الإرشاد الثاني

المعاملات الإلكترونية والتواقيع الإلكترونية

٢

الورقة البحثية الخلفية لإرشاد المعاملات الإلكترونية والتواقيع الإلكترونية

١- هدف البحث

تتناول الورقة البحثية الخلفية موضوع المعاملات والتواقيع الإلكترونية في الدول العربية، رصد وتحليل التشريعات العربية التي عالجت هذه المواضيع ومقارنتها مع بعض التشريعات العالمية، وبالتالي تسليط الضوء على النقاط التي أغفلتها التشريعات العربية بهدف مساعدة الحكومات العربية على معالجتها وتنظيمها من خلال سن أو تعديل تشريعاتها الموجودة أو إصدار تشريعات أو تنظيمات خاصة تتعلق بالمعاملات والتواقيع الإلكترونية.

٢- موضوع وأقسام البحث

ينص مشروع إعداد "إرشادات الإسكوا للتشريعات السيبرانية" على أن تؤخذ بعين الاعتبار الخبرات الدولية والإقليمية المتراكمة مع تركيز خاص على "توجيهات الاتحاد الأوروبي" في هذا المجال لأجل صياغة الإرشاد الخاص بالمعاملات والتواقيع الإلكترونية.

شملت أعمال البحث بشكل رئيسي المواضيع التالية:

١) السندات والتواقيع الإلكترونية والإثبات الإلكتروني: تنظيم السندات الإلكترونية العادية والرسمية، النسخ في السندات الإلكترونية، تحديد الشروط القانونية للاعتراف بالكتابة الإلكترونية وقوتها الثبوتية، والشروط الأساسية لصحة التوقيع الإلكتروني، تحديد البيانات والآليات اللازمة لإنشاء التوقيع إلكتروني، موثوقية التوقيع الإلكتروني وحمايته من التقليد والتزوير، حفظ السندات الإلكترونية والشروط المطلوبة لصحتها.

٢) واجبات ومسؤوليات مزود خدمات المصادقة الإلكترونية وصاحب الشهادة والطرف المعوّل: تحديد وتنظيم مسؤوليات مزود خدمات المصادقة الإلكترونية الذي يصدر شهادة مصادقة موصوفة باعتبار أنها تتمتع بقرينة الموثوقية، ومسؤوليته عن سلامة منظومة التوقيع الإلكتروني الخاصة به وعن سريتها، الآلية المتبعة لإصدار شهادات التصديق وموثوقيتها، ومفاعيل إلغاء شهادة المصادقة؛ مسؤولية صاحب شهادة المصادقة عن صحة المعلومات المتعلقة به المقدمة إلى مزود خدمات المصادقة وتحديثها؛ بالإضافة إلى مسؤولية الطرف المعوّل عن عدم اتخاذ خطوات معقولة للتحقق من موثوقية التوقيع الإلكتروني أو للتحقق من صلاحية الشهادة أو وقفها أو إلغائها أو وجود قيود عليها.

٣) الاعتراف القانوني بشهادات المصادقة الإلكترونية الأجنبية: تعتبر شهادات المصادقة الإلكترونية الأجنبية الموصوفة معادلة من الناحية القانونية لشهادات المصادقة الصادرة عن مزود خدمات مصادقة وطني في حالات معينة، من شأنها أن تساعد على حل الإشكاليات الناشئة عن تجاوز التعاملات الإلكترونية الحدود الوطنية بفعل الإنترنت، والمساهمة في توحيد المتطلبات التي يخضع لها مزودو خدمات المصادقة وشهادات المصادقة.

٤) العمليات المصرفية: تشمل أوامر الدفع والتحاويل الإلكترونية للأموال النقدية، بطاقات الدفع والسحوبات المصرفية الآلية، بالإضافة إلى النقود والشيكات الإلكترونية؛ تحديد مواصفات الأنظمة الإلكترونية المستعملة في العمليات المتعلقة بأوامر الدفع والتحاويل الإلكترونية؛ مسؤولية العميل عن أوامر الدفع أو التحاويل الإلكترونية؛ ومسؤولية المصرف أو المؤسسة المالية المحافظة على سلامة حساب العميل ونظام الدفع الإلكتروني.

قسمت أعمال البحث إلى قسمين أساسيين: القسم الأول تناول الناحية القانونية لموضوع المعاملات الإلكترونية أي الإرشادات والقوانين النموذجية الأجنبية والعربية، والتشريعات الأجنبية والعربية بالإضافة إلى المراجع الفقهية المرتبطة، والقسم الثاني شمل الناحية التقنية لهذا الموضوع وخاصة فيما يتعلق بأنظمة التشفير (encryption systems) وفكها والمفاتيح العامة (Public Key) والمفاتيح الخاصة (Private Key)، بالإضافة إلى بعض أسماء مزودي خدمات التصديق في الدول الأوروبية.

القسم الأول: أبرز ما تناولته أعمال البحث في هذا القسم:

١) الوثائق الرسمية الأساسية الصادرة عن الأمم المتحدة والمجلس الأوروبي، المتعلقة بهذا المجال، ومنها:

- Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.

- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce").

- Model Law 56/80 on Electronic Signatures, adopted by the United Nations Commission on International Trade Law.

- UNCITRAL Legislative Guide on Secured Transactions, Supplement on security Rights in Intellectual Property, United Nations Commission on International Trade Law. Pre-release (15 July 2010).

- OECD Guidelines for Cryptography Policy, 27 March 1997.

- OECD Recommendation on Electronic Authentication, and OECD Guidance for Electronic Authentication.

- Resolution on the communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on ensuring security and trust in electronic telecommunication - towards a European framework for digital signatures and encryption (COM(97)0503 C4-0648/97).

- Commission recommendation 97/489/EC of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder.

- Commission Recommendation 87/598/EEC of 8 December 1987, concerning a European code of conduct relating to electronic payments .

- Commission Decision of 28 July 2010 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States.

٢) بالإضافة إلى ذلك تناولت أعمال البحث مختارات من تشريعات وطنية من دول أجنبية[1] مختلفة تناولت تنظيم المعاملات الإلكترونية، وبخاصة منها التشريعات الأميركية، الفرنسية، البلجيكية، السويسرية، البريطانية، الكندية، الأسترالية، بالإضافة إلى بعض التشريعات الخاصة من دول آسيا الوسطى.

٣) كما وقد تم الاسترشاد بالمراجع الفقهية العالمية الخاصة بالمعاملات الإلكترونية.

- قيمة مستخرجات التقنيات العلمية الحديثة ومدى حجيتها في الإثبات، أسامة أحمد شوقي المليجي، دراسة، مؤتمر معالجة المعلومات القانونية في القرن ٢١ وتحدياتها، بيروت، ٧-٢٠٠١/٢/٩.

- التنظيم القانوني لشبكة الإنترنت، الدكتور طوني عيسى، أطروحة دكتوراة، الجامعة اللبنانية، ٢٠٠٠.

- الإثبات الإلكتروني للقاضي وسيم شفيق حجار، بيروت ٢٠٠٧.

