجل لديه، عن كل تغيير يؤثّر على العناصر المقّدمة في ملف طلب الاعتماد.

ثانياً: موجبات مستخدمي الشهادة

رغم عدم تطرّق معظم القوانين الوضعيّة إلى موجبات طالب شهادة التصديق أو الأشخاص الثالثين المتعاملين معه، إلا أنّ هذه الموجبات تنبثق من القواعد القانونية العامّة وتؤدّي مخالفتها إلى ترتيب مسؤولية قانونية على عاتق هؤلاء.

١. موجبات طالب شهادة التصديق

أ- تقديم بيانات صحيحة

صحيحٌ أنّه من واجب مقدّمي خدمات المصادقة التثبّت من هويّة وبيانات طالب شهادة التصديق كما سبق وأشرنا إليه، إلا أنّ هذا الأمر لا يعفي طالب التصديق من مسؤوليته في حال تقديمه بياناتٍ مزوّرة لإثبات

هويته. فموجب مقدمي المصادقة في هذا المجال هي موجب وسيلة وليس موجب نتيجة، أي بمعنى آخر يقتضي عليها بذل العناية، ويكفي إثباتها هذا الأمر لترفع عنها التبعات القانونية وذلك في حال ثبوت تقديم طالب الشهادة معلومات مزوّرة أو مزيّفة. علمًا أنّ هذا الأمر من شأنه أن يرتّب مسؤوليةً جزائيةً على طالب شهادة التصديق وفق ما نصّت عليه معظم القوانين الوضعيّة، وهو ما سنتناوله بالتفصيل أدناه.

ب-موجب إعلام مزوّد الخدمات

إنّ الهدف الأساسي من شهادة التصديق هي إثبات هويّة حاملها وبالتالي هويّة الموقّع، لذلك يقتضي على حامل هذه الشهادة إعلام مزوّد الخدمات بأيّ تغييرٍ يطرأ فيما بعد على بياناته الشخصيّة التي استحصل على أساسها على شهادة التصديق، وهذا ما نصّت عليه صراحة الفقرة الثانية من الفصل ٢١ من القانون التونسي رقم ٢٠٠٠/٨٣.

ت-الحفاظ على المفتاح الخاص واستعمال الشهادة وفقًا للغاية التي صدرت على أساسها

يقع على عاتق حامل شهادة التصديق أن يستعملها وفق الغاية المعدّة لها كذلك يترتّب عليه موجب بذل العناية للحفاظ على المفتاح الخاصّ وضبطه تحت رعايته طيلة المدّة المتّفق عليها مع سلطات الإصدار، كما يتوجّب عليه المحافظة على سلامة المفتاح الخاصّ ليمنع وقوعه تحت يد أي شخص لا علاقة له به بغية تلافي خطر التوقيع عنه دون إرادته[١].

وقد نصّت المادة ٢١ من القانون التونسي رقم ٢٠٠٠/٨٣ أن صاحب الشهادة هو المسؤول الوحيد عن سرية وسلامة منظومة إحداث الإمضاء (التوقيع الإلكتروني)، وكلّ استعمال لهذه المنظومة يعتبر صادرًا منه.

٢- موجبات الأشخاص الثالثين

يعنى بالأشخاص الثالثين كلّ متعاقد مع حامل شهادة التصديق الإلكتروني والذي يستند بتعامله على موثوقية هذه الشهادة، وبحسب المادة ١١ من قانون الأونسيترال النموذجي فإنّه يقع على الأشخاص الثالثين موجب التثبّت من صلاحية شهادة التصديق ومن كونها سارية المفعول بتاريخ التعاقد ولم يتمّ تعليقها أو إلغاؤها، كذلك يقتضي عليه التثبّت ممّا إذا كان هناك من قيود تخضع إليها الشهادة المذكورة.

[١] ضياء، مشيمش، المرجع السابق، ص. ١٧٣.

ثالثاً: مهامّ مقدّم خدمات المصادقة

فضلا" عن الموجبات الملقاة على عاتقه المنوّه عنها أعلاه، يضطلع مقدّم خدمات المصادقة بعدّة مهامّ تهدف إلى تعزيز الموثوقية بالتوقيع الإلكتروني والحفاظ على قوّته الثبوتية،

وأبرز هذه المهامّ:

١. إصدار شهادات المصادقة

إنّ شهادة المصادقة هي بمثابة بطاقة هوية الكترونية تسمح بإثبات الصلة بين الشسخص والتوقيع الإلكتروني[1]، ونظرًا لما لشهادة المصادقة من دورٍ بارزٍ على صعيد العلاقات التجارية، فقد تضمّنت معظم التشريعات تعريفًا لهذه الشهادة.

أ. شهادة المصادقة ومضمونها

يُقصد بالشهادة بحسب قانون الأونسترال النموذجي، أنّها رسالة بيانات أو سجلّ تؤكّد الرابط بين الموقّع والبيانات المتعلّقة بإنشاء التوقيع". ويُلاحظ أنّ هذا التعريف قد استعمل عبارة "بيانات إنشاء التوقيع التي يُقصد بها المفتاح الخاصّ فسعى بالتالي لربط هذا المفتاح بالموقّع.

أمّا التوجيه الأوروبي رقم ٢٠١٤/٩١٠ فقد ميّز بين نوعين من شهادات المصادقة:

- **شهادة التوقيع الإلكتروني**

وقد عرّفتها الفقرة ١٤ من المادة ٣ من هذا التوجيه بأنّها " الشهادة الإلكترونية التي تربط البيانات الخاصّة بصحّة التوقيع الإلكتروني بشخص طبيعي وتؤكّد على الأقلّ إسم أو الإسم المستعار العائد لهذا الشخص.

- **الشهادة الموصوفة للتوقيع الإلكتروني**

عرّفتها الفقرة ١٥ من المادة ٣ من التوجيه أعلاه بأنّها شهادة توقيع إلكتروني صادرة عن مقدّم خدمات مصادقة معتمد وتلبّي المتطلّبات المنصوص عنها في الملحق رقم ١.

وقد قصد هذا التوجيه بعبارة " البيانات الخاصّة بصحّة التوقيع" المفتاح العام للموقّع الذي سعى لربطه به.

[1] C. Feral Schuhl, op. Cit., p. 55

وبالنسبة للمشرّع الفرنسي قد تبنّى ما جاء في التوجيه أعلاه إذ ميّز بدوره في الفقرتين ٩ و١ من المادة الأولى من القانون رقم ٢٧٢-٢٠٠١ بين الشهادتين المذكورتين أعلاه، فعرّف شهادة التوقيع الإلكتروني بأنّها " مستند إلكتروني يؤكّد الإتّصال بين بيانات التحقّق من التوقيع الإلكتروني وصاحب هذا التوقيع، علمًا أنّ الفقرة ٧ من المادة الأولى أعلاه قد عرّفت "بيانات التحقّق" بأنّها المفتاح العام.

كذلك عرّف المشرّع الفرنسي الشهادة الإلكترونية الموصوفة بأنّها "الشهادة التي تستوفي المتطلبات المنصوص عنها في المادة ٦ من هذا المرسوم".

وقد سار المشرّع المصري على خطى قانون الأنسيترال لناحية ربطه للشهادة بالمفتاح الخاصّ العائد للموقّع فعرّف شهادة التصديق في الفقرة "و" من المادة الأولى من القانون رقم ٢٠٠٤/١٥ ، بأنّها " مستندٌ إلكتروني يؤكّد الإتّصال بين بيانات التحقّق من التوقيع الإلكتروني وصاحب التوقيع، علمًا أنّ مصطلح "بيانات التحقّق قد عرّفته الفقرة الثامنة من المادة الأولى من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري بأنّها " عناصر متفرّدة خاصّة بالموقّع وتميّزه عن غيره، ومنها على الأخصّ مفاتيح الشفرة الخاصّة به، والتي تستخدم في إنشاء التوقيع الإلكتروني".

أمّا المشرّع اللبناني ورغم أهميّة هذه الشهادة فلم يأتِ على ذكرها في القانون ٢٠١٨/٨١.

ب. مضمون شهادة الأمن والسرّية ومعاييرها التقنية

يقتضي أن تتضمّن شهادة الأمن والسرّية البيانات التالية:

- إسم وشهرة صاحب الشهادة أو إسمه المستعار وذلك بهدف التمكّن من التثبّت من هويّته.
- الرقم التسلسلي الذي يمكّن صاحب الشهادة من خلاله استعمال مفتاحه الخاصّ.
- رقم المفتاح أو بصمة المفتاح (بصمة تعريف الشهادة).
- تاريخ إصدار الشهادة وتاريخ انتهاء مدّة استخدامها.
- هويّة سلطة إصدار الشهادات.[١]

وفيما خصّ المعايير التقمية للشهادة، فقد حدّد ضع الإتحاد الدولي للإتصالات معيارًا دوليًا سمّي توصية x509 v.3 وذلك بهدف توحيد نمط الشهادات التي تصدر بطبيعة الحال عن سلطات مصادقة مختلفة، كذلك

[١] رانيا، صليبا، المرجع السابق، صفحة ١٧٦

تهدف هذه التوصية لتسهيل التحقّق من صحّة التوقيع الإلكتروني، وقد تمّ تطوير المعيار أعلاه من قبل منظمة IETF (Internet Engineering Task Force)، التي طوّرت مفهوم عرف "بالبنية التحتية بالمفاتيح العامّة"[١].

ومن واجب مقدّم الخدمات إصدار مفاتيح التشفير أي المفتاح العمومي والمفتاح الخاصّ، فيتولّى بالتالي المصادقة على هويّة حامل المفتاح العمومي (وهو المفتاح الذي يكون معلومًا للجميع)، كذلك فإنّه ومن خلال شهادة المصادقة الصادرة عنه فإنّه يؤكّد أنّ المفتاح العمومي يعود بالفعل للعميل حامل المفتاح الخاصّ.

٢. إصدار مفاتيح وأدوات التشفير

يعدّ إصدار مفاتيح وأدوات التشفير من أبرز الخدمات التي يوفّرها مقدّم خدمات المصادقة. وهناك نوعان من مفاتيح التشفير، كما سبق وأسلفنا، المفتاح العام الذي يستخدم في عمليّة تشفير السند الالكتروني، ويمكن لجميع المستخدمين الاطّلاع عليه،

والمفتاح الخاصّ المستخدم في عمليّة فكّ التشفير، والذي يتوجّب على صاحبه الاحتفاظ به وعدم تسريبه أو تمكين أحد من الوصول إليه.

ويقوم مقدّم خدمات المصادقة أيضًا بإصدار بطاقة ذكية أو شرائح الكترونية منفصلة (Smart Tokens) تحتوي على البيانات الشخصيّة العائدة للموقّع والتي تعرف ببيانات إنشاء التوقيع الالكتروني. ويتمّ تثبيت هذه البيانات على السند الالكتروني باتّباع طرقٍ فنيّةٍ من شأنها المحافظة على سريّة هذه البيانات المذكورة، خاصّة وأنّ البطاقة أعلاه لا يمكن استنساخها كونها محميّة برقمٍ سرّي[٢] ، كما يمكن أن تُستعمل فيها تقنية SCMS[3]، وهذه التقنية تمنع إجراء نسخ إلا بالعدد المسموح من صاحب التوقيع الالكتروني أو مقدّم خدمات المصادقة، كذلك تمنع إجراء نسخ إضافية عن النسخ التي تمّ إصدارها[٤].

---

[1] T. Piette-Coudol, op. Cit ,p.29.

[٢] عبير، الصفدي، رسالة بعنوان: النظام القانوني لجهات توثيق التوقيع الالكتروني، جامعة الشرق الأوسط للدراسات العليا، الأردن ٢٠٠٩، ص. ٧٤.

[3] Serial Copy management.

[4] Daniel Becourt en collaboration avec Sandrine Carneroli, Depôt legal de l'écrit à l'electronique, éditions Litec, France, 2001, p. 126.

٣. أرشفة بيانات التوقيع الالكتروني والسندات الالكترونية

نتيجة التطوّر التكنولوجي المتسارع والمستمرّ بات من المستحيل ضمان أمان السندات الالكترونية بالشكل عينه بعد عدّة سنوات. ويرى البعض أنّه يمكن للتطوّر التكنولوجي التوصّل لمعرفة المفتاح الخاصّ عن طريق عمليّات حسابية بمجرّد معرفته بالمفتاح العام[١].

وفي هذا السياق يبرز دور مقدّم خدمات المصادقة لحماية حجيّة التوقيع الالكتروني في تحقيق الأمان المنشود بحفظه المعلومات والشهادات التي يُصدرها عن طريق خدمة الأرشفة التي يمكن أن يضطلع بها.

تهدف الأرشفة لحماية حجيّة التوقيع الإلكتروني ، ففي حال لم يتمّ حفظ مفاتيح التشفير، الشهادات وأجهزة إنشاء هذا التوقيع، سيصبح من المستحيل، بعد مرور بعض الوقت، التأكّد من هويّة الموقّع وموثوقية السند الإلكتروني[٢].

وتبرز أهميّة الأرشفة لجهة إمكانية تحديد تاريخ إبرام التصرّفات القانونية، فيمكن بالتالي لمقدّم الخدمات أن يضمن تحديد تاريخ هذه التصرّفات.

أمّا بالنسبة للمدّة التي يتوجّب فيها حفظ البيانات المذكورة، فيرى البعض[٣] أنّه يقتضي حفظ المعلومات خلال "مدّة مفيدة" والتي يُقصد بها المدّة التي تبقى شهادة المصادقة صالحة لتقديمها أمام المحاكم أي مدّة التقادم المحدّدة للتصرّف الثابت للشهادة.

---

[1] V. Sedaillan, Preuve et signature électronique, revue du droit des technologies de l'informatique ,information, Mai 2000, N° 3, P. 8.

[2] M. Demoulin et D. Gobert: l'archivage dans le commerce électronique: comment raviver la mémoire?, cahier du CRID n° 23, mai 2003, p. 101-130.

[٣] سعيد قنديل،التوقيع الالكتروني ماهيته-صوره- حجيته في الاثبات بين التداول والقتباس، دار الجامعة الجديدة، مصر ٢٠٠٦، ص. ١٠٤.

المبحث الثاني: مسؤولية مقدّمي خدمات المصادقة والحماية الجزائية للتّوقيع الإلكتروني

بهدف تدعيم الثقة بالتقنيات الجديدة، وتحفيز قبول الجمهور لها، وإعطائها نفس القوّة الثبوتيّة التي تُعطى للتّعاملات الجارية بالأساليب التقليدية، كان لا بدّ من توفير الحماية القانونية اللازمة للتوقيع الإلكتروني، كما هي الحال بالنسبة للتّوقيع الورقي.