- الإثبات الإلكتروني في القانون اللبناني للقاضي سامي منصور، مجلة العدل، ٢٠٠١.

- الدليل الكتابي وحجية الكمبيوتر في الإثبات في المواد المدنية والتجارية ، بحث، مؤتمر القانون والكمبيوتر والإنترنت، ١-٢٠٠٠/٥/٣.

- La signature Electronique, Transactions et confiance sur Internet, par Arnaud-F. Fausse, Paris 2001.

- De L'Ecrit Electronique et des signatures qui s'y attachent, 14 Juin 2000.

- Le droit de la preuve est un Totem Moderne (Le commerce électronique), par Cyrille Charbonneau et Frédéric-Jérôme Pansier, Avril 2000.

- Hirst (M.): Computers and the English Law of Evidence, Law, Computers & Artificial Intelligence, 1992.

- Bensoussan (A.) Contributions théoriques au droit de la prevue dans le domaine informatique: Aspects techniques et solutions juridiques, Gaz.Pal., 1991,2.

- The Legal and Market Aspects of Electronic Signatures by the European Commission - DG Information, Society final version.
http://ec.europa.eu/information_society/eeurope/ 2005/all_about/security/electronic_sig_report.pdf

- Commission welcomes new legal framework to guarantee security of electronic signatures, Brussels, 30 November 1999.
http://ec.europa.eu/dg15en/media/sign/index.htm

- Digital Signature Guidelines Tutorial, American Bar Association.
http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html

- Cryptographie et signature Electronique, Aspects Juridiques; Alain Bensoussan, Yves le Roux, Hermes, 1999.

- How Encryption Works by Jeff Tyson published on. http://computer.howstuffworks.com/encryption1.htm

- Digital Signatures and European Laws, by Mirella Mazzeo, 26 Jan 2004.
http://www.symantec.com/connect/articles/digital-signatures-and-european-laws

- Cryptography for Network and Information Security.
http://technet.microsoft.com/en-us/library/cc962027.aspx

- Cryptography Policy, by Lance J. Hofjhan, Fam A. Ali, Steven L. HeAle+, Am Huybredtts, September 1994.
http://www.cspri.seas.gwu.edu/Mazz.%20Papers/p109-hoffman%20Crypto%20Policy%20CACM.pdf

- Data Encryption Standard (DES), Federal Information, Processing Standards Publication 46-2, 1993 December 30.

- Advanced Encryption Standard (AES), Federal Information, Processing Standards Publication 197, November 26, 2001.

- The National Strategy to Secure Cyberspace, the White House Washington- February 2003.

- Privacy and Encryption controls: A Crypto Trilogy (Bernstein, Junger & Karn), by Keith Aoki. This module has been revised to reflect the state of affairs as of August 24, 2000. The earlier 1999 version of this model is superceded

- The Codebreakers: The Story of Secret Writing (1973; rev. ed, 1996); by David Kahn
http://www.britannica.com/dday/article-7517

- Data Encryption for QUB Confidential Data, Security Policy User Guide1, Queen's University, Belfast.23 February 2009.
http://www.qub.ac.uk/directorates/InformationServices StaffComputing/ITServices/FileStoresecuritypolicies/word/Filetoupload,140675,en.doc

- Information Privacy in Cyberspace Transactions by Jerry Kang, April 1998
http://www.ntia.doc.gov/ntiahome/privacy/files/cprivacy.pdf

- Les enjeux de la cryptographie, Lionel Thoumyre, November 1998.
http://www.juriscom.net//espace2/crypto2.htm

٤) وقد تم الاسترشاد أيضاً بالدراسات التي أعدتها الإسكوا في هذا المجال وأهمها: ١- متابعة التطورات الحاصلة في التشريعات السيبيرانية في الأردن وسوريا ولبنان وفلسطين والعراق. ٢- وضع التشريعات السيبرانية في سلطنة عمان ، دولة الإمارات العربية المتحدة ، دولة قطر. ٣- وضع التشريعات السيبرانية في السعودية والكويت واليمن.

٥) كذلك تناولت أعمال البحث التشريعات ومشاريع القوانين التابعة للدول العربية الأعضاء في الإسكوا؛ إضافة إلى القرارات والقوانين النموذجية الصادرة عن جامعة الدول العربية والأنشطة والتجارب التي قامت بها ضمن هذا النطاق.

تجدر الإشارة من ناحية أخرى إلى أنه تم التركيز على تحليل التشريعات الوطنية العربية الخاصة بتنظيم المعاملات الإلكترونية؛ ومدى شمولية هذه التشريعات النقاط التي يجب أن يتناولها هذا الإرشاد.

وبالتالي سنعرض أهم مخرجات البحث لهذه الجهة.

أ- بالنسبة للتشريعات الوطنية العربية الخاصة بالمعاملات الإلكترونية والتواقيع الإلكترونية:

تبين أثناء أعمال البحث أن معظم دول الإسكوا، عملت على إصدار تشريعات خاصة وإقرار نظام للتعاملات الإلكترونية، بحيث تهدف هذه التشريعات إلى ضبط التعاملات والتوقيعات الإلكترونية، وتنظيمها وتوفير الإطار النظامي لها، وإضفاء الحجية عليها. حيث تتمّ أيضاً معاملة المستند الإلكتروني - متى توافرت فيه الشروط والمواصفات المطلوبة نظاماً - معاملة المستند الورقي المكتوب، لجهة ترتب الآثار النظامية عليه، وقبول حجيته في الإثبات وغير ذلك من الأمور النظامية والقانونية لقبول هذه المعاملات والاعتماد عليها كوسيلة جديدة من وسائل التعامل.

إن دول الإسكوا التي أصدرت تشريعات خاصة بالمعاملات الإلكترونية هي التالية:

١- الأردن:
قانون رقم الصادر في ٢٠٠١/١٢/٣١ بشأن المعاملات الإلكترونية.
http://www.lob.gov.jo/ui/laws/search_no.jsp?no=85&year=2001

٢- الإمارات العربية المتحدة:
قانون رقم (٢) صادر في ٢٠٠٢/٠٢/١٢ بشأن المعاملات والتجارة الإلكترونية.
http://www.theuaelaw.com/vb/showthread.php?t=1137

٣- البحرين:
مرسوم بقانون رقم ٢٨ الصادر بتاريخ ١٤ سبتمبر ٢٠٠٢ بشأن المعاملات الإلكترونية وتعديلاته.
http://www.moic.gov.bh/MoIC/Ar/Industry/ResourcesLaws/CommerceLaw/eLaw/

٤- سوريا:
قانون رقم ٤ الصادر في ٢٠٠٩/٠٢/٢٥ بشأن التوقيع الإلكتروني وخدمات الشبكة.
http://www.moct.gov.sy/moct/?q=ar/node/69

٥- السودان:
قانون المعاملات الإلكترونية لسنة ٢٠٠٧.
http://www.cbos.gov.sd/node/281

٦- سلطنة عمان:
قانون رقم ٦٩ لسنة ٢٠٠٨ بشأن المعاملات الإلكترونية.
http://www.ita.gov.om/ITAPortal_AR/Businesses/Businesses_Projects.aspx?NID=97

٧- قطر:
قانون المعاملات والتجارة الإلكترونية تاريخ ١٩ اغسطس ٢٠١٠.
http://www.ict.gov.qa/files/images/e-commerce_law_updated.pdf

٨- مصر:
قانون رقم ١٥ لسنة ٢٠٠٤ بشأن التوقيع الإلكتروني.