وقد برز الطابع الدولي لهذه المسألة، مع تخطّي المعاملات الإلكترونية الحدود الجغرافية للدول، وأصبحت تتمّ على نطاقٍ واسعٍ، كالمعاملات التي تحصل من بلدٍ إلى بلد، أو التي تتضمّن عنصراً أجنبياً، وذلك على الرغم من عدم انسجام التشريعات الوطنية في هذا المجال أو حتّى تناقضها في أحيان أخرى. والذي تطلّب أحياناً تأمين تناسق التواقيع الإلكترونية بين مختلف الدّول، فضلاً عن توحيد الشروط الفنية التي تخضع لها، والدعوة لوضع أطر قانونية للمعاملات الإلكترونية تأخذ طابع دولي، ويؤمّن الإنسجام فيما بينها،

وسنتطرّق أدناه إلى مسؤولية مقدّم خدمات المصادقة المدنية (الباب الأول)، فضلا" عن الحماية الجزائية التي سعت التشريعات الدولية والمحليّة لتوفيرها بغية حماية التوقيع الإلكتروني (الباب الثاني).

الباب الأول: مسؤولية مقدّمي خدمات المصادقة بحسب القواعد العامة للمسؤولية

تعتبر مرحلة التصديق على التوقيع الإلكتروني من أهمّ مراحل إبرام العقد الإلكتروني، على اعتبار أنّ لها دورٌ بارزٌ في إثبات إنعقاد العقد، والتأكّد من صحّة ما ورد فيه من بيانات. ومقدّمو خدمات المصادقة هم أطرافًا يمثّلون هيئةً خاصة تلبّي حاجة المتعاملين عبر شبكة الإنترنت بوصفهم طرفًا ثالثًا، يعمل على ترسيخ الثّقة فيما بينهم، عبر إصدار شهادة مصادقة لكل مشترك تشهد بموجبها بصحّة المعاملات والبيانات الواردة فيها. حتّى أنّ البعض رأى أنّ مقدّمي خدمات المصادقة بمثابة كتّاب عدل، تسند إليهم مهمّة توثيق المعلومات والاحتفاظ بأصولها وتسليم شهادات في آخر المطاف.[1]

[1] ضياء، نعمان، المصادقة الإلكترونية على ضوء قانون التبادل الإلكتروني للمعطيات القانونية، مجلة الدراسات القانونية والقضائية، العدد الأول، اوكتوبر ٢٠٠٩، ص. ١٢٩.

كلّ ذلك دفع الدول لتكثيق جهودها محلّياً ودولياً في هذا السياق من أجل حماية وضمان حقوق المتعاملين مع مقدّم الخدمات عن طريق إصدار تشريعاتٍ تعنى بمسؤوليته، وسنتناول أدناه نظام هذه المسؤولية وفقًا للقواعد القانونية العامّة (فقرة أولى)، وموقف التشريعات الدولية والمحلية من هذه المسؤولية (فقرة ثانية).

الفقرة الأولى: المسؤولية المدنية لمقدّم خدمات المصادقة

إنّ العلاقة القائمة بين طالب شهادة التصديق ومزوّد الخدمات هي علاقةٌ تعاقدية ترتّب موجبات على كليهما، وبالتالي فإنّ أي إخلال بهذه الموجبات يلقي على الطرف الناكل مسؤوليةً تؤدّي إلى إلزامه بالتعويض عن الضرر الذي سبّبه، وسنبيّن أدناه الأساس القانوني الذي ترتكز عليه هذه المسؤولية.

أولاً: المسؤولية التعاقدية لمقدّم خدمات المصادقة

إنّ قيام المسؤولية العقدية محصورٌ في نطاق إنفاذ عقدٍ صحيحٍ قائم وملزمٍ لطرفيه ومبناها عدم تنفيذ بعض أو كلّ الموجبات التي تضمّنها من قبل الطرف الآخر[١].

يتوافر خطأ مقدّم خدمات التصديق عن طريق إخلاله بالموجبات الملقاة على عاتقه استنادًا للعقد الموقّع بينه وبين طالب شهادة التصديق (أو العميل). ومن الأمثلة على هذا الخطأ إصدار شهادة تصديق تتضمّن خطأ ببيانات مختلفة عن تلك التي تمّ تزويده بها، أو التأخّر بإصدار هذه الشهادة أو عدم إصدارها كذلك في حال إلغائها أو تعليق العمل بها دون مسوغ شرعيّ.

أمّا بالنسبة للضرر الذي يتوجّب التعويض على أساسه فهو الضرر المباشر أي أن يكون هذا الضرر مرتبطا سببيًا بعدم تنفيذ العقد وهو ما يسمّى بالخطأ العقدي[٢]. ولا يلزم مقدّم الخدمات بالتالي التعويض عن الضرر الحاصل نتيجة قوّة قاهرة أو خطأ المتضرر أو الغير.

[١] مصطفى، العوجي، القانون المدني، الجزء الثاني، المسؤولية المدنية، منشورات الحلبي الحقوقية ٢٠٠٩، صفحة ٣١.

[٢] مصطفى، العوجي، المرجع نفسه، صفحة ٦١.

ثانيًا: المسؤولية التقصيرية لمقدمي خدمات التصديق

تتحقّق شروط هذه المسؤولية بالإستناد لفعل شخصي (صادر عن مقدم خدمات المصادقة) يحدث ضررًا للغير، ويتّصف هذا الفعل بالخطأ[1]، والمقصود بالغير هنا الأشخاص الثالثين الذين ليسوا طرفًا بالعلاقة التعاقدية الحاصلة بين مقدّم خدمات التصديق وحامل الشهادة، ولا بدّ من قيام الصلة السببية بين الضرر والخطأ حتى تقوم مسؤولية المتسبّب به فيرتّب عليه موجب التعويض.

وموجب التعويض في حالة المسؤولية التقصيرية يختلف عن ذاك المترتّب استنادًا للمسؤولية العقدية، إذ إنّه في حالة المسؤولية التقصيرية يكون موجب التعويض مطلقًا سواء أكانت الأضرار مباشرة أو غير مباشرة.

إلا أنّ مسألة إثبات العلاقة السببية بين الخطأ والضرر هي بغاية الصعوبة نظرًا لتشعّب الإجراءات التقنية المرتبطة بالتوقيع الإلكتروني، فيصبح المتضرّر أمام عجزٍ لإثبات خطأ مقدّم خدمات التصديق، وهذا ما دفع ببعض الفقهاء لاعتبار أنّ مسؤولية مقدّم الخدمات تستحقّ أن تصنّف كموجب نتيجة كون هذه العمليّة هي تقنيّة بحتة.[2]

الفقرة الثانية: موقف التشريعات الدولية والمحلية

تظهر الجهود الدولية في هذا السياق بشكل واضح وجليّ، تحديداً فيما يتعلّق بإقرار الإرشادات والتوجيهات والقوانين والقواعد والأنظمة. وسنتطرّق أدناه إلى موقف التوجيه الأوروبي والتشريع الفرنسي (أولا)، موقف القانون التونسي والمصري (ثانيًا) وإلى موقف التشريع اللبناني بهذا الخصوص (ثالثًا).

أولاً: موقف التوجيه الأوروبي والتشريع الفرنسي

١. التوجيه الأوروبي رقم ٢٠١٤/٩١٠

نصّت المادة ١٣ من التوجيه الأوروبي رقم ٢٠١٤/٩١٠ على أنّ مقدّمي خدمات المصادقة مسؤولون عن التعويض عن الأضرار التي ألحقت بكلّ شخص طبيعي أو معنوي ناتج عن قصد أو إهمال بسبب مخالفة الإلتزامات المنصوص عنها في التوجيه أعلاه، أمّا بالنسبة لعبء الإثبات فقد ميّزت هذه المادة بين حالتين:

---

[1] مصطفى، العوجي، المرجع نفسه، صفحة ١٥٩.

[2] P. Le Tourneau. op. Cit., p.392.

أ. حالة مقدّم الخدمات غير المعتمد: واشترطت في هذه الحالة على المتضرّر إثبات الخطأ أو الإهمال المرتكب من قبل مقدّم الخدمات.

ب. أمّا في حال كان مقدّم الخدمات معتمدًا فقد نصّت على أنّ مسؤوليته مفترضة ويتوجب على مقدّم الخدمات في هذه الحالة، ولرفع المسؤولية عنه، أن يثبت عدم ارتكابه لأي خطأ أو تقصيرٍ بواجباته.

٢. موقف التشريع الفرنسي

إنّ مسؤولية مقدّمي خدمات المصادقة بحسب أحكام المادة ٣٣ من القانون رقم ٢٠٠٤-٥٧٥ تاريخ ٢١ حزيران ٢٠٠٤، المتعلّق بالثقة في الإقتصاد الرقمي، هي مسؤولية مفترضة، فيقتضي بالتالي على مقدّمي خدمات المصادقة التعويض عن الضرر اللاحق بالأشخاص الذين اعتمدوا، بشكل معقول، على الشهادات الصادرة عنهم على اعتبار أنّهم مؤهلون، وذلك في حال:

أ. كانت العلومات الواردة في الشهادة، بتاريخ التسليم، غير دقيقة.

ب. كانت البيانات المطلوبة لاعتبار الشهادة مؤهلة كانت غير مكتملة.

ج. تسليم الشهادة لم يؤدِ للتحقّق من أنّ المفتاح الخاصّ، الذي يحمله الموقّع، يطابق المفتاح العام الذي تحمله الشهادة.

د. لم يقم مقدّمو الخدمات بتسجيل إلغاء الشهادة وجعل هذه المعلومات متاحة للأشخاص الثالثين.

كذلك نصّت هذه المادة على إمكانية تنصّل مقدمي خدمات المصادقة من مسؤوليتهم في حال أثبتوا عدم ارتكابهم لأي خطأ قصدي أو إهمال، وأضافت أنّ مقدّمي الخدمات غير مسؤولون عن الضرر الناتج عن استعمال شهادة تتجاوز القيود الموضوعة على استخدامها، شرط أن تكون هذه القيود مدرجة في الشهادة وتكون بمتناول المستخدمين.

ثانياً: موقف التشريعين التونسي والمصري

١. موقف التشريع التونسي

نصّ الفصل ٢٢ من القانون التونسي رقم ٢٠٠٠/٨٣ على مسؤولية مزوّد خدمات المصادقة الإلكترونية عن كلّ ضرر حصل لكلّ شخص وثق عن حسن نيّة في الضمانات المنصوص عنها في الفصل ١٨ من هذا القانون وأبرز هذه الضمانات بحسب الفصل ١٨ المذكور هي ضمان صحة المعلومة المصادق عليها التي

تضمنتها الشهادة في تاريخ تسليمها وضمان الصلة بين صاحب الشهادة ومنظومة التدقيق في الامضاء الخاصة به.

إضافة إلى ذلك، نصّت الفقرة الثانية من الفصل ٢٢ من القانون عينه على مسؤولية مزوّد خدمات المصادقة عن الضرر الحاصل لكلّ شخص نتيجة عدم تعليق أو إلغاء الشهادة طبقًا للفصلين ١٩ و٢٠ من هذا القانون.

وبالعودة إلى أحكام المادتين ١٩ و٢٠ أعلاه، نجد أنّ المشرّع التونسي قد أجاز تعليق وإلغاء الشهادة بناءً لطلب صاحبها أو بقرارٍ من مزوّد الخدمات وفق حالاتٍ وشروط حدّدها حصرًا، لذا يقتضي التمييز بين الحالات التالية:

أ. حالة إلغاء أو تعليق الشهادة بناءً لطلب من صاحبها، فإنّ هذا الأخير هو الذي يتحمّل المسؤولية عن الضرر الذي لحق بالغير على أساس أحكام المسؤولية التقصيرية، إلاّ في حال كان هناك من عقدٍ يربط هذا الغير مع صاحب الشهادة فتطبّق هنا أحكام المسؤولية التعاقدية.

ب. حالة إلغاء أو تعليق الشهادة بناءً لقرارٍ صادر عن مزوّد الخدمات وألحقت ضررًا بحامل الشهادة، ففي هذه الحالة يمكن إلزامه بالتعويض بالإستناد إلى أحكام المسؤولية التعاقدية.

أمّا إذا ألحق هذا الأمر ضررًا بشخصٍ ثالث فيُلزم مزوّد الخدمات بالتعويض وفقًا لأحكام المسؤولية التقصيرية. ويُلاحظ ممّا تقدّم أنّ المشرّع التونسي قد أعفى مقدّم الخدمات الإلكترونية من المسؤولية في الحالات التي لا يمكن فيها أن يُنسبَ الخطأ إليه كما في حالة طلب حامل الشهادة تعليقها أو إلغاءها أو في حالة مخالفته شروط استعمال هذه الشهادة أو شروط التوقيع الإلكتروني وفق ما جاء صراحةً في الفقرة الأخيرة من الفصل ٢٢ أعلاه.

٢. موقف المشرّع المصري

من مراجعة القانون المصري رقم ١٥ لسنة ٢٠٠٤ المتعلّق بتنظيم التوقيع الالكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات نجد أنّ المشرّع لم يتطرّق إلى مسؤولية مزوّدي الخدمات المدنيّة الناتجة عن مخالفتهم للموجبات الملقاة على عاتقهم، لذا فإنّه لإلزام مزوّدي خدمات التصديق بالتعويض عن ضرر ناتج عن الإخلال بموجباتهم يقتضي العودة للقواعد العامة المنصوص عنها في القانون المدني المصري ولا سيّما أحكام المادتين ١٦٣ و٢١٥ المتعلقتان بالمسؤولية التعاقدية والمسؤولية التقصيرية.

ثالثاً: موقف المشرّع اللبناني

يتّضح من خلال مراجعة القانون ٢٠١٨/٨١، أنّ المشرّع اللبناني لم يعالج موضوع مسؤولية جهات المصادقة بشكل واسع كحال المشرّع الفرنسي أو التونسي، بل اكتفى فقط في المادة ٢٩ بالإشارة إلى جانبٍ واحدٍ من هذه المسؤولية والمتعلّق بمسألة الموثوقية فاعتبر أنّ مقدم خدمات المصادقة المعتمد مسؤولاً عن موثوقية وسائل الحماية المشمولة بشهادة الاعتماد خلافاً لكلّ اتّفاقٍ مخالف، مُلزِمًا إيّاه بالتعويض عن الاضرار التي قد تلحق بزبائنه من جرّاء سوء تنفيذ موجباته التعاقدية.

ونلاحظ أنّ المشرّع اللبناني قد تناول جانبًا واحدًا من المسؤولية ومن التعويض وهو المتعلّق فقط بزبائن مقدّمي الخدمات دون الأشخاص الثالثين، لذا فإنّه لمساءلة مقدّمي الخدمات عن الضرر اللاحق بالغير أو حتى بحامل الشهادة (باستثناء الحالة المنصوص عنها في المادة ٢٩ أعلاه)، نتيجة إخلالهم بموجباتهم أو إهمالهم، فإنّه يقتضي العودة للأحكام العامّة للمسؤولية المنصوص عنها في قانون الموجبات والعقود اللبناني، ولا سيّما أحكام المادتين ١٢٢ و٢٥٢ منه.