٩- السعودية:
مرسوم ملكي رقم ١٨ لسنة٢٠٠٧ خاص بنظام التعاملات الإلكترونية.
http://www.ncda.gov.sa/low21/7.pdf

١٠- اليمن:
قانون رقم ٤٠ لسنة ٢٠٠٦ بشأن انظمة الدفع والعمليات المالية والمصرفية الإلكترونية.
http://www.centralbank.gov.ye/ar/CBY.aspx?keyid=80&pid=74&lang=2&cattype=1

واقر مجلس الوزراء الكويتي مؤخراً "مشروع قانون المعاملات الإلكترونية" الذي تسري أحكامه على المعاملات الإلكترونية والدفع الإلكتروني والرسالة الإلكترونية والأنظمة المؤتمتة. وينص المشروع للمرة الأولى على أنه "لا يجوز إغفال الأثر القانوني للتوقيع الإلكتروني من حيث صحته وإمكان العمل به لمجرد وروده في شكل إلكتروني، ويكون للتوقيع الإلكتروني المحمي في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للتوقيع الكتابي المنصوص عليها في أحكام قانون الإثبات في المواد المدنية والتجارية، متى روعي في إنشائه وإتمامه الضوابط الفنية الواردة في هذا القانون ولائحته التنفيذية".

تجدر الإشارة إلى أن ثمة بلداناً عربية أخرى قد أطلقت ورشة إعداد مشاريع قوانين لإصدار قانون خاص بالمعاملات الإلكترونية، وهي: لبنان، وفلسطين[٢] التي قامت بإعداد مشروع قانون المبادلات والتجارة الإلكترونية الصادر عام ٢٠٠٣.

من ناحية أخرى، نفيد ضمن هذا المجال أن جامعة الدول العربية قد قامت بإصدار القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة[٣]، وقد تناول هذا القانون أحكاماً حول حجية الكتابة والمحرّرات والتواقيع الإلكترونية، والهيئة المختصّة، وجهة التوثيق الإلكتروني المنظمة لشهادات التوثيق الإلكتروني والجرائم المرتكبة في هذا المجال وعقوباتها. كما وأصدرت القانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية، الذي تناول أحكاماً حول رسالة البيانات، والعقود الإلكترونية، والدفع الإلكتروني، والعقوبات التي تفرض عند مخالفة هذه الأحكام بالإضافة إلى القانون الواجب تطبيقه والمحكمة المختصة.

ب - شمولية التشريعات الوطنية الخاصة

إزاء التطور والتغيير الكبير الحاصلين في مجال تقنيات المعلومات والتغييرات الحاصلة في أشكال المعاملات الإدارية والتجارية من خلال استعمال الوسائل الإلكترونية والشبكات والوسائط المعلوماتية، عملت جميع الدول العربية على تنظيم موضوع التعاملات الإلكترونية ضمن إطار تشريعي متكامل. فقام بعضها بإصدار تشريعات تشمل في آن المعاملات والتواقيع الإلكترونية بالإضافة إلى التجارة الإلكترونية، ولم تخصص لها تشريعات منفردة ومستقلة، باستثناء بعض النصوص القانونية الوطنية التي تراعي أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية كما هو الحال في اليمن؛ والقرارات الإدارية أو تعاميم المصرف المركزي فيما يتعلق بالتحاويل الإلكترونية، والعمليات المالية والمصرفية بالوسائل الإلكترونية والصراف الآلي وبطاقات الإئتمان والوفاء كما هو الحال في لبنان.

عالجت التشريعات الوطنية العربية ونظمت: الكتابة والسندات الإلكترونية والرسائل والسجلات وآثارها القانونية؛ التواقيع الإلكترونية، آلية إنشاء التوقيع الإلكتروني، قوته

الثبوتية وحمايته؛ واجبات ومسؤولية وسيط الشبكة الإلكترونية؛ واجبات ومسؤولية مزودي خدمات المصادقة الإلكترونية، مسؤولية صاحب الشهادة والجهات المختصة لتنظيم نشاطات تقديم خدمات التوقيع الإلكتروني، منح وإلغاء الترخيص الخاص بممارسة نشاطهم؛ إبرام العقود والتعبير عن الإيجاب والقبول وأثره القانوني عند إبداء النوايا؛ التحاويل الإلكترونية للأموال وأنظمة الدفع وشروطه والشيكات الإلكترونية وحجية الوفاء الإلكتروني ووسائله؛ والعقوبات التي تفرض عند مخالفة نظم المعلومات وارتكاب أعمال التزوير أو التحريف أو التعديل في السندات الإلكترونية، ومخالفة الأحكام الخاصة بمنظومة التوقيع الإلكتروني وصحته، الخ.

أصدرت مملكة البحرين المرسوم بقانون رقم ٢٨ لسنة ٢٠٠٢ الخاص بالمعاملات الإلكترونية، وهو قانون شامل إذ أنه يغطي معظم الجوانب المتعلقة بالمعاملات الإلكترونية، بحيث تطرق إلى كيفية إبرام العقود وصحة انعقادها ودور الوكلاء الإلكترونيين في إبرام العقود، الإسناد الإلكتروني وإثباته، السجلات الإلكترونية، الإقرار بتسلمها، وقت ومكان إرسال وتسلم السجلات الإلكترونية وقوتها الثبوتية، اعتماد مزودي خدمة الشهادات الوطنيين والخارجيين واجباتهم ومسؤولياتهم، بالإضافة إلى أحكام خاصة بمستندات نقل البضائع، وأحكام خاصة بتسجيل أسماء النطاق وتنظيم تسجيل واستعمال اسم النطاق (Domain Name)، بالإضافة إلى كيفية الطعن في صحة السجلات والتوقيعات الإلكترونية.

انفردت سلطنة عمان ضمن مرسومها السلطاني رقم ٢٠٠٨/٩٦ المتعلق بإصدار قانون المعاملات الإلكترونية بتخصيص فصل يتعلق بطرق حماية المعاملات الإلكترونية التي لم تتطرق إليها ولم تعالجها باقي الدول العربية، فنصت على أحكام تقضي باستخدام التشفير كوسيلة لحماية المعاملات الإلكترونية بهدف المحافظة على سرية المعلومات أو البيانات التي تحويها الرسالة الإلكترونية، وتحديد الطرق الخاصة بحماية نظم المعلومات أي اعتماد التشفير بطريق المفتاح العام، الجدران النارية (Fire Wall)، مرشحات المعلومات، البرامج المضادة للديدان (worm) والفيروسات (Viruses)، الخ.