الباب الثاني: الحماية الجزائية للتوقيع الإلكتروني

نتيجة تعاظم دور وسائل الاتصال الحديثة في مجال الأعمال التجارية سعت المنظّمات الدوليّة كما وتشريعات الدول لتأمين الحماية القانونية للتجارة الإلكترونية، وبطبيعة الحال للتوقيع الالكتروني الذي يمثّل حجر الزاوية في هذه التجارة، خاصّة وأنّ الجرائم الالكترونية لا تترك أثرًا ماديًا في مسرح الجريمة كغيرها من الجرائم التي تعتبر ذات طبيعةٍ مادّية، فهذه الجرائم يصعب إثباتها خاصّة وأنّ مرتكبيها يمتلكون القدرة على إتلاف أو إضاعة دليل إدانتهم بفترة قصيرة جدًّا[١]، وسنبيّن أدناه مساعي المنظّمات الدولية لمكافحة الجرائم الالكترونية (الفقرة الأولى)، كذلك مساعي التشريعات الوطنية بهذا الخصوص(الفقرة الثانية).

الفقرة الأولى: مساعي المنظّمات الدولية لمكافحة الجرائم الإلكترونية

تعمل الدول على تنسيق جهودها في مجال مكافحة الجرائم الدولية، بدءًا من تجريم الجرائم الإلكترونية، وصولاً إلى وضع القوانين الإجرائية التي تحدّد قواعد الإثبات والإجراءات الجزائية. وتسعى لتسهيل التعاون الدولي فيما بينها، وتنسيق الصكوك الثنائية والإقليميّة والمتعدّدة الأطراف بشأنها، حيثما دعت الحاجة. ويتمّ تسهيل هذه المسائل من خلال المعاهدات الثنائية والمتعدّدة الأطراف.

أولاً: مؤتمر الأمم المتّحدة الثامن لمنع الجريمة

انعقد هذا المؤتمر في مدينة هافانا– كوبا في ٢٧ آب ١٩٩٠، بهدف تعزيز تعاون الدولي لمنع الجريمة ومعاملة السجناء، ومن أبرز التوصيات[٢] التي خرج بها هذا المؤتمر:

١. تحسين تدابير الوقاية والأمن المتعلّقين بالحاسب الآلي مع مراعاة حماية الخصوصية واحترام حقوق الإنسان وحريّاته الأساسية.

---

[١] حاتم، ماضي، محاضرة ألقاها في المؤتمر الإقليمي الأول لمكافحة جريمة الإحتيال الالكتروني، نقابة المحامين في بيروت أيلول ٢٠١٢.

[2] https://www.unodc.org/documents/congress//Previous_Congresses/8th_Congress_1990/046_ACONF.144.IPM.5_Topic_V-UN_Norms_and_Guidelines_in_Crime_Prevention_and_Criminal_Justice_F.pdf,acceced:01-10-2022.

٢. اعتماد إجراءات وتدابير مناسبة لتدريب وتأهيل القضاة والمسؤولين والأجهزة الأمنية المسؤولة عن منع الجرائم الاقتصادية والجرائم المتعلّقة بأجهزة الحاسوب.
٣. التعاون مع المنظّمات المهتمّة بالموضوع في وضع قواعد للآداب المتّبعة في استخدام أجهزة الحاسوب وتدريس هذه الآداب ضمن المنهج الدراسيّ.
٤. اعتماد سياسات بشأن ضحايا الجرائم الإلكترونية تنسجم مع إعلان الأمم المتّحدة بشأن مبادئ العدل المتعلّقة بضحايا الإجرام والتعسّف باستعمال السلطة.

ثانياً: معاهدة مجلس الاتحاد الأوروبي المتعلّقة بالجرائم الالكترونية

وقّعت هذه المعاهدة في بودابست– هنغاريا بتاريخ ٢٠٠١/١١/٢٣ [١]، وقد هدفت لبناء تعاون دولي لا يقتصر فقط على الدول الأعضاء في الاتحاد الأوروبي بل يسعى لضمّ أكبر عددٍ ممكنٍ من الدّول بغية وضع مبادئ مشتركة لمكافحة الجرائم الالكترونية في العالم وتعزيز مقوّمات القضاء والعمل على تطوير التعاون الدولي في هذا المجال، وبالفعل فقد وّقعت على هذه الاتفاقية العديد من الدّول من خارج هذا الاتحاد لا سيّما الولايات المتّحدة الأميركية واليابان وغيرها.

تنطوي المعاهدة أعلاه على اعترافٍ بضرورة حصول انسجام بين قوانين الدول المعنيّة، كما جاء في ديباجتها، وقد تحقّق هذا التعاون في السنوات الماضية عن طريق سلسلة من معاهدات تسليم المجرمين وتبادل المساعدات القانونية وتحقيق ما يُعرف بازدواج العمل الإجرامي [٢].

قد بيّنت في المادة ٢٣ منها على أسس التعاون الدولي، إذ حثّت الدول الأطراف للعمل فيما بينها في الشؤون الجزائية والتدابير المنصوص عنها في التشريعات الخاصّة بخصوص مبدأ المعاملة بالمثل وذلك لأقصى الدرجات الممكنة للأهداف المتعلّقة بعمليّات البحث والتحقيق أو تلك المتعلّقة بالجرائم أو ببيانات الحاسب الآلي، أو لجمع الأدلّة المتعلّقة بالجرائم بصورة إلكترونية.

حدّدت هذه الاتّفاقية الأفعال التي يقتضي على الأطراف سنّ التشريعات واتّخاذ التدابير لتجريمها، أبرزها:

١– الولوج غير المشروع إلى بيانات الحاسب الآلي دون وجه حقّ (المادة الثانية).

---

[1] https://treaties.un.org/doc/Publication/UNTS/Volume%202296/v2296.pdf, acceced: 01-10-2022.

[٢] حاتم، ماضي، المرجع السابق.

٢- اعتراض سير البيانات عمدًا ودون وجه حقّ عن طريق استخدام وسائل فنّية تهدف لقطع عمليّات الإرسال والبثّ (المادّة الثالثة).
٣- التدخّل العمدي ودون وجه حقّ ببيانات الحاسب الآلي عن طريق إتلافها، إلغائها، إفسادها، تغييرها أو تدميرها (المادة الرابعة).
٤- تزوير البيانات الالكترونية والذي يتمّ (بحسب أحكام المادة السابعة من هذه المعاهدة) عن طريق تزويد الحاسب الآلي ببيانات غير صحيحة بهدف دراستها أو معالجتها أو العمل بها لأهدافٍ مشروعة كما لو كانت صحيحة.

الفقرة الثانية: الحماية الجزائية للتوقيع الالكتروني في التشريعات الوطنية

يمكن اختصار أبرز الأفعال الجرميّة التي تلحق بالتوقيع الالكتروني بما يلي:

١- إفشاء سرّية المعلومات من قبل مزوّدي خدمات المصادقة.
٢- إصدار شهادات مصادقة دون ترخيص أو بعد سحبه.
٣- إدلاء صاحب التوقيع ببياناتٍ كاذبة.
٤- التزوير الذي يمكن أن يطال التوقيع الالكتروني بحدّ ذاته أو شهادة المصادقة.
٥- استعمال توقيع الكتروني أو شهادة مصادقة مزوّرين.
٦- الاعتداء على سلامة التوقيع لا سيّما عن طريق حيازة أو إنتاج برامج معلوماتية بهدف تزويره.
٧- الدخول إلى قاعدة بيانات التوقيع الالكتروني عن طريق الغشّ.
٨- فضّ المفاتيح المتعلّقة بعمليّة التشفير.

وقد سعت معظم القوانين الوضعيّة إلى حماية التوقيع الالكتروني وتجريم الاعتداء عليه أو استعماله بشكلٍ غير مشروع، وسنبيّن أدناه موقف القانون الفرنسي (فقرة أولى)، القانون المصري (فقرة ثانية)، القانون التونسي (فقرة ثالثة) والقانون اللبناني (فقرة رابعة).

أولاً: الحماية الجزائية للتوقيع الإلكتروني في القانون الفرنسي

سارع المشرّع الفرنسي لسنّ قوانين تتعلّق بتجريم الجرائم الالكترونية، وقد أجرى عدّة تعديلاتٍ على نصوص قانون العقوبات تصبّ في هذا الإطار، ومن أبرز الأفعال التي جرّمها المشرّع الفرنسي:

١. الولوج عن طريق الغشّ إلى نظام معالجة آلي أو إبقاء الاتصال به بصورة غير مشروعة

عاقب المشرّع الفرنسي في الفقرة الأولى من المادة ٣٢٣-١[1] من قانون العقوبات هذا الفعل الجرمي بالحبس لمدّة سنتين وغرامة قدرها ٦٠ ألف يورو.

وفي حال نتج عن هذا الولوج حذفٍ أو تعديلٍ في بينات هذا النظام أو تغييرٍ في تشغيله عوقب الفاعل بالحبس لمدّة ثلاث سنوات وغرامة بقيمة ١٠٠ ألف يورو.

وفي الحالة التي تُرتكب الجرائم المنصوص عليها في الفقرتين أعلاه ضدّ نظامٍ آلي لمعالجة البيانات الشخصية تنفّذه الدولة، يتمّ زيادة العقوبة إلى الحبس لمدة خمس سنوات وغرامة قدرها ١٥٠ ألف يورو.

٢. فعل إدخال بيانات بصورة غير مشروعة إلى نظام معالجة بيانات آلي أو تعديل أو إلغاء بياناتٍ يحتويها هذا النظام بشكلٍ غير مشروع

حدّدت المادة ٣٢٣-٣[2] من قانون العقوبات الفرنسي عقوبة هذا الفعل بالحبس لمدّة خمس سنوات وبغرامة قيمتها ١٥٠ ألف يورو، على أن تصل هذه العقوبة لمدّة سبع سنوات حبس إضافة إلى غرامة

---

[1] Article 323-1,Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4:

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende.

[2]Article 323-3,Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4:

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

بقيمة ٣٠٠.٠٠٠ يورو في الحالة التي يكون فيها هذا الجرم واقعًا على نظامٍ آلي لمعالجة البيانات الشخصية تنفّذه الدولة.

واللافت أنّ المشرّع الفرنسي قد تيقّن لمدى خطورة هذه الجرائم وأهميّة ردعها لذا فقد فنصّ على معاقبة محاولة ارتكابها كما يتبيّن من نصّ المادة ٤٢٧-١[1] والتي حدّدت عقوبة المحاولة بعقوبة الجرم نفسه.

٣. التزوير

سعى المشرّع الفرنسي لتوفير حمايةٍ للتوقيع الإلكتروني ولكافّة المستندات الالكترونية بشكلٍ عام، فقام بتعديل نصّ المادة ٤٤١ من قانون العقوبات[2]، لتطال بعد تعديلها التزوير الالكتروني، وقد نصّت هذه المادة على ما حرفيته:

"يعتبر تزويرًا كلّ تغيير احتيالي للحقيقة، من شأنه إحداث ضررٍ ويتمّ بأيّة وسيلة كانت، سواء وقع على كتابة أو أي دعامة تعبّر عن الرأي تهدف أو يمكن أن تشكّل إثباتًا لعمل قانوني أو لواقعة لها آثار قانونية." ويلاحظ أنّ المشرّع الفرنسي قد استعمل عبارة "بأيّة وسيلةٍ" وذلك رغبة منه أن يكون هذا النصّ شاملا" كافّة الوسائل التي يمكن أن يتمّ بها التزوير.

وقد حدّد المشرّع الفرنسي عقوبة التزوير واستعمال المزوّر بالحبس لمدّة ثلاث سنوات وبغرامةٍ قيمتها ٤٥.٠٠٠ يورو.

٤. التعدّي على بطاقات السحب الآلي أو بطاقات الوفاء

لحظت المادة ٦٧ من المرسوم تاريخ ١٩٣٥/١٠/٣٠ المعدّلة بموجب القانون رقم ٩١-١٣٨٣ تاريخ ١٩٩١/١٢/٣٠ ثلاث جرائم متعلّقة بالبطاقات الائتمانية، وهي:

أ- تزوير أو تقليد بطاقة سحب أو وفاء.

---

[1] Article 323-7, modifié par Loi n°2004-575 du 21 juin 2004 - art. 46 () JORF 22 juin 2004 : La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

[2] Article 441-1, modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002:

Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques.

Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45 000 euros d'amende.

ب–استخدام أو محاولة استخدام بطاقة سحب أو وفاء مزوّرة أو مقلّدة مع العلم بذلك.

ت–قبول الدفع ببطاقة مزوّرة أو مقلّدة مع العلم بهذا الأمر.

ثانياً: التشريع المصري

سعى المشرّع المصري لتأمين حمايةٍ جزائية للتوقيع الإلكتروني في القانون رقم ٢٠٠٤/١٥ المتعلّق تنظيم التوقيع الالكتروني، ويمكن تلخيص الجرائم التي نصّ عليها القانون المذكور بما يلي:

١. تقديم خدمة المصادقة الالكترونية دون الاستحصال على ترخيص أو بعد سحبه

اشترطت المادة ١٩ من القانون أعلاه على مقدّم خدمات التصديق الاستحصال مسبقًا على ترخيصٍ من هيئة تنمية صناعة تكنولوجيا المعلومات. ويتمثّل السلوك الجرمي في هذه الحالة بانتحال الفاعل صفة مزوّد خدمات المصادقة الحائز على ترخيصٍ بذلك خلافًا للحقيقة، وإصداره شهادة مصادقة بناءً على هذا الأمر.

٢. إفشاء بيانات التوقيع الالكتروني

نصّت المادة ٢١ السالفة الذكر على سرّية بيانات التوقيع الإلكتروني والوسائط الإلكترونية والمعلومات التي تقدّم إلى الجهة المرخّص لها بإصدار شهادات التصديق الإلكتروني محظّرة من قُدّمَت إليه أو اتصل بها بحكم عمله إفشاءها للغير أو استخدامها في غير الغرض الذي قدمت من أجله. ويُقصد بالإفشاء النشر علانية لهذه البيانات. ويُلاحظ أنّ المشرّع المصري قد حصر نطاق التجريم بالجهة مصدرة شهادات التصديق وبمن قُدّمت إليه البيانات السالفة الذكر بحكم عمله. ويرى البعض[١] أنّه كان الأجدى بالمشرّع المصري تجريم انتهاك سرّية بيانات التوقيع الالكتروني بشكلٍ عام.

وبحسب أحكام المادة ٢٣ من القانون عينه، إنّ عقوبة هذه الجريمة هي الحبس وغرامةٌ لا تقلّ عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين، مع عدم الإخلال بأيّة عقوبة أشدّ منصوصٌ عليها في قانون العقوبات المصري أو في أي قانون آخر.

٣. إتلاف أو تعييب أو تزوير التوقيع الالكتروني

[١] أيمن رضا، محمد أحمد, التوقع الإلكتروني , رسالة لنيل درجة الدكتوراه في الحقوق , كلية الحقوق بجامعة عين شمس (القاهرة–مصر)، ٢٠١٠، ص ١٤٢.

نصّت المادة ٢٣/ب من القانون رقم ٢٠٠٤/١٥ على تجريم هذه الأفعال، ويُقصد بالإتلاف شلّ قدرة البرنامج المعلوماتي على العمل بشكلٍ كامل، أمّا التعييب فمن شأنه أن يُفقد هذا النظام قدرته على العمل بشكلٍ جزئي.

ويتحقّق التزوير بحسب أحكام المادّة المذكورة عن طريق الإصطناع أو التعديل أو التحوير أو أي طريق آخر، وبهذا نجد أنّ المشرّع المصري كحال المشرّع الفرنسي لم يحدّد بشكلٍ حصريّ وسائل التزوير وذلك كي يطال التجريم أيّة وسيلةٍ يمكنها تحقيق هذه الغاية.

كذلك جرّمت الفقرة ج من المادة ٢٣ أعلاه استعمال توقيع الكتروني معيب أو مزوّر والاحتجاج به على أنّه توقيع صحيح.

٤. الحصول بغير حقّ على توقيع الكتروني

جرّم المشرّع المصري هذا الفعل بموجب أحكام الفقرة "هـ" من المادة ٢٣، ويتحقّق هذا الجرم عن طريق الاستيلاء على التوقيع الالكتروني عن طريق السرقة أو الإحتيال مثلا" أو بأيّ طريقة تحصل دون رضى صاحب التوقيع.

ويُلاحظ أنّ المشرّع المصري لم يتطرّق إلى الأفعال الجرميّة التي تلحق ببطاقات الإئتمان فيقتضي بالتالي بهذا الخصوص العودة لأحكام قانون العقوبات.

ثالثاً: التشريع التونسي

نظرًا لانتشار التجارة الالكترونية في تونس ولأهمّية التوقيع الالكتروني في هذا المجال سعى المشرّع التونسي لتوفير حمايةٍ جزائية لهذا التوقيع، وقد تضمّن قانون المبادلات والتجارة الالكترونية رقم ٢٠٠٠/٨٣ تاريخ ٢٠٠٠/٨/٩ تجريمًا لعدّة أفعالٍ اعتبرها المشرّع التونسي بمثابة اعتداءٍ على التوقيع الالكتروني وحجّيته، وهذه الأفعال هي التالية:

١. مباشرة خدمات المصادقة بدون ترخيص

نصّ الفصل ٤٦ من القانون رقم ٢٠٠٠/٨٣ على معاقبة كلّ من يمارس نشاط مزوّد خدمات المصادقة الالكترونية دون ترخيصٍ مسبق وأنزل به عوبة السجن لمدّة تتراوح بين شهرين و٣ سنوات وبغرامةٍ تتراوح بين ١٠٠٠ دينار تونسي و١٠٠٠٠ دينار أو بإحدى هاتين العقوبتين.

علمًا أنّ المشرّع التونسي قد أولى الوكالة الوطنية للمصادقة الالكترونية صلاحية منح التراخيص لمقدّمي خدمات المصادقة. وتتمتّع هذه الوكالة بسلطةٍ رقابية للتثبّت من مدى توافر الشروط المطلوبة بمقدّمي خدمات المصادقة الالكترونية.

٢. إفشاء المعلومات المتعلّقة بالتوقيع الالكتروني

نصّ الفصل ٥٢ من القانون أعلاه على معاقبة مزوّد خدمات المصادقة ومساعديه الذين يفشون أو يحرّضون أو يشاركون في إفشاء المعلومات التي عُهدت إليهم في إطار تعاطي نشاطاتهم باستثناء تلك التي أجاز صاحب الشهادة كتابيًا أو الكترونيًا في نشرها أو الإعلام به. وقد أحال المشرّع التونسي إلى الفصل ٢٥٤ من المجلة الجزائية المتعلّقة بإفشاء السرّ المهني لتحديد عوبة هذه الجريمة والتي حدّدها الفصل المذكور بالسجن مدّة ستة أشهر وبغرامة وقدرها ١٢٠ دينار. ويُلاحظ أنّ المشرّع التونسي إسوةً بالمشرّع المصري قد اكتفى بمعاقبة مقدّم خدمات المصادقة ومساعديه.

٣. التصريح قصدًا بمعطياتٍ خاطئة

نصّ الفصل ٤٧ من القانون السالف الذكر على معاقبة كلّ من يصرّح بمعطيات خاطئة لمورّد خدمات التوثيق الالكتروني. ويهدف تجريم هذه الأفعال إلى حماية التجارة الالكترونية والحؤول دون استقبال بياناتٍ خاطئة يمكن أن تؤثّر على الثقة المُفترض توافرها في هذه التجارة، فبالتالي إنّ التجريم المذكور يزيد من ثقة المتعاملين في التجارة الالكترونية ويحافظ على حقوقهم.[١]

٤. فضّ تشفير توقيع الكتروني

نصّ الفصل ٤٨ من قانون المبادلات والتجارة الالكترونية التونسي على معاقبة كلّ من استعمل بصفةٍ غير مشروعة عناصر تشفيرٍ شخصيّة متعلّقة بتوقيع الغير بالسجن لمدّة تتراواح بين ستّة أشهر وعامين وبغرامةٍ مالية تتراوح بين ١٠٠٠ و ١٠٠٠٠ دينار.

٥. التعدّي على البطاقات المصرفية

بخلاف المشرّع المصري، سعى المشرّع التونسي لمعاقبة الجرائم المتعلّقة بالبطاقات المصرفية عن طريق نصوصٍ خاصّة. وبالفعل فقد جرّم بموجب القانون رقم ٢٠٠٥/٥١ تاريخ ٢٠٠٥/٦/٢٧، والمتعلّق بالتحويل الالكتروني للأموال، أفعال التعدّي على البطاقات المصرفية. كذلك جرّم الفصل ١٧ من القانون المذكور ثلاثة

[١] عبد الفتاح، حجازي، النظام القانوني لحماية التجارة الالكترونية، دار الفكر الجامعي، مصر ٢٠٠٢، ص. ٨٣.

أفعالٍ بهذا الخصوص، ونظرًا لخطورة هذه الأفعال اعتبرها المشرّع التونسي أنّها تشكّل جنايةً فعاقب عليها بالسجن لمدّة عشرة سنوات وبالغرامة بقيمة عشرة آلاف دينار، وهذه الأفعال هي:

أ. تزوير أداة تحويل إلكتروني للأموال
ب. استعمل أداةً مزوّرة مع العلم بذلك.
ج. قبول تحويل باستعمال أداة تحويل إلكتروني للأموال مزوّرة مع العلمه بذلك.

ويُلاحظ أنّ المشرّع التونسي قد جرّم تزوير البطاقات المصرفية دون أن يحدّد الوسائل أو الطرق المتّبعة لهذه الغاية. ونظرًا للطابع التقني الذي يميّز البطاقة المصرفيّة فإنه يصعب تخيّل تزويرها عن طريق تغيير البيانات المدوّنة عليها، وبالتالي فإنّ المقصود بالتزوير هو الإصطناع، ويُعنى بالإصطناع في هذا المجال خلق بطاقةٍ مصرفية بكامل أجزائها على غرار البطاقة الأصليّة[١].

٦. الاستعمال غير القانوني للبطاقة المصرفية

نصّ الفصل ١٨ من القانون رقم ٢٠٠٥/٥١ على معاقبة كلّ من استعمل أداة تحويلٍ الكتروني للأموال دون إذن صاحبها بالسجن مدّة ثلاث سنوات وبغرامة وقدرها ثلاثة آلاف دينار، وقد لحظ المشرّع التونسي عقوبةً مخفّفة لهذا الجرم مقارنةً مع الجرائم المنصوص عنها في الفقرة السابقة ومردّ ذلك هو استعمال بطاقةٍ مصرفية صادرة عن الجهة المختصّة بإصدارها إنّما جرى استعمالها من قبل غير صاحبها، وتتحقّق هذه الجريمة سواء باستخدام جسم البطاقة المصرفية مع رقمها السرّي أو بالاكتفاء بالبيانات المدوّنة عليها عن طريق استعمالها للشراء على شبكة الإنترنت.

ويُلاحظ أنّ المشرّع التونسي، ونظرًا للصبغة التقنيّة والفنّية لهذه الجرائم، فقد حرص أن تتمّ معاينتها عن طريق أشخاصٍ متخصّصين بهذا المجال، مع إمكانية الإستعانة بأفراد الضابطة العدلية وفق ما نصّ عليه الفصل ٤٣ من القانون رقم ٢٠٠٠/٨٣ أو الفصل ١٩ من القانون رقم ٢٠٠٥/٥١.

[١] المؤتمر التاسع لرؤساء المحاكم العليا، بيروت ١٧ و ١٨ كانون الأول ٢٠١٨، الجرائم االلكترونية الواقعة على الأموال في القانون التونسي، بيان الوفد التونسي، منشور على الرابط التالي:

http://www.cassation.tn/fileadmin/user_upload/news/crimes-electroniques-sur-argent-en-droit-tunisien.pdf, consulté le: 10-10-2022.

رابعاً: التشريع اللبناني

سعى المشرّع اللبناني من خلال القانون ٢٠١٨/٨١ إلى معالجة بعض الثغرات في قانون العقوبات والتي كانت تحول دون ملاحقة بعض الجرائم الالكترونية، وبالفعل فقد قام المشرّع اللبناني بموجب المادة ١١٨ من القانون ٢٠١٨/٨١ بتعديل نصّ البند الثالث من المادة ٢٠٩ من قانون العقوبات، المتعلّقة بتعريف وسائل النشر ليضيف إليها وسائل النشر الالكترونية.

كذلك قام المشرّع اللبناني بموجب المادة ١١٩ من قانون المعاملات الالكترونية بتعديل نصّ المادة ٤٥٣ من قانون العقوبات المتعلّقة بالتزوير ليشمل هذا الجرم الوسائل الإلكترونية لتصبح هذه المادة بعد تعديلها على الشكل التالي: "التحريف المتعمّد للحقيقة، في الوقائع، أو البيانات التي يثبتها صكّ أو مخطوط أو دعامة ورقية أو إلكترونية أو أية دعامة أخرى". أمّا بالنسبة أبرز الجرائم التي نصّ عليها القانون رقم ٢٠١٨/٨١ فهي:

١. الولوج غير المشروع الى نظام معلوماتي

نصّت الفقرة الأولى من المادة ١١٠ من القانون رقم ٢٠١٨/٨١ على معاقبة كلّ من أقدم، بنيّة الغشّ، على الوصول او الولوج الى نظام معلوماتي بكامله او في جزء منه او على المكوث فيه، بالحبس من ثلاثة أشهر الى سنتين وبالغرامة من مليون الى عشرين مليون ليرة لبنانية او بإحدى هاتين العقوبتين. أمّا الفقرة الثانية فقد نصّت على عقوبة مشدّدة وهي الحبس من ستة أشهر الى ثلاث سنوات والغرامة من مليونين الى اربعين مليون ليرة، إذا نتج عن العمل الغاء البيانات الرقمية او البرامج المعلوماتية او نسخها او تعديلها او المساس بعمل النظام المعلوماتي.

ويُلاحظ أنّ الفقرة الأولى قد أوجبت للعقاب توافر نيّة الغشّ بحيث لا عقاب في حال الولوج إلى نظام معلوماتي عن طريق الخطأ وبحسن نيّة، أمّا بالنسبة للفقرة الثانية، فقد قصد بها المشرّع اللبناني جرم القرصنة، وقد حرص على تشديد العقوبة إذ نتج ضرر ملحوظ عن الفعل المادّي المتمثّل بالوصول أو الولوج إلى نظام معلوماتي أو المكوث فيه[١].

٢. التعدي على سلامة النظام

[١] هاني، الحبال، المرجع السابق، ص ٨٢.

نصّت المادّة ١١١ على معاقبة كلّ من أقدم، بنيّة الغش وبأي وسيلة على إعاقة عمل نظام معلوماتي أو على إفساده بالحبس من ستّة أشهر الى ثلاث سنوات وبالغرامة من ثلاثة ملايين الى مئتي مليون ليرة لبنانية او بإحدى هاتين العقوبتين.

ويلاحظ أيضًا أنّ المشرّع اللبناني قد افترض أيضًا، كما في المادة السابق ذكرها، توافر نيّة الغشّ لمعاقبة هذا الفعل.

٣. التعدّي على سلامة البيانات الرقمية

نصّت المادّة ١١٢ من القانون رقم ٢٠١٨/٨١ على معاقبة كلّ من أدخل بيانات رقمية، بنية الغش، في نظامٍ معلوماتي وكلّ من ألغى أو عدّل، بنيّة الغشّ، البيانات الرقمية التي يتضمّنها نظامًا معلوماتيًا بالحبس من ستة أشهر الى ثلاث سنوات وبالغرامة من ثلاثة ملايين الى مئتي مليون ليرة لبنانية او بإحدى هاتين العقوبتين. ويرى البعض[١] في هذا السياق أنّ نصّ هذه المادّة هو" في غاية الأهمّية كونها حلّت معضلةً كبيرة، حيث كان يتعذّر على المحاكم تجريم هذا النوع من التعدّيات لانتفاء نصّ خاصّ ممّا دفع القضاة للاجتهاد وتطبيق قانون الملكية الفكرية عندما كان التعدّي يطال القطاع الخاص".

أمّا في حال حصول اختراقٍ لبياناتٍ متعلّقة بالإدارات العامّة أو مواقع المصارف، فيرى القاضي حمادة أنّ بعض المحاكم حاولت التوسّع بتفسير المادة ٢٨٢ ق.ع. ولا سيّما عبارة "معلومات" الواردة فيها لتطبّق على هذه الأفعال نصّ السرقة وهو توجّه خاطئ بالنسبة لحمادة، وبالفعل نجد أنّ محكمة التمييز الجزائية قد أيّدت موقف القاضي حمادة إذ جاء في أحد قراراتها[٢] ما يلي:

"حيث يتبيّن من الوقائع المدعى بها أن موضوعها إقدام المدعى عليه المميز على نقل معلومات الكترونياً من هاتف (Data) المدعية المستدعى ضدها إلى جهاز الكمبيوتر العائد إليه وقد توصل القرار المطعون فيه إلى أن المستدعي المدعى عليه قد أقدم على سرقة معلومات موجودة على هاتف المدعية المستدعى بوجهها دون علمها وأدانه بجرم المادة (٦٣٦/عقوبات).