كما قامت السعودية بإصدار ضوابط لتطبيق التعاملات الإلكترونية الحكومية من شأنها المحافظة على المعلومات والبيانات الحكومية، حيث تقوم كل جهة حكومية بإدارة وحفظ وتوثيق البيانات التابعة لها، وإتاحة البيانات المشتركة منها إلكترونياً للجهات الحكومية الأخرى المستفيدة لتأمين تكامل البيانات بين الأجهزة الحكومية وذلك ضمن الالتزام بمعايير محددة لحماية الخصوصية والمعلومات بالإضافة إلى معايير استرشادية تعدها الجهة المعنية.

نظمت إمارة دبي أيضاً بقانونها رقم ٢ لسنة ٢٠٠٢ الخاص بالمعاملات والتجارة الإلكترونية الاستخدام الحكومي للسجلات والتوقيعات الإلكترونية وقبول وإيداع المستندات والإصدار الإلكتروني للمستندات، وتطرقت في إحدى مواد القانون إلى التوقيع الإلكتروني المحمي دون أن تفرد له أحكاماً خاصة بحمايته عبر استعمال وسيلة التشفير.

أما اليمن فعملت على تضمين قانونها رقم (٤٠) لسنة ٢٠٠٦ ما يتعلق بأنظمة الدفع والعمليات المالية والمصرفية والإلكترونية، وهو ينظم بشكل مفصل أنظمة الدفع وتحويل الأموال إلكترونياً، والآثار المترتبة على كل من السجل والعقد والرسالة والتوقيع الإلكتروني، كما نظم تداول الوثائق والسجلات والرسائل الإلكترونية بإنشائها وإرسالها واستلامها، ونظم أيضاً إجراءات توثيق السجل والتوقيع الإلكتروني، وهو ما كان ضروريا لسد النقص في تنظيم هذه المسائل خصوصاً مع غياب التنظيم التشريعي الكامل لها.

لا بد من الإشارة إلى أنه، وبالرغم من أن جميع الدول العربية باستثناء أربع دول قد أصدرت قوانين خاصة بالمعاملات والتواقيع والتجارة الإلكترونية، إلا أنها لم تعالج بشكل تفصيلي جميع النقاط التي يجب أن تتضمنها هذه التشريعات. نقدم أمثلة على ذلك:

- لم تصدر الدول العربية أنظمة أو أحكاماً خاصة بوسائل حماية المستندات والمعاملات والتواقيع الإلكترونية وأنواعها وإجراءاتها مثال التشفير باستثناء سلطنة عمان وإمارة دبي. إلا أن هذه الأخيرة قد ذكرتها في مادة واحدة ولم تخصص لها فرعاً أو فصلاً، أي أنها لم تعالجها بشكل تفصيلي.

- لم تتطرق بعض الدول العربية ضمن تشريعاتها الخاصة بالمعاملات الإلكترونية إلى عمليات التحاويل والدفع الإلكتروني مثال: سلطنة عمان، السعودية، البحرين، وسوريا، وهذه العمليات تحتاج بلا شك إلى تنظيم قانوني لما تنطوي عليه من أهمية بالغة. إلا انه بالمقابل أصدرت اليمن نصاً خاصاً يراعي أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية؛ وأصدر لبنان عدداً من القرارات الإدارية أو تعاميم المصرف المركزي المتعلقة بالتحاويل الإلكترونية، والعمليات

المالية والمصرفية بالوسائل الإلكترونية والصراف الآلي وبطاقات الائتمان والوفاء.

القسم الثاني: تناولت أعمال البحث في هذا القسم بعض أنظمة حماية المعلومات، وبعض أنظمة التشفير المعتمدة، وبعض أسماء مزودي خدمات التصديق وذلك من أجل إتاحة المجال أمام المشترع العربي للاطلاع على هذه الوثائق ومساعدته في وضع التشريعات المناسبة آخذاً بعين الاعتبار المعطيات التقنية المطلوبة، وأبرزها:

١) بعض أنظمة حماية المعلومات:

- Guidelines on Firewalls and Firewall Policy.
http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

- Payment Application Data Security Standard.
https://www.pcisecuritystandards.org/documents/pa-dss_v2.pdf

- Methods, software programs, and systems for electronic information security.
http://www.freepatentsonline.com/7395436.html

- Secured electronic mail system and method.
http://www.freepatentsonline.com/y2002/0007453.html

- Creating, verifying, managing, and using original digital files.
http://www.freepatentsonline.com/y2002/0055942.html

٢) بعض أنظمة التشفير المعتمدة في العالم وأبرزها:

- DES-Data Encryption Standard.
http://www.itl.nist.gov/fipspubs/fip46-2.htm

- AES-Advanced Encryption Standard.
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

- RSA's security system.
http://ecommerce.hostip.info/pages/914/RSA-Data-Security.html

- BLOWFISH encryption algorithm.
http://www.schneier.com/blowfish.html

- IDEA International Data Encryption Algorithm.
http://www.quadibloc.com/crypto/co040302.htm

- SEAL encryption algorithm.
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_se.html#wp1027129

- RC4 encryption algorithm.
http://www.codeproject.com/KB/recipes/rc4csharp.aspx

- The CSS Decryption Algorithm.
http://www.cs.cmu.edu/~dst/DeCSS/Gallery/plain-english.html

- PHP – Simple Encryption and Decryption algorithm.
http://flax.ie/php-simple-encryption-and-decryption-algorithm/

- CAS Central Authentication Service project.
http://www.jasig.org/cas

٣) أسماء بعض مزودي شهادات التصديق:

- List of European Service Providers Issuing Qualified Certificates.
http://eu.adr.eu/html/en/adr/electronic_signatures/PDF1.pdf

- Global List of PCI DSS Validated Service Providers.
http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf

- Qualified Security Assessor (QSA) companies.
https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

- قائمة مزودي خدمات التصديق في السعودية:
http://www.internet.gov.sa/learn-the-web-ar/guides-ar/DSPs-ISPs-List

- المركز الوطني للتصديق الرقمي، وزارة الاتصالات وتقنية المعلومات في السعودية:
http://www.mcit.gov.sa/arabic/NationalCenter

- مزودو خدمات التصديق الإلكتروني في دولة الإمارات
http://www.tra.gov.ae/news100-A.php

٤) لائحة ببعض أسماء الشركات مزودي خدمات التشفير:

- http://searchmobilecomputing.bitpipe.com/data/olist?iStart=1&t=itmgmt_10_50_20_28_2

- Protectyon, established in Haarlem (the Netherlands). As a team of web designers, software developers and application engineers we have been fighting copyright infringement since day one, which gave us the idea to provide a new innovative service to fight online piracy.
http://www.protectyon.com/about.php

- Verisign company.
http://www.verisign.com/

هوامش

١- تراجع لائحة تشريعات الدول الأجنبية - ملحق رقم ٥ من التسليم الاول.