---

[١] زاهر، حمادة، المحامي العام الاستئنافي في بيروت، مؤتمر "المعاملات الإلكترونية من التشريع إلى التطبيق" المنعقد في بيت المحامي في بيروت بتاريخ ١٥ آذار ٢٠١٩، منشور على الرابط:
https://www.youtube.com/watch?v=ZAv_vGcEKjw&t=3909s

[٢] محكمة التمييز، قرار رقم ٢٠٦ تاريخ ٢٠١٨/٥/١٠، منشور في المصنّف الالكتروني.

وحيث أن القرار المطعون فيه لم يبحث فيما إذا كانت المعلومات الالكترونية المدعى سرقتها تنطبق على مفهوم المال المنقول المقصود بالمادة (٦٣٥/عقوبات) فيكون القرار المطعون فيع قد أخطأ بعدم مناقشة أحد العناصر المكوّنة للجرم فيقتضي نقضه سنداً للفقرة (ب) من المادة (٢٩٦/أ.م.ج.)."

٤. تقليد وتزوير البطاقة المصرفية والنقود الالكترونية والرقمية والشيك الالكتروني والرقمي

نصّت المادة ١١٦ من القانون ٢٠١٨/٨١ على ما حرفيّته: " يعاقب بالحبس من ستّة أشهر الى ثلاث سنوات وبالغرامة من عشرة ملايين الى مئتي مليون ليرة لبنانية او بإحدى هاتين العقوبتين كل من:

أ. قلّد بطاقةً مصرفية أو زوّرها.

ب. استعمل او تداول، مع علمه بالأمر، بطاقةً مصرفيةً مزوّرة أو مقلّدة.

ج. قبل قبض مبالغ من النقود مع علمه بأن الايفاء تمّ بواسطة بطاقة مصرفية مزوّرة او مقلّدة.

د. قلّد نقوداً الكترونية أو رقميّة.

هـ. استعمل، مع علمه بالأمر، نقوداً الكترونية أو رقميّة مقلّدة.

و. قلّد شيكاً الكترونياً او رقمياً.

ز. استعمل مع علمه بالامر، شيكاً الكترونياً او رقمياً مقلداً.

تطبق احكام المادتين ١١٤[١] و ١١٥[٢] على الافعال الجرمية المذكورة في هذه المادة." يُلاحظ أنّ المشرّع اللبناني لم ينصّ على كيفيّة وقوع التزوير بل جاء شاملا" بهذا الخصوص، وقد حذا حذو نظيره الفرنسي إذ نصّ في المادة ١١٥ من القانون رقم ٢٠١٨/٨١ على معاقبة المحاولة في الجرائم السالفة الذكر الواردة في الفصل الأول من الباب السادس من هذا القانون، كذلك بالنسبة للجرائم المنصوص عنها في المادة ١١٦ السالفة الذكر. وحسنًا فعل كون هذه الجرائم هي من فئة الجنح وبالتالي لا عقاب على المحاولة في الجنح إلا

---

[١] نصّت المادة ١١٤ من القانون رقم ٢٠١٨/٨١ على ما يلي:

"يعاقب بالحبس من ستة أشهر الى ثلاث سنوات وبالغرامة من ثلاثة ملايين الى مئتي مليون ليرة لبنانية او بإحدى هاتين العقوبتين كل من استورد او أنتج او حاز او قدّم او وضع في التصرف او نشر، دون سبب مشروع، جهازاً او برنامجاً معلوماتياً او اي بيانات معدة او مكيفة، بهدف اقتراف اي من الجرائم المنصوص عليها في المواد السابقة من هذا الفصل."

[٢] نصّت المادة ١١٥ من القانون عينه على ما يلي:

"يعاقب بالعقوبة ذاتها على المحاولة في الجرائم المنصوص عليها في هذا الفصل."

بنصّ خاصّ وذلك بحسب أحكام الفقرة الأولى من المادة ٢٠٢ ق.ع.

ونظرًا لخطورة هذه الجرائم لم ينصّ المشرّع اللبناني على تخفيض عقوبتها فلا تجد الفقرة الثانية من المادة ٢٠٢ المذكورة تطبيقًا لها في هذا السياق كون المادة ١١٥ أعلاه قد نصّت صراحةً على إنزال عقوبة الجرم نفسه على المحاولة.

تجدر الإشارة إلى أنّه وقبل صدور القانون ٢٠١٨/٨١، استقرّ اجتهاد المحاكم على إخضاع فعل تزوير البطاقة لأحكام المادة ٤٥٣ ق.ع. التي تحدد العناصر المشتركة لجرائم التزوير المستندي معتبرًا أنّ هذه البطاقة هي من فئة من الأوراق الخاصة، وبالتالي فيُعاقب على جرم التزوير سندا" للمادة ٤٧١ ق.ع. وعلى جرم استعمال بطاقة مزورة مع العلم بالأمر سندا" للمادة ٤٥٤ معطوفة على المادة ٤٧١ ق.ع.:

".....وحيث يتبين من ذلك ان الاسناد الوارد ذكرها في المادة ٤٥٣ تجارة والتي يعتبر تزويرها من قبيل الجناية هي تلك القابلة للتداول ويمكن تسعيرها في الاسواق المالية في حين ان بطاقات الائتمان لا تتمتع بهذه المميزات اذ انها ليست قابلة للتداول بل تصدر باسم من يودع اموالا في المصرف يستعملها لسحب هذه الاموال؛ كما انه لا يمكن تسعيرها في الاسواق المالية الامر الذي يؤدي الى عدم اعتبارها بمثابة الاوراق الرسمية ويكون تزويرها بالتالي من قبيل التزوير في الاوراق الخاصة...[١]."

وقد استغلّت المحاكم الجزائية في لبنان مرونة نصّ المادة ٦٥٥ ق.ع.، التي حدّدت وعلى سبيل المثال لا الحصر أبرز أوجه المناورات الاحتيالية وصيغها، إذ جاء في هذه المادة:

تُعتبر من المناورات الاحتيالية "...، ما أفسح المجال واسعًا أمام الاجتهاد كي يتوسع في تفسير هذه المناورات لتشمل" المناورات المعلوماتية."

وبالفعل فقد استغلّ القاضي الجزائي اللبناني المرونة التي اتّسمت بها صياغة المادة ٦٥٥ من قانون العقوبات، لمعاقبة جرائم المعلوماتية، وقد قُضي[٢] أنّ " استصناع البطاقات المصرفية واستعمالها لحمل صيدلي على تسليمه بضاعة يدخل ضمن إطار المناورات الاحتيالية المنصوص عنها في المادة ٦٥٥ ق.ع." فأدين الفاعل بجنح التزوير واستعمال المزوّر والإحتيال وذلك سندا لاحكام المواد ٤٧١ و٤٥٤/٤٧١ و٦٥٥ من قانون العقوبات.

---

[١] محكمة التمييز الغرفة الثالثة، تاريخ ٢٠٠٧/٦/٦ ، منشور في مجموعة المستشار الإلكتروني .

[٢] القاضي المنفرد الجزائي في بيروت، قرار رقم ٢٠٠٩/٥٨٧، تاريخ ٢٠١٠/١٠/٥، غير منشور.

الخاتمة

شكّل ظهور التوقيع الالكتروني وتطوّره إلى خلق واقعٍ جديدٍ في الميدان القانوني، لذا فقد سعت معظم التشريعات والمنظمات الدولية لوضع أطرٍ لهذا التوقيع وهو ما بحثناه في دراستنا، كذلك فقد بحثنا بصور التوقيع الالكتروني التي تختلف بحسب التقنيّة المستخدمة، فمنها ما يعتمد على رقم سرّي وأخرى تعتمد على خواصّ الإنسان الطبيعية كبصمة اليد أو العين، ومنها ما يعتمد على تقنية التشفير. كذلك بحثنا في سياق دراستنا مدى إمكانية التوقيع الالكتروني من تحقيق أهداف التوقيع اليدوي لا بل تتخطّاها كون هذا التوقيع قادر على التثبّت من عدم حصول أيّ تلاعب طال الرسالة الإلكترونية خاصّة في الحالة التي يتمّ فيها استعمال التوقيع الرقمي المستند إلى تقنية التشفير.

وقد بحثنا بالوسائل التقنية لحماية التوقيع الالكروني والتي تتمثّل بالتشفير وبتدخّل شخص ثالث وهو مقدّم خدمات المصادقة الذي يقوم بتوثيق التوقيع عن طريق شهادةٍ يصدرها، كذلك بحثنا بالحماية الجزائية التي وفّرتها القوانين الوضعيّة للتوقيع الالكتروني.

ومن خلال بحثنا وتمحيصنا بالنصوص القانونية العربية والأجنبية، تبيّن لنا مدى أهميّة هذا التوقيع وإمكانيته تخفيف أعباء عديدة عن كاهل مستخدميه، وقد برزت أهميّة التوقيع الالكتروني والحاجة أكثر فأكثر للاستعانة به في أوائل العام ٢٠٢٠ وحتى يومنا هذا وذلك نتيجة انتشار فيروس كورونا المستجدّ المعروف بِـ Covid 19 الذي اعتبرته منظمة الصحة العالمية وباءً عالميًّا، فاضطرّت دول العالم بأسره لاتّخاذ إجراءات للحدّ من انتشار هذا الوباء. ونتيجة هذه القيود اضطرّت العديد من الدول لتعديل قوانينها الوضعيّة بغية تسهيل أمور مواطنيها.

وقد ساهم التوقيع الإلكتروني في حلّ العديد من مشاكل المواطنين إذ ساعدهم على إنجاز معاملاتهم عن بعد، كذلك فقد سعت العديد من الدول لإجراء تعديلاتٍ في تشريعاتها لتخطّي العقبات التي سبّتها هذه الجائحة، فقد أجاز المشرّع الفرنسي إجراء الطلاق عن بعد كذلك بعض الأعمال المتعلّقة بكاتب العدل، كذلك أجاز المشرع التونسي المتقاضين من مباشرة بعض الإجراءات القانونية بالطرق الإلكترونية.

أمّا على الصعيد الوطني، فقد اعتُبِر إقرار المشرّع اللبناني للقانون رقم ٢٠١٨/٨١ خطوةً إجابيّةً طال انتظارها رغم أنّ البعض يرى أنّ هذا القانون ما كان ليقرّ لولا الزخم التشريعي الذي حصل في البرلمان اللبناني

في العام ٢٠١٨ مواكبةً لمؤتمر سيدر[١]. إلاّ أنّه ورغم إجابيّة هذه الخطوة، فقد اعترى القانون المذكور عدّة أخطاء جوهريّة في صياغته، نذكر من بينها نصّ المادة ٧٩ المتعلّقة بهيئة إدارة أسماء نطاق الإنترنت ".lb" فنصّت هذه المادة أنّ انتخاب أعضاء هذه اهيئة يتمّ من قبل الهيئة نفسها، وهو خطأ فادح أدّى إلى ولادة هيئة ميتة، كذلك نجد أنّ هذا القانون لم يتبنّ المفاهيم الحديثة لحماية البيانات الشخصية لا سيّما العايير الأوروبية GDPR بل تبنّى معايير تخطّاها التطوّر التكنولوجي والقانوني.

ونجد أيضًا أنّ العديد من الأخطاء اللغوية في هذا القانون كذلك في ترجمة بعض المصطلحات التقنيّة، فمصطلح Online ترجمته المادة ٣٢ من القانون المذكور بـ "على الخط" بدلا" من " متّصل بالانترنت"، كذلك في نصّ المادة ١٠٦ التي نصّت على العقوبة الأخفّ أي الغرامة فبل عقوبة الحبس وقد لاقى هذا الأمر انتقادًا من قبل البعض[٢] باعتباره يشكل مخالفة لأبسط قواعد العلم الجزائي.

أمّا فيما يختصّ بموضوع دراستنا أي التوقيع الالكتروني فنجد أنّ القانون ٢٠١٨/٨١ لم يعرّف هذا التوقيع إسوةً بالتشريعات العربية أو الأجنبية، كذلك يُلاحظ أنّ هذا التوقيع لم يأخذ حيّزًا كبيرًا في القانون المذكور لا سيّما لناحية تنظيم عمل مقدمي خدمات المصادقة وتحديد مهامها ومسؤولياتها بشكلٍ واضحٍ وفصّل.

التوصيات

استنادًا لم تقدّم في هذه الدراسة، فإنّنا نقترح التوصيات التالية:

١- إطلاق عجلة المجلس الوطني للاعتماد COLLIBAC المُنشأ بموجب القانون رقم ٢٠٠٤/٥٧٢ والذي لا زال حتّى تاريخه غير فاعلٍ.

٢- إصدار المرسوم المتعلّق بالأسناد الرسمية المنصوص عنه في المادة ٨ من القانون رقم ٢٠١٨/٨١.

٣- إصدار مراسيم تطبيقية وفقًا لأحكام المادة ١٣٣ من القانون ٢٠١٨/٨١ لمواكبة التطوّر الحاصل في ميدان التكنولوجيا الرقمية والذي ينعكس بشكلٍ مباشر على التوقيع وسائل الإثبات الالكترونية بشكلٍ عام والتوقيع الالكتروني بشكلٍ خاصّ والإسترشاد بما توصّل إليه في هذا المجال التشريع الفرنسي لا

---

[١] شربل، شبير، منشور على الرابط التالي:
https://www.elnashra.com/news/show/1552395/%7B%7Burl%7D%7D تمّ الإطلاع عليه بتاريخ: ٢٠٢٢/١٠/٥٥.

[٢] هاني، الحبال، المرجع السابق، ص. ٧٩.

سيّما في المرسوم رقم ١٤١٦-٢٠١٧ وما نصّ عليه المشرّع المصري في اللائحة التنفيذية الجديدة لقانون ٢٠٠٤/١٥ الصادرة بتاريخ ٢٠٢٠/٤/٢٣.

٤- تنظيم دوراتٍ تدريبية للقضاة والمساعدين القضائيين لمواكبة التطوّر التقني في مجال الإثبات الالكتروني.

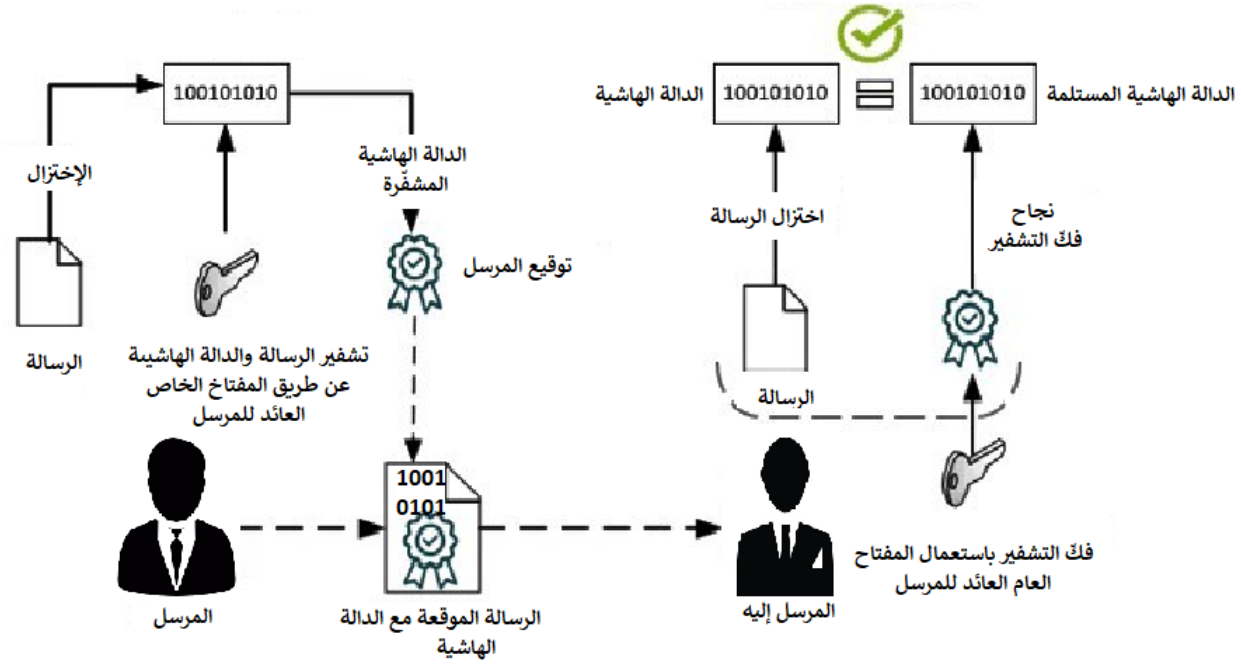
٥- العمل على إنشاء محاكم مختصّة بالتجارة الالكترونية.

٦- تنظيم عمل مقدمي خدمات المصادقة بشكلٍ أدقّ ولا سيّما تلك المتعلّقة بمهامها كتعليق أو إلغاء شهادات المصادقة الذي لم يلحظه القانون ٢٠١٨/٨١ رغم أهميته، علمًا أنّ هذا الأمر قد نصّ عليه اقتراح القانون المقدّم من النائب غنوة جلّول.

٧- تعديل قانون العقوبات لناحية المسؤولية الجزائية لمقدّمي خدمات المصادقة نظرًا لما تشكّله من أهميّة في مجال التجارة الالكترونية لا سيّما لناحية إرساء الثقة والإستقرار في هذا المجال.

الملاحق

ملحق رقم ١: رسم بياني بعنوان كيفيّة عمل التوقيع الرقمي، من إعداد الطالب



ملحق رقم ٢: نموذج العقد المعتمد من قبل بنك لبنان والمهجر المتعلّق بالخدمات الإلكترونية

BLOM BANK s.a.l.
Peace of Mind

eBlom Portal Usage Conditions

This agreement is made and entered into by and between

BLOM Bank s.a.l.

Referred to hereafter as "The bank", OR "BLOM Bank".

And

Mr./Ms

eBlom Portal Username :

eBlom Portal Mailbox :

eBlom Portal Primary Mobile Number :

eBlom Portal Secondary Mobile Number :

Nickname :

referred to hereafter as "The Customer"

1. Positioning and Definition of the eBlom Portal

1.1.The eBlom Portal is meant to be an electronic channel through which BLOM BANK delivers selected products and services using the Internet. While BLOM BANK may, at its own discretion, choose to provide access, through the eBlom Portal channel, to any subset of the products and services that are available through other traditional or electronic delivery channels, BLOM BANK may also provide access, through the eBlom Portal delivery channel, to products and services that are not available through other channels. BLOM BANK reserves the right to expand or to reduce the range of products and services available through this channel at any time without prior notice. BLOM BANK reserves also the right to put certain limitations, exclusions and/or constraints that may vary with time and/or according to customer profiles on the services and products that are provided through this channel.

1.2. The eBlom Portal may be used by BLOM BANK's sister or affiliated companies that may provide electronic access to their products and services through the eBlom Portal channel.

1.3. Customer agrees and undertakes to be bound by and to comply with any and all of this agreement's annexes and by all BLOM BANK's procedures, requirements, restrictions, instructions or any additional conditions pertaining to the access and use of the eBlom Portal website and its related services as may be issued by BLOM BANK from time to time and/or posted on the eBlom Portal website.

2.Enrollment to the eBlom Portal

The enrollment to the eBlom Portal has to be executed according to "Annex 1: eBlom Portal Enrollment and Authentication Procedures".
The customer shall create his eBlom Portal Credentials by supplying the required information. After positive verification of the customer's identity using applicable procedures, the customer shall be enrolled to the eBlom Portal.
After successful enrollment to the eBlom Portal, the customer shall activate his eBlom Portal credentials.

3.eBlom Portal Authentication Methods

The customer shall authenticate himself to the eBlom Portal as per "Annex 1: eBlom Portal Enrollment and Authentication Procedures".
Each person completing the authentication process is deemed by BLOM BANK to be a rightful user regardless of whether the party in question is actually an Authorized User.
BLOM BANK shall be regarded as authorized to execute any instruction coming via the eBlom Portal provided that the system has granted access on the basis of a positive identity check as per BLOM Bank's electronic records.

4. Risks

4.1. The customer bears solely the risks arising from (i) the manipulation of his information system (i.e. PC, Network ...) by wrongful users, (ii) the compromise of the username and/or its protecting password, (iii) the loss of the mobile phone, (iv) or in conjunction with data transmission.

4.2. The customer is aware of the risks that may arise from transactions conducted using the eBlom Portal delivery channel via open systems accessible to anyone (such as but not limited to: public and private data transmission networks, Internet servers, access providers...). The encryption used cannot prevent unauthorized persons from carrying out targeted manipulations on the INFORMATION system of an Authorized User, especially via the Internet, for which the customer must assume responsibility.

If a connection with BLOM BANK is established through the eBlom Portal channel, the Authorized User agrees to monitor, for the purpose of combating errors and abuses, the correctness of the BLOM BANK address dialed and the encryption of the data transmission using a security symbol as defined in electronic communication material on the eBlom Portal website. In the event of any discrepancy, the connection must be broken off immediately and the observations made must be reported to BLOM BANK.

4.3. Moreover, the Authorized User agrees to take the necessary precautions to ensure the security of any data stored in that person's INFORMATION system.

5. Obligation to Exercise Due Diligence

5.1. It is the responsibility of the Customer to be aware of any security precautions required to protect his eBlom Portal credentials which are defined in this agreement's annexes. The Customer must take the most recent and up-to-date security measures in order to minimize the security risks associated with Internet use.

5.2. The customer is obliged to take particular care to protect the customer credentials from unauthorized access or use. The eBlom Portal credentials are to be kept secret. They may under no circumstances be divulged, let alone, passed on, to other persons or stored electronically.

5.3. Passwords must be chosen in such a way that they are not easy to detect or work out (i.e., not based on telephone numbers, birth-days, car license plates, etc.). The customer shall change from time to time his eBlom Portal password.

5.4. Customer shall make sure that any computer or other device which is used to access the eBlom Portal is free from and adequately protected against spyware, computer viruses and other invasive, destructive or disruptive components by using Anti-Virus, Anti-Spyware, Personal Firewall and Application Firewall. Customer is responsible for applying the latest security patches on his operating system, browser and other applications installed on his computer or another device used to access the eBlom Portal.

5.5. Customer shall comply with the instructions or recommendations we may issue to him from time to time about eBlom Portal security, as displayed and accessible from time to time through the eBlom Portal. However, we do not guarantee that these security tips are exhaustive or complete.

5.6. When the customer is instructed to contact the Call Center, customer shall make sure to dial the Call Center's number on 961-1-753000 or 961-1-758000 or on another number as published on BLOM BANK's official website or official communication material.

5.7. The customer undertakes to notify and/or contact BLOM BANK immediately if there is reason to believe, suspect that or have knowledge that:
(a) the eBlom Portal credentials may have been compromised;
(b) the mobile number registered with BLOM BANK is lost, missing or replaced
(c) the SMS-based One-Time-Passwords (OTPs) sent by BLOM BANK (where applicable) has become known or been revealed to any person other than the customer
(d) there has been an unauthorized access to the eBlom Portal or there has been an unauthorized transaction or instruction on accounts accessible via the eBlom Portal

6. Accountability

6.1. The customer is accountable and legally liable for all activities carried out after the system has authorized access on the basis of a positive credentials check. The Customer cannot, in any case, reject an operation executed via the eBlom Portal and its related services and in case of litigation; the electronic support kept at BLOM BANK will constitute the sole conclusive evidence. The Customer acknowledges that it is impossible, regarding the kind of electronic operations and the practices that administer them to require another evidence.

6.2. BLOM BANK shall be regarded as charged with executing any orders and complying with any instructions and notifications coming to it via the eBlom Portal delivery channel, provided the system has authorized access on the basis of a positive credentials check; any such orders, instructions or notifications are deemed to have been entered by an Authorized User. Thus BLOM BANK has performed correctly if it complies with orders, instructions and notifications received by it within the scope of the business relationship.

6.3. When orders are placed with BLOM BANK via the eBlom Portal channel, BLOM BANK is nevertheless entitled to refuse or to disregard individual orders at its own discretion in the event of inadequate cover or in the event that an order exceeds an approved line of credit, or if the order is erroneous, incomplete, inconsistent or if it does not comply with the applicable laws or with BLOM BANK's internal policies and procedures or with BLOM BANK's sister or affiliated companies' internal policies and procedures.

6.4. BLOM BANK cannot be held responsible of delaying, deferring or suspending the execution of any order, nor can it be held responsible of refusing or disregarding any order, for any reason whatsoever.

6.5. All the articles, clauses and provisions of the opening of account contracts or other contracts entered into between BLOM BANK and/or its sister or affiliated companies and the Customer will apply to the present contract to the extent that they do not contradict, refute or are not inconsistent with the articles and provisions of this contract.

7. Limitation of Liability

7.1. The customer agrees and acknowledges the agreed authentication procedures outlined in "Annex 1: eBlom Portal Enrollment and Authentication Procedures" and he confirms that BLOM BANK shall in no event be liable for any direct, indirect, incidental, punitive, special or consequential damages or economic loss incurred by him arising from but not limited to:
(a) losses, damages or costs arising from or referable to the Instructions given via the eBlom Portal being incorrect or inaccurate in any manner whatsoever
(b) losses, damages or costs arising as a result of use of compromised eBlom Portal Credentials by a fraudulent third-party
(c) any delay or failure to send SMS-based One-Time-Passwords (OTPs) or SMS-based login and/or transaction notification (where applicable)

1/4

BLOM BANK S.A.L.
Peace of Mind

(d) losses, damages or costs arising as a result of any service agreements prescribed by telecommunications carriers and/or Internet service providers or as a result of any machine, system or communications breakdown, interruption, malfunction or failure, default or fault of any telecommunications carriers and/or Internet service providers and/or SMS service providers or operators;
(e)damages for loss of profits, goodwill, use, data or other intangible losses arising from or in connection with causes such as but not limited to:
(i) any use, inability to use , interruption or disturbance in the use of the eBlom Portal for any reason whatsoever; or
(ii)any system, hardware, software, telecommunications, server or connection failure, error, omission, interruption, delay in transmission, or computer virus.
(f) Losses, damages or costs suffered due to transmission errors, technical faults or defects, breakdowns or illegal intrusion or intervention in terminals, screens or other systems of the Customer or in systems generally accessible to the public.

8.Force Majeure

8.1. BLOM BANK and/or its sister or affiliated companies shall not be responsible or liable to the customer for:
(a) delays or failure in performance, whether foreseeable or not; and/or
(b) any losses, expenses or damages howsoever arising, whether foreseeable or not, resulting from or due to any circumstances or causes whatsoever which are not within the reasonable control of BLOM BANK and/or its sister or affiliated companies.

9. Notice

9.1. Any or all of the BLOM BANK's and/or its sister or affiliated companies services delivered through the eBlom Portal channel can be terminated at any time, either by the customer by letter, or by BLOM BANK with immediate effect without prior notice. Notwithstanding such notice of termination, BLOM BANK and/or its sister or affiliated companies shall still be entitled on behalf of the Customer to settle with legally binding effect any transaction commenced before the termination notice was received by BLOM BANK and/or its sister or affiliated companies.

10. Electronically displayed legal instructions/restrictions

10.1. The customer is hereby informed that in view of the internationalization and globalization of the markets BLOM BANK is compelled to issue legal instructions/restrictions on electronically communicated information and certain services. These instructions/restrictions are considered to be legally binding on the customer and the latter is duly notified as soon as they are posted on the eBlom Portal Website. If he/she does not wish to accept them, he/she must cease using the information/services in question immediately. The complete text of these instructions/restrictions is available at any time from BLOM BANK or at the eBlom Portal website.

11. Suspending the access to eBlom Portal

11.1. When expressly requested to do so, BLOM BANK shall suspend electronic access via the eBlom Portal channel. Access can be suspended at BLOM BANK's initiative or following a request submitted by the customer himself.

11.2. BLOM BANK reserves the right to suspend the access, at any time, without prior notice, if so is judged appropriate. Suspended access at BLOM BANK's initiative cannot be restored until so requested by the customer in writing and only if the conditions that led to the suspension are not applicable anymore.

11.3. Suspended access by request from the customer shall be restored at the suspension maturity date which is determined by the customer, provided that by this date this agreement remains valid.

12.Provisions governing power of attorney

12.1. Under the terms of this agreement, a holder of a power of attorney to be considered as the authorized signatory on behalf of the customer needs to be explicitly authorized in writing by the Customer to use the eBlom Portal channel in order for him to be able to use this power of attorney to access BLOM BANK's and/or its sister or affiliated companies' products and services via the eBlom Portal channel. This written authorization is deemed to be valid in each case until it is explicitly revoked by the Customer, notwithstanding any registration or publication to the contrary.

12.2. All the terms and conditions of this agreement do apply on a holder of a power of attorney who uses this authorization to represent the customer who granted him this power of attorney.

12.3. It is hereby expressly agreed that the deletion of such a holder's authority to sign does not automatically invalidate the eBlom Portal credentials. Nor does the death or loss of the capacity to act of the customer or the holder of a power of attorney automatically result in the written authorizations being revoked or the eBlom Portal credentials being rendered invalid. On the contrary, explicit written notification from the customer, the heirs or the eligible persons is required to block access in each case.

12.4. When explicit written instructions to block access are communicated, the Customer bears any risks resulting from the use of his eBlom Portal credentials before the block has had time to be put into effect using normal procedures.