٢- راجع مشروع قانون المبادلات والتجارة الإلكترونية الفلسطيني المنشور على الموقع الالكتروني:
http://www.pita-palestine.org/PITA%20files/proposed%20e_commerce%20law.doc

٣- القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة، أعتمده مجلس وزراء العدل العرب بقرار رقم ١٧٧/د٢٤ - ٢٧/١١/٢٠٠٨

مقدمة إرشاد المعاملات الإلكترونية والتواقيع الإلكترونية

تعاظم حجم التعاملات الإلكترونية في ظل تطور التقنيات وتنامي استعمال الحاسوب والإنترنت وانتشار ثقافة المعلوماتية بين الجمهور.

عند بداية الثمانينيات من القرن العشرين بدأ استعمال الحاسوب من قبل القطاع الخاص، إلا أن استعماله في المعاملات اقتصر على إدخال البيانات واستخراجها وطباعة المستندات آلياً مما شكل نقلة نوعية عن الطباعة على الآلة الكاتبة أو عن حفظ الملفات ورقياً وبواسطة أنظمة أرشفة تقليدية.

أدى السماح للجمهور باستعمال شبكة الإنترنت في بدايات التسعينيات من القرن الماضي، إلى ظهور أنواع جديدة من إمكانيات الاتصال والتعامل والتعاقد. وقد أدّى بالتالي إلى إمكانية تبادل المعلومات في بداية الأمر ثم إلى تبادل الرسائل والمعاملات في وقت لاحق واستّعمل كوسيلة لتسليم بعض المنتجات ذات الطابع الإلكتروني، وهو ما أصبح يعرف بالمعاملات الإلكترونية. وهنا برزت إشكالية صحة وسلامة كلّ من المستند الإلكتروني غير المطبوع ورقياً والتوقيع. فنسخ التوقيع الخطي وإيراده إلكترونياً لا يحقق ذات القوة الثبوتية للتوقيع الخطي على ركيزة ورقية، ذلك أن حماية الصورة المنسوخة قد تتعرض للانتهاك.

يشكل المستند الورقي وسيلة حفظ وإثبات وحجة على من وقعه أو صاغه وله قوة ثبوتية شاملة نظراً لأنه يسمح لأي شخص كان، حتى ولو لم يكن يتمتع بمعرفة تقنية أو خبرة، باكتشاف أي تعديل يطرأ على المستند أو مضمونه. فإن مجرد النظر بالعين المجردة إلى أي مستند ورقي يمكّن الناظر من ملاحظة أي حشو أو إضافة أو تشطيب، أو قطع أو تمزيق أو محو، مما يفيد الناظر بأن المستند لم يعد بحالته السليمة ومما يفيد بأن هذه التغييرات من شأنها المساس بالقوة الثبوتية أو بصلاحية المستند الورقي لإنتاج الآثار القانونية الناجّة عنه وعن مضمونه لو كان بقي سليماً. لذا فإن القانون قد فرض التوقيع مجدداً فوق كل تمحية أو حشو وذلك لإضفاء المشروعية على مثل هذا التعديل ليعود المستند الورقي سليماً ومنتجاً لآثار القانونية.

من هنا يبرز الفرق بين المستند الورقي والمستند الإلكتروني، إذ إن المستند الإلكتروني لا يسمح عادة بفعل طبيعته الإلكترونية (أي أنه مؤلف من كتابة وفقاً للنظام الثنائي ٠١٠١٠٠١) باكتشاف أي تعديل أو تغيير فيه، لأن طبيعة حفظه بصورة إلكترو-مغناطيسية تسمح بتعديله بدون أن يتمكن من يعاينه من اكتشاف أي تعديل طرأ عليه منذ صياغته الأولى "الأساسية".

من هنا كان لا بد من وضع معايير لحماية المستند الإلكتروني مثل التشفير والصعوبات التقنية الأخرى التي تمنع الولوج إليه، وقد تم كذلك وضع برمجيات قادرة على كشف أي خرق أو تلاعب بسلامته. فضلاً عن ذلك، فإن إسناد المستند الإلكتروني إلى من صاغه هو أمرٌ لا بد من التأكد منه. من هنا كانت الحاجة إلى أن يجري توقيع المستند الإلكتروني بطريقة تلائم طبيعته غير الملموسة. يُعرف التوقيع عادةً بأنه إشارة أو رسم أو كتابة بخط يد شخص ما، تعبر عن هوية ومصدر ونية وموافقة صاحب التوقيع على مضمون ما وقعه. يتمتع التوقيع بقوة ثبوتية قانونية نظراً لأنه صادر عن شخص طبيعي معين، ويعتبر التوقيع إقراراً من الموقع على مضمون ما تم توقيعه، وهو الوسيلة القانونية المثلى لنسبة مستند مكتوب وموقّع إلى شخص الموقِع.

لذا كان لا بد من إيجاد بديل إلكتروني للتوقيع الخطي اليدوي. وهنا نشأ التوقيع الإلكتروني الذي يعرّف بأنه بيانات بشكل إلكتروني متصلة أو مرتبطة منطقياً ببيانات إلكترونية أخرى، وهي تستعمل كوسيلة لتأكيد الموثوقية.

يتمتع التوقيع الإلكتروني بعدد من الإجراءات التقنية التي تسمح باعتماده والتأكد من صحته ومن صدوره عن الشخص المعني به، وتعرف هذه الوسائل بآليات إنشاء التوقيع الإلكتروني والتحقق من صحته.

ومع تطور عالم المعلوماتية واعتماد الحاسوب من قبل القطاع الخاص، تطورت الأساليب التجارية واتجهت أكثر نحو استعمال الإنترنت كوسيلة اتصال وكوسيلة تبادل للأموال لا سيما عندما أصبحت المصارف تقبل الحوالات النقدية الإلكترونية. تساهم المعاملات الإلكترونية[1] في النمو الاقتصادي الوطني، مما يعكس اهتمام مختلف الدول بتحفيزها وتنظيمها. إلا أن هذه المعاملات تثير إشكاليات جديدة يعجز النظام القانوني السائد حالياً[2] عن إيجاد حلول وافية لها في ظل قوانين لم تلحظ الطابع الإلكتروني كركيزة يمكن استعمالها مكان

الركيزة الكتابية أو الورقية، ومن هذه الإشكاليات عدم الاعتراف بالقوة الثبوتية للسندات الإلكترونية وعدم اعتماد وقبول التواقيع الإلكترونية وعدم الركون إلى موثوقيتها. يُضاف إلى ذلك وجود تفاوت واضح في المعرفة التقنية بين الممتهن والمتعامل العادي، مما قد يُضاعف أخطار التلاعب في المعاملات الإلكترونية، وممّا قد يدفع المتعاملين إلى الإحجام عن التعاملات الإلكترونية، الأمر الذي سيؤدي إلى الإضرار بالاقتصاد الوطني. وبالتالي كان لا بد من وضع إطار قانوني لتنظيم المعاملات الإلكترونية ومسائل الإثبات الإلكتروني، ولاسيما التواقيع الإلكترونية وموثوقيتها، وذلك لتدعيم الثقة بالتقنيات الجديدة وتحفيز قبول الجمهور لها وإعطائها نفس القوة الثبوتية التي تُعطى للتعاملات الجارية بالأساليب التقليدية أي الخطية.