13. Case of a joint account / product co-ownership

13.1. Under the terms of this agreement, a customer who is a co-holder of an account or a co-owner of a product or service at BLOM BANK and/or at its sister or affiliated companies cannot request eBlom Portal credentials related to that account, product or service unless he has obtained a written and explicit authorization to do so from all the other account co-holders or product co-owners.

13.2. In cases where such an authorization has been granted by the account co-holders or product co-owners, all the terms and conditions of this agreement apply on all the account co-holders or product co-owners.

13.3. It is hereby expressly agreed that the revocation of such a co-holder's or co-owner's authority by anyone of the remaining co-holders or co-owners should be done in writing and that it will result in the termination of the present agreement.

13.4. The co-holders or co-owners bear solely, jointly and severally and without division between them any risks resulting from the use of the eBlom Portal credentials before the termination has had time to be put into effect using normal procedures.

14. Service Fees

14.1. The Customer will be informed by electronically communicated instructions available at the eBlom Portal website about the service fees and the way to pay these fees. These instructions are considered to be legally binding on the Customer and the latter is duly notified as soon as they are posted on the eBlom Portal Website. If he does not wish to accept them he must cease to use the service immediately.

15. Duration of this agreement

15.1. The duration of this agreement is set to one year starting from the date of the signature of this agreement by the Customer.

15.2. This agreement is subject to automatic renewal for one year at every new expiry unless a written instruction stating the contrary has been sent at least one month prior to expiry by the customer to BLOM BANK.

15.3. Pending orders or instructions received via the eBlom Portal from the Customer, under this agreement prior to its expiry, are executed by the bank even if their execution date is beyond the expiry date of this agreement, provided that the customer accounts permit the execution of such orders or instructions.

16. Case of Death or Incapacity

16.1. In case of death or incapacity of the Customer or of the holder of a power of attorney, the deletion of the authority to sign and the invalidation of the eBlom Portal credentials cannot occur until explicit written notification is sent by the heirs or by the eligible person and duly notified to the Bank.

16.2. Even when such explicit written notification is communicated to the bank, the heirs or the eligible person bear solely any risks resulting from the use of the eBlom Portal credentials under this contract before its block or invalidation has had time to be put into effect using normal procedures.

17. Applicable Law

17.1. All disputes arising in connection with the present contract shall be finally settled under the Rules of Conciliation and Arbitration at the Beirut Chamber of Commerce and Industry by one or more Arbitrators appointed in accordance with the said Rules.

17.2. The contracting parties declare accepting the provisions of the said Rules and undertake to abide by them.

17.3. The Customer, as much as needed, raises towards the arbitrators and any other persons in charge of the arbitration or who intervenes in its course and in the execution of the sentence and within the limits that BLOM BANK considers necessary for the defense of its interests, the Bank secrecy, as defined in the Lebanese Banking Secrecy Law, on the operations executed within the scope of this contract.

17.4. The Lebanese Law is applicable for the proceedings and as Law of the merits of the litigation.

18. Successors

18.1. The present agreement binds the parties and their successors in an indivisible way.

19. Special Condition

19.1. All the terms of this "eBlom Portal Usage Conditions" constitute the "General Conditions" contract and therefore are automatically applicable to any annex to it signed by the Customer.

2/4

تابع ملحق رقم ١

BLOM BANK SAL
Peace of Mind

Annex 1
"eBlom Portal Enrollment and Authentication Procedures"
to the "eBlom Portal Usage Conditions"

1.Creation of the eBlom Portal Credentials

The customer shall create his eBlom Portal Credentials by supplying a username, a valid mailbox, a primary and secondary mobile phone that he has in his possession and three Security Questions & Answers.

After positive verification of the customer's signature against the bank's specimen, the customer shall be enrolled to the eBlom Portal. After successful enrollment to the eBlom Portal, the customer shall receive a first-time password on his mailbox and a One-Time-Password (referred thereafter as OTP) as an SMS on his primary mobile phone. The customer shall use the first time password and the OTP in addition to his username to login to the eBlom Portal. Upon successful login, the customer shall be required to change his password to a new value and set his Password Reset Question and Answer (to be used whenever the customer would need to reset his password) in order for his eBlom Portal credentials to be activated.

2.eBlom Portal Authentication Methods

2.1. eBlom Portal Authentication Method

All customers enrolling to the eBlom Portal shall need to authenticate themselves using a two-factor authentication method which uses a combination of two different factors, including the customer's user name and password which are the part of the credentials that a customer knows and an SMS-based OTP which is the other part of the credentials that the customer would need to retrieve from his mobile phone that he has in his physical possession.

The customer shall receive on a regular basis a batch of SMS-based OTPs in order to be used for subsequent logins after the first-time eBlom Portal Credentials activation.

The customer shall receive an SMS notification upon successful login to the eBlom Portal.

For convenience and on his own risk, the customer can choose to receive OTPs via email in which case, the OTPs will be sent as an email to the customer's registered mailbox.

The customer can also choose to remove the OTP security feature on his own risk by using any method that shall be put at his disposal by BLOM BANK including written or electronic instructions or through the Call Center and to login to the eBlom Portal using his username and password only.

2.2. Bypass of the OTP security feature

The customer who chooses to remove the OTP security feature and to login to the eBlom Portal using his username and password only should know that BLOM BANK strongly discourages the removal of the second factor of authentication as the customer can be easily exposed to Internet-based attacks and/or password discovery attacks.

The customer opting for the single factor of authentication for the purpose of logging in to the eBlom Portal shall do so at their own risk and shall not hold BLOM BANK responsible for any loss or damage resulting from a fraudulent usage of his eBlom Portal Credentials. In addition, BLOM BANK's electronic records shall be the only evidence for the customer's applied authentication method at any time.

Each person completing the authentication process as described above is deemed by BLOM BANK to be a rightful user regardless of whether the party in question is actually an Authorized User. BLOM BANK shall be regarded as authorized to execute any instruction coming via the eBlom Portal provided that the system has granted access on the basis of a positive identity check.

2.3. Change of the eBlom Portal Credentials

Customer shall be able to change one or more of his eBlom Portal Credentials should the need for doing so arise. The customer shall be guided on how to do so. In some cases and as BLOM BANK deems appropriate, the customer shall need to enter an authentication code that will be sent on his registered mailbox. In other cases, the customer may need to contact BLOM BANK's Call Center and after doing so, the Call Center agent will make sure of the customer's identity by taking him through a security procedure in order to carry out the required change in the eBlom Portal Credentials. The customer shall be aware that this call may be recorded and that this recording will constitute a proof of the operation executed and will be kept in BLOM BANK's electronic records.

BLOM BANK shall not be liable for any losses arising as a result of a refusal by the Call Center agent to carry out any of the matters referred to in the Clause above.

2.4. Security Questions and Answers

Customer shall supply upon enrollment three Security Questions and Answers that would be used to verify the customer's identity whenever the need arises. Customer shall choose security questions that have an easy-to-remember answer but are personal enough to remain private.

تابع ملحق رقم ١

BLOM BANK S.A.L.
Peace of Mind

Annex 2
"eBlom Portal Service Subscription: eBlom Internet/Mobile Banking" to the "eBlom Portal Usage Conditions"

This agreement is made and entered into by and between

BLOM Bank s.a.l.
Referred to hereafter as "The bank", OR "BLOM Bank"

And

Mr. /Ms.

Service Name: eBlom Internet/Mobile Banking

Client ID :

eBlom Portal Username

referred to hereafter as "The Customer"

1.Positioning and Definition of eBlom Internet/Mobile Banking

1.1. eBlom Internet/Mobile Banking is meant to be an electronic channel through which BLOM BANK delivers selected products and services using the Internet/Mobile. While BLOM BANK may, at its own discretion, choose to provide access, through the eBlom Internet/Mobile Banking channel, to any subset of the products and services that are available through other traditional or electronic delivery channels, BLOM BANK may also provide access, through the eBlom Internet/Mobile Banking delivery channel, to products and services that are not available through other channels. BLOM BANK reserves the right to expand or to reduce the range of products and services available through this channel at any time without prior notice. BLOM BANK reserves also the right to put certain limitations, exclusions and/or constraints that may vary with time and/or according to customer credentials on the services and products that are provided through this channel.

2.Enrollment to eBlom Internet Banking

2.1. The customer shall enroll to the eBlom Portal in order to gain access to the eBlom Internet/Mobile Banking service.
Conditions stated in the eBlom Portal Usage Conditions and all its related annexes shall constitute an integral part of the present document and these documents shall constitute the Enrollment Agreement between BLOM BANK and the Customer.
After positive enrollment to the eBlom Portal, the customer shall have a set of credentials in order to gain access to the eBlom Internet/Mobile Banking service.

3. Information from eBlom Internet/Mobile Banking

3.1. BLOM BANK does not guarantee in any way the accuracy or completeness of information and reports obtained using eBlom Internet/Mobile Banking delivery channel; in particular, information regarding accounts, safekeeping accounts (account balances, statements of account, transactions, etc.), is not legally binding and must be considered provisional.

4. Privacy

4.1. BLOM BANK is hereby explicitly authorized to process all information on the customer systematically for its own marketing requirements.

4.2. BLOM BANK is bound by Lebanese laws on banking secrecy and data protection.

4.3. The customer acknowledges and accepts the fact that BLOM BANK may delegate to some persons, external to the bank, the task of performing some jobs related to the operations, maintenance or auditing of the eBlom Internet/Mobile Banking channel. These persons are usually bound by a non-disclosure agreement, however they are not necessarily bound by the Lebanese banking secrecy law.

لائحة المصادر والمراجع

١. مراجع باللغة العربية

أ. الكتب باللغة العربية

١) بايبر، فريد؛ شون، ميرفي، علم التشفير (مقدّمة قصير جداً)، ترجمة: محمد، سعد طنطاوي، مراجعة: هاني فتحي سليمان، مراجعة علمية: حاتم بهيج، مؤسسة هنداوي للتعليم والثقافة، الطبعة الأولى، مصر، ٢٠١٦

٢) الحبال، هاني، قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي، بيروت ،٢٠١٩.

٣) الحجار، وسيم، الإثبات الإلكتروني، المنشورات الحقوقية صادر، بيروت ٢٠٠٢

٤) حجازي، عبد الفتاح، النظام القانوني لحماية التجارة الالكترونية، دار الفكر الجامعي، مصر ٢٠٠٢.

٥) حمزة، طارق، النقود الإلكترونية كإحدى وسائل الدفع- تنظيمها القانوني والمسائل الناتجة عن استعمالها، منشورات زين الحقوقية، لبنان، ٢٠١١.

٦) الدبيسي، وائل، البطاقات المصرفية أنظمة وعقود، منشورات صادر، بيروت، ٢٠٠٤.

٧) الدحداح، خليل، بطاقة الاعتماد، بدون ناشر، بيروت ١٩٩٨.

٨) دويدار، هاني، النقل البحري والجوي، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، ٢٠٠٨.

٩) السنهوري، عبد الرزاق، الوسيط في شرح القانون المدني، ج ٢، المجلد الأول، دار النهضة العربية، مصر،١٩٨٢.

١٠) صليبا، رانيا، الإثبات بين التقليد والحداثة في ظل قانون أصول المحاكمات المدنية ومتطلبات العصر: دراسة مقارنة، المنشورات الحقوقية صادر، بيروت، ٢٠٠٨.

١١) عبد الحميد، ثروت، التوقيع الإلكتروني- ماهيته- مخاطره وكيفية مواجهتها- مدى حجيته في الإثبات، دار الجامعة الجديدة، مصر، ٢٠٠٧

١٢) العلبي، أنس، النظام القانوني لبطاقات الاعتماد، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٥.

١٣) العوجي، مصطفى، القانون المدني، الجزء الثاني، المسؤولية المدنية، منشورات الحلبي الحقوقية ٢٠٠٩.

١٤) عيد، إدوار، موسوعة أصول المحاكمات والإثبات والتنفيذ، صادر، الجزء ١٤، لبنان، ١٩٩١.

١٥) عيسى، طوني، التنظيم القانوني لشبكة الانترنت: دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية، صادر للمنشورات الحقوقية، بيروت ٢٠٠١.

١٦) فتح الله بصلة، رياض، حدود الإثبات العلمي في قضايا التزييف والتزوير، دار النهضة العربية، مصر، ٢٠١٠.
١٧) فريدريش، يوهانس، تاريخ الكتابة، ترجمة د. سليمان أحمد الضاهر، منشورات الهيئة العامة السوريّة للكتاب، سوريا، ٢٠١٣.
١٨) القارح، شربل، قانون الإنترنت، ج٨، المنشورات الحقوقية صادر، بيروت، ٢٠١٩.
١٩) قنديل، سعيد، التوقيع الالكتروني ماهيته–صوره– حجيته في الاثبات بين التداول والاقتباس، دار الجامعة الجديدة، مصر ٢٠٠٦، ص ١٠٤.
٢٠) مشيمش، ضياء، التوقيع الإلكتروني – دراسة مقارنة، المنشورات الحقوقية صادر، بيروت، ٢٠٠٢.
٢١) المهتار، بسام، معاهدة بروكسل وتعديلاتها، منشورات الحلبي الحقوقية الطبعة الأولى، بيروت، ٢٠٠٦.
٢٢) موسى، أحمد، النقود الإلكترونية وتأثيرها على دور المصارف المركزيّة في إدارة السياسة النقدية، الجديد في أعمال المصارف من الوجهتين القانونية والسياسية، أعمال المؤتمر العلمي السنوي لكليّة الحقوق بجامعة بيروت العربية، منشورات الحلبي الحقوقية، الطبعة الأولى، الجزء الأول، ٢٠٠٢.
٢٣) الناشف، أنطوان؛ الهندي، خليل، العمليات المصرفية والسوق المالية، مؤسسة حديثة للكتاب، الجزء الأول، لبنان، ١٩٩٨.
٢٤) ناصيف، الياس، الكامل في قانون التجارة، عويدات للطباعة والنشر، الجزء الأول، بيروت، ١٩٩٩.
٢٥) ناصيف، الياس، موسوعة العقود المدنية والتجارية، مطبعة نمنم، الجزء الأول، بيروت،١٩٨٦.

ب. مجلات ودوريات

١) أدهم، المعتصم بالله، دراسة بعنوان الإثبات الإلكتروني في ضوء قانون المعاملات الإلكترونية رقم ٢٠١٨/٨١، مجلّة الجامعة العربية، بيروت.
٢) خضور، أحمد، منظومة تقنية لتأمين أمن تبادل المعلومات– مجلة جامعة دمشق للعلوم الهندسية، المجلد الرابع والثلاثون، العدد الثاني، سوريا ٢٠١٨.
٣) دحماني، سمير، التصديق الإلكتروني كوسيلة أمان لآليات الدّفع الإلكتروني عبر الإنترنت، مجلّة الدراسات القانونية المقارنة، المجلد ٠٤، العدد ١، الجزائر، ٢٠١٨.
٤) زهرة، محمد المرسى، الدليل الكتابي وحجية مخرجات الكومبيوتر في الاثبات، في المواد المدنية والتجارية، من بحوث مؤتمر القانون والكومبيوتر والانترنت، ١–٣ أيار ٢٠٠٠، جامعة الامارات العربية المتحدة.