كان لا بد إذاً من توفير الحماية القانونية اللازمة للسند الإلكتروني كما هي الحال للسند العادي أي الورقي. إذ أن إمكانية ضبط وكشف أي تعديل أو تحريف يجري على السند الخطي، هي سهلة وواضحة للعين المجردة. فالشخص المعني يستطيع بسهولة التمييز بين السند الأصلي والسند المحرّف. لذا كان لا بد عند إضافة أي تعديل أو حشو على المستند الخطي، من أن يوقع الفرقاء عليه لإعطائه المصداقية والقوة الثبوتية. إلا أن هذا الأمر يستحيل تطبيقه في السند الإلكتروني إذ ليس هناك من إمكانية تسمح بذلك في إحدى مكونات الحاسوب وذاكرته. لهذا السبب، اقتضى وجود أنظمة توفر الحماية القانونية للسند الإلكتروني ومنع أي وصول غير مشروع أو تعدي على سريته وكشف ما قد يصيبه من تعديلات بصورة غير مشروعة. من هنا بروز أهمية تطبيق وسائل التشفير[٣] وتطوير تقنياته وأنظمته[٤] لأجل توفير سرية المعلومات وصحتها، بالإضافة إلى تطوير أنظمة تسمح برصد وكشف ما إذا كان قد حصل أي تعديل غير مشروع على السند الإلكتروني. وبرز اتجاهان في مجال التشفير، فالاتجاه الأول اكتفى باللجوء إلى تطبيق وسائل التشفير في التشريع العام دون التدخل في أنظمته الخاصة لأنها قابلة التعديل، أما الاتجاه الثاني فقد حدد ضوابط تقنيات التشفير في التشريع الخاص على أن يتم تعديلها عند تغيير هذه التقنيات.

ويبرز الطابع الدولي للمسألة من خلال تخطي المعاملات الإلكترونية الحدود الجغرافية للدول، حيث أصبحت تتم على نطاق واسع كالمعاملات التي تحصل من بلد إلى بلد أو التي تتضمن عنصراً أجنبياً، بالرغم من عدم انسجام التشريعات الوطنية في هذا المجال وفي بعض الأحيان تناقضها. كما يقتضي هذا الطابع الدولي للمسألة تأمين تناسق منتجات التواقيع الإلكترونية بين مختلف الدول، ولاسيما توحيد الشروط الفنية التي تخضع لها، مما يساهم في تأمين حرية تبادلها بين الدول دون أية عوائق، الأمر الذي يدعو أيضاً إلى وضع إطار قانوني للمعاملات الإلكترونية يأخذ بطابعها الدولي ويسعى إلى تأمين الانسجام بينها.

لقد ظهر جهد واضح على الصعيد الدولي في مجال إقرار الإرشادات والتوجيهات والقوانين والقواعد المنظّمة في هذا المجال. فلقد أصدر البرلمان الأوروبي[٥] في ١٩٩٩/١٢/١٣ إرشاداً يتعلق بالتواقيع الإلكترونية. كما اعتمدت لجنة القانون التجاري الدولي لدى الأمم المتحدة في العام ٢٠٠١ قانون الأونسيترال النموذجي حول التواقيع الإلكترونية. وعلى الصعيد الوطني، لقد حدّثت الكيبيك-كندا منذ العام ١٩٩٣ قانونها من أجل الاعتراف بالقوة الثبوتية للتسجيلات المعلوماتية. كما أقرت بريطانيا في العام ١٩٩٥ قانوناً يعترف بالسند الإلكتروني، وأتبعته عام ٢٠٠٠ بقانون حول الاتصالات الإلكترونية يتضمن التوقيع الإلكتروني والتخزين الإلكتروني للمعلومات. وأصدر الرئيس الأميركي في ٢٠٠٠/٦/٣٠ قانوناً فديرالياً حول التوقيع الإلكتروني في مجال التجارة الداخلية والدولية. وأقر المشرع الفرنسي بتاريخ ٢٠٠٠/٣/١٣ القانون رقم ٢٠٠٠/٢٣٠ حول تكييف الإثبات مع تقنيات المعلوماتية وحول تعلّقه بالتواقيع الإلكترونية.

كما وظهرت معايير وبروتوكولات عديدة تهدف إلى تنظيم المعاملات الإلكترونية وتوفير الحماية والأمان للجهات الراغبة بالتواصل عبر شبكات الانترنيت وأهمها بروتوكولات التشفير[٦] وبروتوكولات التصديق[٧]. قامت بعض الدول العربية في منطقة الإسكوا بوضع تشريعات تتعلق بالمعاملات والتواقيع الإلكترونية، ومنها من وضع أيضاً لوائح تنظيمية لهذه القوانين. إلا أنه وعلى رغم مرور بضع سنوات على تلك التشريعات، ما زالت الاجتهادات المرتبطة بتلك التشريعات قليلة ولم تؤدِ بعد أي دور فعال في سبيل تطوير هذه القوانين.

وقد تم الاسترشاد بالإرشاد الأوروبي الصادر عام ١٩٩٩ المتعلق بالتواقيع الإلكترونية وبقانون الأونسيترال النموذجي حول التواقيع الإلكترونية وبالقوانين الوطنية المختلفة، في إعداد نصوص الإرشاد الحالي الموجه إلى الدول العربية حول المعاملات الإلكترونية والتواقيع الإلكترونية والإثبات الإلكتروني.

لقد تم تقسيم القانون الاسترشادي المُقترح على خمسة أبواب تتناول مختلف جوانب المعاملات الإلكترونية والتواقيع الإلكترونية والإثبات الإلكتروني. وهذه الأبواب هي:

الباب الأول: أحكام عامة.
الباب الثاني: السندات والتواقيع الإلكترونية.
الباب الثالث: مسؤوليات مزود خدمات المصادقة الإلكترونية وصاحب الشهادة والطرف المعوّل/المعتمد
الباب الرابع: الاعتراف القانوني بشهادات المصادقة الإلكترونية الأجنبية.
الباب الخامس: العمليات المصرفية.