٥) شرف الدين، أحمد، ضوابط حجية المحررات الالكترونية في الاثبات تعليق على تحديثات اللائحة التنفيذية لقانون التوقيع الالكتروني في ضوء أحكام محكمة النقض، المجلة الدولية للفقه والقضاء والتشريع المجلد ٢، العدد ١، ٢٠٢١.
٦) شريفة، هنية، الشيك الإلكتروني كوسيلة وفاء حديثة، مجلّة الحقوق والعلوم الإنسانية، العدد ٢٠، المجلّد الأول، الجزائر، كانون الأول ٢٠١٤.
٧) ضياء، نعمان، المصادقة الإلكترونية على ضوء قانون التبادل الإلكتروني للمعطيات القانونية، مجلة الدراسات القانونية والقضائية، العدد الأول، الجزائر، تشرين الأول ٢٠٠٩.
٨) ماضي، حاتم، محاضرة ألقاها خلال المؤتمر الإقليمي الأول لمكافحة جريمة الاحتيال الالكتروني، نقابة المحامين في بيروت، أيلول ٢٠١٢.
٩) منصور، سامي، الاثبات الالكتروني في القانون اللبناني: معاناة قاض، العدل عدد ١، ٢٠٠١

ج. دراسات ورسائل وأطاريح

١) رضا أيمن، احمد محمد، التوقع الإلكتروني، رسالة لنيل درجة الدكتوراه في الحقوق, كلية الحقوق بجامعة عين شمس، مصر، ٢٠١٠.
٢) الصفدي، عبير، رسالة بعنوان: النظام القانوني لجهات توثيق التوقيع الالكتروني، جامعة الشرق الأوسط للدراسات العليا، الأردن ٢٠٠٩، ص. ٧٤

د. قوانين لبنانية

١) قانون الموجبات والعقود تاريخ ٠٩/٠٣/١٩٣٢ منشور في الجريدة الرسمية عدد ٢٦٤٢، تاريخ النشر ١١/٠٤/١٩٣٢، ص. ٢-١٠٤.
٢) قانون أصول المحاكمات المدنية رقم ٨٣/٩٠، منشور في الجريدة الرسمية عدد ٤٠ تاريخ ١٩٨٣/١٠/١، ص. ٣-١٢٨.
٣) قانون العقوبات، مرسوم اشتراعي رقم ٣٤٠ تاريخ ١٩٤٣/٣/١، منشور في الجريدة الرسمية عدد ٤١٠٤ تاريخ ١٩٤٣/١٠/٢٧، ص. ١-٧٨.
٤) قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي رقم ٢٠١٨/٨١ تاريخ: ٢٠١٨/١٠/١٠، منشور في الجريدة الرسمية عدد ٤٥ تاريخ ٢٠١٨/١٠/١٨، ص. ٤٥٤٦-٤٥٦٨.

هـ. تشريعات عربية

١) تشريعات مصرية

أ- قانون الإثبات في المواد المدنية والتجارية رقم ٢٥ لسنة ١٩٦٨ الجريدة الرسمية العدد ٢٢ في ٣٠ مايو ١٩٦٨، آخر تعديل في ٦ تموز ٢٠٠٧.

ب-قانون ١٥ لسنة ٢٠٠٤، تاريخ ٢١ نيسان ٢٠٠٤، المتعلّق بتنظيم التوقيع الالكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، منشور في الجريدة الرسمية عدد ١٧ تابع (د) في ٢٢ نيسان ٢٠٠٤ ص. ١٧.

ت-قرار وزير الاتصالات وتكنولوجيا المعلومات رقم ٣٦١ لسنة ٢٠٢٠ تاريخ ٢٠٢٠/٤/١٩، الخاصّ بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات رقم ١٥ لسنة ٢٠٠٤، الوقائع المصرية، العدد ٩٥ (تابع)، ٢٠٢٠/٤/٢٣.

ث-قرار وزير الاتصالات وتكنولوجيا المعلومات رقم ١١٩ لسنة ٢٠٠٥ تاريخ ٢٠٠٥/٥/١٥، الخاصّ بتعديل اللائحة التنفيذية لقانون التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات رقم ١٥ لسنة ٢٠٠٤ الوقائع المصرية، العدد ١١٥ (تابع)، ٢٠٠٥/٥/٢٥.

٢) تشريعات تونسية

أ- قانون الالتزامات والعقود تاريخ 1906،/12/15 منشور في الرائد الرسمي ملحق عدد ١٠٠ بتاريخ ١٥ ديسمبر ١٩٠٦.

ب-قانون التحكيم التونسي عدد ٤٢ لسنة ١٩٩٣، تاريخ ١٩٩٣/٤/٢٦، منشور في الرائد الرسمي عدد ٣٣ بتاريخ ١٩٩٣/٥/٤ ص. ٥٨٠

ت-قانون الموجبات والعقود التونسي ١٥ ديسمبر ١٩٠٦، منشور في الرائد الرسمي ملحق عدد ١٠٠ بتاريخ ١٥ ديسمبر ١٩٠٦.

ث-قانون العقوبات تاريخ ١٩١٣/٧/٩، منشور في الرائد الرسمي عدد ٧٩ المؤرخ في ١٩١٣/١٠/١.

ج- قانون رقم ٢٠٠٠/٨٣ تاريخ ٢٠٠٠/٨/٩، المتعلّق بالمبادلات والتجارة الإلكترونية، منشور في الرائد الرسمي عدد ٦٤ تاريخ ٢٠٠٠/٨/١١.

ح- قرار وزير تكنولوجيا الاتصالات مؤرّخ في ٢٠٠١/٧/١٩ متعلّق بضبط المواصفات التقنية لمنظومة إحداث الإمضاء الإلكتروني، منشور في الرائد الرسمي للجمهورية التونسية بتاريخ ٢٠٠١/٦/٢٧، ص. ٢٣٨٥.

د. معاهدات ونصوص دولية

١) قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية مع دليل الإشتراع، ٢٠٠١، منشورات الأمم المتحدة، رقم المبيع A.02.V.8

٢) معاهدة مجلس الاتحاد الأوروبي المتعلّقة بالجرائم الالكترونية المنعقدة في بودابست– هنغاريا بتاريخ ٢٠٠١/١١/٢٣.

٣) اتفاقية الأمم المتّحدة للنقل البحري للبضائع بالبحر لسنة ١٩٧٨، المعروفة باتّفاقية هامبورغ تاريخ ١٩٧٨/٣/٣.

ذ. قرارات قضائية

١) الهيئة العامة لمحكمة التمييز، قرار رقم (٢٩) تاريخ ٢٠١٧/٤/٢٤، كساندر ٢٠١٧، عدد ١

٢) محكمة التمييز، الغرفة السادسة، قرار رقم ١ تاريخ ١٩٩٧/١/١٤، كساندر ١٩٩٧، عدد ١

٣) محكمة التمييز، الغرفة الثالثة، قرار تاريخ ٢٠٠٧/٦/٦، منشور في مجموعة المستشار الإلكتروني.

٤) محكمة التمييز، قرار رقم ٢٠٦ تاريخ ٢٠١٨/٥/١٠، منشور في مجموعة المستشار الإلكتروني.

٥) استئناف بيروت، قرار تاريخ ١٩٧٠/١١/٢١، مجلّة العدل لسنة ١٩٧٠، عدد ٢

٦) القاضي المنفرد الجزائي في بيروت– قرار رقم ٢٠٠٩/٥٨٧، تاريخ ٢٠١٠/١٠/٥، غير منشور.

٧) نقض مصري، طعن رقم ١٥٧ – صادر بتاريخ ١٩٧٣/٤/٢٤، مكتب فني ٢٤ ج ٢ ق ١١٧ ص ٦٦٧.

٨) نقض مصري، طعن رقم ٧٨/١٧٠٥١، تاريخ ٢٠١٩/٣/٢٨، مكتب فني ٧٠ ق ٦٤ ص ٤٨٢.

2. Bibliographie

A- Ouvrages

1) A. F.Fausse, la signature électronique transaction et confiance sur internet, Dunod, Paris,2000.

2) C.Feral Schuhl, cyberdroit , le droit à l'épreuve de l'internet, 5ème edition Dalloz, 2009-2010.

3) D. Becourt ; S. Carneroli, Depôt legal de l'écrit à l'electronique, éditions Litec, France, 2001.
4) E.Caprioli, Signature électronique et dématerialisation, éditions Lexis Nexis,Paris 2014.
5) J. Stern, La science du secret, Ed. Odile Jacob, Paris,1998.
6) M-C. Piatu, Les Libertes individuelles à l'epreuve des NTIC, Editions Presses Universitaires de Lyon, Pul, 2001.
7) P. Le Tourneau, Contrats informatiques et éléctroniques, Dalloz, 7ème édition, Paris, 2012-2013.
8) T. verbiest ; E. wery : Le droit de l'internet et de la société de l'information, édition larcier, Belgique,2001.
9) T. Piette- Coudol- Signature électronique- Editions Litec, Paris 2001
10) V. Sedaillan, Droit de l'internet, collection AUI, Paris 1997
11) V. Grautrais- Le contrat electronique international- Editions Bruylant, Bruxelles, 2002.
12) V. Grautrais- Le contrat electronique international- Editions Bruylant, Bruxelles, 2002, p. 123.
13) X.Linant de Bellefonds et A. Hollande, Droit de l'informatique et de la Télématique, 2ème édition, Masson, Paris, 1990.

B-Revues et Articles

1) C. DEVYS, Du sceau numérique à la signature numérique, Rapp. OJTI, nov.1995, pub.in OJTI, ss dir. C. -DHENIN, Vers une administration sans papiers, Paris, La documentation française, 1996
2) D.Gobert; E. Montero, La signature dans les contrats et les paiements électroniques: l'approche fonctionnelle Publié au DA/OR, avril 2000, n° 53
3) E. Caprioli, EDI et commerce électronique au regard des normes juridiques internationales, Lamy Contrats internationaux, Div. 2, Annexe 100/2-1, 1996

4) E. Caprioli, Preuve et signature dans le commerce électronique, droit et patrimoine, n° 53 , Decembre 1997.
5) F. Chamoux, la loi du 13 juillet 1980, une ouverture sur de nouveaux moyens de preuve, JCP édition, 1981, II, 13491

c- Législations Françaises et Européennes

1) Loi nº 2004-575 du 21 juin 2004, relative à la confiance dans l'économie numérique, JORF n°0143, 22 juin 2004, p. 11168.
2) loi n°83-353 du 30 avril 1983, relative à la mise en harmonie des obligations comptables des commercants et de certaines sociétés avec la iv^{ème} directive adoptée par le conseil des communautés européennes le 25-07-1978, jorf du 3 mai 1983.
3) Décret n° 75-1123 du 5 décembre 1975 instituant un nouveau code de procédure civile Le nouveau code de procédure civile, JORF n°0285 du 9 décembre 1975, numéro complémentaire page1.
4) Ordonnance n ° 2016-131 du 10 février 2016, contenant le code civil français .
5) Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.
6) Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique, JORF n°0229 du 30 septembre 2017.
7) Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,JO n° L 281 du 23/11/1995 p. 0031 – 0050,

8) directive 1999/93/ce du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques JO L 13 du 19.1.2000, p. 12.
9) règlement (ue) no 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, Publié au JO L, No L 257/73,28/8/2014

D- Jurisprudence

1) Cass. Civ. 1ère, 30 sept. 2010, N° 09-685555, BICC N° 734, 15 Janv. 2011
2) Cass, com, 2 décembre 1997, JCP G 1998
3) Cass. 2e civ 30 avril 2003, 00-46.467, Bulletin 2003 II N° 118
4) Cass. 2e civ., 28 mai 2020, n° 19-11.744, Bull 2020
5) CA Montpellier, 17e ch., sect. D, 9 avril 1987, JCP., éd. G., II, n° 20984
6) CA Besançon, ch soc. 20 oct 2000; SARL Chalets Boisson c/Gros: Jurisdata n° 2000-125582

٣. مواقع إنترنت

١) https://www.almaany.com/ar/dict
٢) https://www.dgobert.be/images/pdf/signature_rgdc.pdf
٣) https://www.iso.org/obp/ui/#iso:std:iso:7498:-2:ed-1:v1:en
٤) /https://www.lebarmy.gov.lb/ar/content
٥) https://uncitral.un.org/sites/uncitral.un.org/files/media-documents
٦) https://doctrine.fr/d/CA/Nimes/2019/C52D70AD1C86427FE2BCD
٧) https://www.tuntrust.tn/sites/default/files/reglementationsAR/Arrete
٨) https://backlinko.com/whatsapp-users
٩) https://faq.whatsapp.com/820124435853543
١٠) https://web.mit.edu/ecom/Spring1997/gr13/overview.html

(١١ www.Shippingandfreightresource.com
(١٢ https://www.caprioli-avocats.com/fr/
(١٣ www.inodocs.com/blog/electronic
(١٤ https://al-akhbar.com/Opinion
(١٥ https://publicadministration.un.org/egovkb
(١٦ https://academy.binance.com/ar/articles/history-of-cryptography
(١٧ https://repo.zenksecurity.com/
(١٨ https://md5decrypt.net
(١٩ https://bletchleypark.org.uk/our-story/enigmas-of-bletchley-park
(٢٠ https://academy.binance.com/ar/articles/history-of-cryptography
(٢١ https://www.lri.fr/~fmartignon/documenti/systemesecurite/4-DES.pdf
(٢٢ https://down.ketabpedia.com/files/bnr/bnr14599-1.pdf
(٢٣ www.security.nknu.edu.tw/crypto/faq/html
(٢٤ https://eur-lex.europa.eu/legal-content
(٢٥ https://www.ssi.gouv.fr/uploads/2014
(٢٦ https://itida.gov.eg/Arabic/Pages/E-Signature.aspx
(٢٧ http://industry.gov.lb/Media/News
(٢٨ https://treaties.un.org/doc/Publication/UNTS
(٢٩ https://www.unodc.org/documents/congress
(٣٠ http://www.cassation.tn/fileadmin/user_upload/news
(٣١ https://www.youtube.com/watch?v=ZAv_vGcEKjw&t=3909s
(٣٢ https://www.elnashra.com/news/show
(٣٣ https://www.giac.org/
(٣٤ https://www.cairn.info/revue-humanisme-2006-4-page-85.htm
(٣٥ /http://www.protectionproject.org/wp-content/uploads/2013/12
(٣٦ https://tech-echo.com/2021/09/nft-what-is-nfts-crypto-how-work-create-sell-buy/

قائمة المحتويات