يتضمن **الباب الأول** المعنون "أحكام عامة" تحديداً لنطاق تطبيق القانون وتعاريف للمصطلحات الواردة في القانون وعرضاً للمبادئ الخاصة بالأسواق الداخلية التي يطبق عليها القانون. تحدّد المادة الأولى منه هدف القانون. فهو يرمي إلى تسهيل استخدام التواقيع الإلكترونية والاعتراف القانوني بها. وإلى حسن سير المعاملات من خلال وضع إطار قانوني للتواقيع الإلكترونية وبعض خدمات المصادقة. إلا أن الإرشاد لا يغطي الجوانب المتعلقة بإبرام وبصحة العقود أو غيرها من الموجبات القانونية عندما يكون هناك متطلبات شكلية بموجب القوانين الوطنية. ولا يمس هذا الإرشاد القواعد والقيود التي تنظم استخدام المستندات الواردة في القوانين الوطنية. فالقانون الحالي لا يسعى إلى تعديل القواعد القانونية التقليدية المختصة بالعقود والمستندات. بل إلى إدخال السندات والتواقيع الإلكترونية إلى النظام القانوني وتأمين الاعتراف بها. أما المادة ٢ من القانون. فتتضمن تعاريف لمختلف المصطلحات الواردة فيه باعتبار أن هذه المصطلحات هي إما تقنية معقدة. تتطلب بياناً لشروطها ومواصفاتها. وإما قانونية لها معانٍ خاصة يقتضي توضيحها. فالسند الإلكتروني هو القيدً أو العقد أو المراسلة التي تنشأ أو ترسل أو تسجل أو تسلم أو تحفظ بوسائل إلكترونية أو على وسيط إلكتروني ويمكن استخراجها بشكل مفهوم. والتوقيع هو علامة مميزة تسمح بتحديد هوية الشخص الموقع وتعبر عن رضاه والتزامه بمضمون السند الموقَع. أما التوقيع الإلكتروني[٨] فهو بيانات بشكل إلكتروني متصلة أو مرتبطة منطقياً ببيانات إلكترونية أخرى. وهي تخدم كوسيلة لتأكيد الموثوقية. إن وظيفة التوقيع الإلكتروني هي. كما الحال في التوقيع اليدوي. التعريف عن هوية صاحب التوقيع وتأكيد موافقته على محتوى السند الموقّع. إلا أن شكل وآليات وضع التوقيع الإلكتروني والتحقق منه تختلف. وقد ميّز كل من التوجيه الأوروبي[٩] وقانون الأونيسترال حول التواقيع الإلكترونية بين التوقيع الإلكتروني العادي والتوقيع الإلكتروني المتقدم. إذ أن الأمر يعود إلى التقنية المستعملة لضمان سلامة التوقيع وصدوره عن الشخص الموقع.

والتوقيع الإلكتروني المتقدم هو التوقيع الرقمي المستند إلى التشفير[١٠] عبر مفتاح غير متماثل.

لا يمكن فهم التواقيع الإلكترونية دون التطرق إلى التشفير. إذ أن التوقيع بالمفاتيح العمومية والخصوصية يرتكز على وسائل التشفير؛ فالتواقيع الإلكترونية تشكل إحدى تطبيقات التشفير[١١]. التوقيع الإلكتروني يسمح بالتأكد من هوية الموقع ومن صحة المعلومات. بينما يستخدم التشفير لضمان سرية المعلومات والاتصالات. بعد توقيع السند الإلكتروني. يقتضي نقله إلى الشخص المقصود بطريقة آمنة. عبر تحويله إلى شكل غير مفهوم إلا من قبل هذا الأخير. وبالتالي فان التوقيع الإلكتروني المتقدم هو التوقيع الذي يلبي متطلبات إضافية مجتمعة تعزز من موثوقيته: منها أن يكون مرتبطاً فقط بالموقّع. وأن يسمح بتحديد الموقّع. وأن يُنشأ بوسائل تكون تحت رقابة الموقّع الحصرية. وتكون مرتبطة بالبيانات المُوقّعة ارتباطاً يجعل كل تعديل لاحق في البيانات الموقعة قابلاً للاكتشاف. وبالتالي. وبالنظر لهذه المتطلبات. يُعرف التوقيع الإلكتروني المتقدم من قرينة الموثوقية بالمقارنة مع التوقيع الإلكتروني العادي الذي يجب إثبات موثوقيته من قبل من يتمسك به. الموقّع هو كل شخص يحوز آلية لإنشاء توقيع ويتصرف إما لحسابه الخاص أو لحساب شخص طبيعي أو معنوي يمثّله. أما الطرف المعوّل أي الطرف المعتمد فهو كل شخص يجوز أن يتصرف استناداً إلى شهادة مصادقة إلكترونية أو إلى توقيع إلكتروني. الطرف المعول/المعتمد قد يكون مُستقبل الرسالة الإلكترونية الموقّعة أو حتى الأشخاص الثالثين الذين يستندون على التزام الموقع بفعل توقيعه الإلكتروني وذلك في تصرفاتهم القانونية.

إن البيانات اللازمة لإنشاء توقيع إلكتروني هي بيانات فريدة. مثل رموز أو مفاتيح تشفير خاصة[١٢]. يستخدمها الموقّع لإنشاء توقيع إلكتروني[١٣]. ويقتضي الانتباه إلى عمليات حفظ هذه البيانات أو نسخها باعتبار أنها تعرض هذه البيانات لخطر الاختراق من قبل الغير. أما الآلية لإنشاء توقيع إلكتروني. فهي برنامج معلوماتي أو تجهيزات معلوماتية معدة لتضع موضع التطبيق البيانات اللازمة لإنشاء توقيع إلكتروني. يقتضي التفريق بين الآلية العادية لإنشاء التواقيع الإلكترونية والآلية الآمنة لإنشاء التواقيع إلكترونية التي يجب أن تلبي متطلبات إضافية. تخولها بالتالي. خلافاً لتلك العادية. الاستفادة من قرينة الموثوقية. والمتطلبات الإضافية هي الوسائل التقنية والإجراءات الملائمة التي تضمن عدم مصادفة بيانات إنشاء التوقيع إلكتروني إلا مرة واحدة وكذلك سريتها. وتضمن عدم إيجاد بيانات إنشاء التوقيع بالاستنتاج

وحمايته من التزوير والتقليد[14]، وحماية بيانات إنشاء التوقيع من أي استخدام من قبل الغير، وعدم تعديل آلية التوقيع الآمنة للبيانات الموقعة. أما البيانات اللازمة للتحقق من التوقيع الإلكتروني، فهي بيانات، مثل رموز أو مفاتيح تشفير عامة[15]، تستخدم للتحقق من توقيع إلكتروني. وتُعرّف الآلية للتحقق من توقيع إلكتروني[16] بأنها برنامج أو تجهيزات معلوماتية معدة من أجل وضع بيانات التحقق من التوقيع الإلكتروني موضع التطبيق. يورد القانون في مادته الثانية عند تعريف آلية التحقق من توقيع إلكتروني قواعد موجهة لضمان فعالية هذه العملية، ولاسيما التأكد من أن البيانات المُستخدمة من أجل التحقق من التوقيع تُطابِق البيانات المعروضة بوجه المُتحقِّق المُتعامل الآخر، وأنه يمكن التحقق من التوقيع بطريقة أكيدة، وأن نتيجة التحقق تُعرض بطريقة صحيحة، وأن المُتحقِّق المُتعامل الآخر يستطيع بشكل أكيد، عند الاقتضاء، تحديد مضمون البيانات الموقّعة، وأنه يمكن التحقق من مصداقية الشهادة وصحتها، التي تكون لازمة للتحقق من التوقيع الإلكتروني، وأنه تعرض بشكل صحيح نتيجة عملية التحقق من التوقيع الإلكتروني وهوية الموقّع، وأنه يذكر بشكل واضح أنه تم استعمال اسم مستعار، وأن كل تعديل له تأثير على الأمان قابل للاكتشاف. إن ذكر اسم مستعار في شهادة المصادقة لا يعفي مزود خدمات المصادقة من الاستحصال على الهوية الحقيقية لتقديمها للسلطات عند الحاجة.

أما شهادة المصادقة الإلكترونية[17]، فهي شهادة إلكترونية تربط بين بيانات التحقق من التوقيع الإلكتروني وشخص معين وتؤكد هوية هذا الشخص. فلكل شخص نوعان من البيانات: بيانات لإنشاء التوقيع وبيانات للتحقق من هذا التوقيع. يستعمل المُوقّع بيانات إنشاء التوقيع للتوقيع، وتكون هذه البيانات محمية وتحت سلطة المُوقّع الحصرية مخافة أن يستعملها الغير للتوقيع عن المُوقّع. أما بيانات التحقق من التوقيع فهي متاحة لكل شخص ليستعملها للتحقق من صحة توقيع المُوقّع. إن بيانات الإنشاء وبيانات التحقق تكون مترابطة، إلا أنه لا يمكن استنتاج إحداها من الأخرى. يتدخل شخص ثالث[18] مستقل وحيادي ومُفترض أنه موثوق للتعريف عن المُوقّع وللمصادقة على كون بيانات معينة للتحقق من التوقيع تعود لهذا المُوقّع، وتكون شهادة المصادقة الإلكترونية موصوفة عندما تلبي بعض الشروط لجهة مشتملاتها ولجهة صدورها عن مزود خدمات مصادقة إلكترونية يلبي بدوره شروطاً خاصة. تستفيد شهادة المصادقة الإلكترونية الموصوفة بدورها من قرينة الموثوقية. يجب أن تشتمل الشهادة الموصوفة على: ذكر بأنها شهادة موصوفة، تحديد مزود خدمات المصادقة الإلكترونية والبلد الذي يقيم فيه، اسم الموقّع، صفة خاصة للموقّع، بيانات التحقق من التوقيع الإلكتروني، تحديد بداية مدة صلاحية الشهادة وانتهائها، رقم الشهادة، التوقيع الإلكتروني المتقدم لمزود خدمات المصادقة الإلكترونية، حدود استخدام الشهادة، القيمة القصوى للمعاملات التي يمكن استخدام الشهادة فيها. أما الشروط الإضافية المطلوبة لمزود خدمات المصادقة الإلكترونية الصادرة عنه شهادة المصادقة الموصوفة، فهي: تقديم الإثبات على موثوقيته، تقيده بالقواعد القانونية الموضوعة لحماية البيانات ذات الطابع الشخصي، تأمين خدمة سريعة وأكيدة لدليل للشهادات وخدمة أكيدة وآنية لإلغاء الشهادات، إتاحة المجال لتحديد تاريخ ووقت إصدار الشهادة وإلغائها بشكل دقيق، التحقق بوسائل ملائمة ومتوافقة مع القوانين الوطنية من هوية ومن الصفات الخاصة للشخص الذي صدرت له الشهادة، استخدام عناصر بشرية كفوءة ومتخصصة، تطبيق إجراءات وطرق إدارية منطبقة على المعايير المتعارف عليها، استخدام أنظمة ومنتجات موثوق بها، اتخاذ تدابير ضد تزوير وتقليد الشهادات، توفير موارد مالية كافية للعمل، تسجيل جميع المعلومات الملائمة المتعلقة بالشهادة الموصوفة خلال المدة المفيدة، عدم حفظ وعدم نسخ بيانات إنشاء التوقيع الإلكتروني، التقيد بموجب إعلام المتعاملين معه، استخدام أنظمة موثوق بها من أجل حفظ الشهادات في شكل قابل للتحقق منه وفق شروط معنية.

أما مزود خدمات مصادقة إلكترونية، فهو كل هيئة أو شخص طبيعي أو معنوي يسلّم شهادات إلكترونية أو يقدم خدمات إلكترونية أخرى مرتبطة بالتواقيع الإلكترونية. يُعرّف منتوج توقيع إلكتروني بأنه كل منتوج تجهيزات أو برامج أو عنصر خاص من هذا المنتوج، معدّة للاستخدام من قبل مزود خدمات مصادقة إلكترونية من أجل تقديم خدمات التواقيع الإلكترونية، أو معدّة للاستخدام من أجل إنشاء التواقيع الإلكترونية أو التحقق منها. يُنشىء القانون الحالي نظاماً للاعتماد الاختياري لمزودي خدمات المصادقة الإلكترونية في حال تلبيتهم الشروط القانونية المطلوبة، وذلك للتشجيع على تعزيز موثوقية خدمات المصادقة المقدمة. لكن هذا النظام لا يمنع مزودي خدمات المصادقة غير المُعتمدين من العمل، بل يترك تقدير موثوقية الشهادات الصادرة عنهم وفق كل حالة للإثباتات المقدّمة. ويُعرّف الاعتماد الاختياري بأنه كل ترخيص يحدد الحقوق والموجبات الخاصة بتقديم خدمات المصادقة الإلكترونية، يُعطى، بناءً لطلب مزود خدمات المصادقة الإلكترونية المعني، من قبل هيئة عامة أو خاصة مكلفة بوضع هذه الحقوق والموجبات وبمراقبة احترامها. وتستكمل المادة ٢ التعاريف الواردة في القانون

بتعريف المصطلحات الخاصة بالعمليات المصرفية. فأمر الدفع الإلكتروني أو التحويل الإلكتروني للأموال النقدية هو الأمر الذي ينظم كلياً أو جزئياً بوسيلة إلكترونية، ويفوض بموجبه العميل مصرفاً أو مؤسسة مالية، بإجراء دفع إلكتروني أو تحويل إلكتروني للأموال النقدية أو إتمام قيد دائن أو مدين على حسابه. أما بطاقة الدفع أو السحب المصرفية فهي أداة صادرة عن مصرف أو عن مؤسسة مالية، وهي تتيح لصاحبها سحب الأموال وتحويلها، أو سحبها فقط. والنقود الإلكترونية تتكون من وحدات تسمى وحدات نقد إلكتروني يمكن حفظها على دعامة إلكترونية لمدة محددة، وتصدر مقابل نقد تتم مبادلته فوراً، بنفس القيمة ونفس العملة، وتتيح للغير دون المصدر إتمام عمليات دفع. والشيك الإلكتروني هو الشيك الذي يتم إنشاؤه والتوقيع عليه وتداوله إلكترونياً.

أما المادة ٣ من القانون، فهي تعطي لكل دولة عضو الحق بتطبيق تشريعاتها الوطنية، التي تقرها وفقاً لهذا الإرشاد، على مزودي خدمات المصادقة الإلكترونية العاملين على أراضيها وعلى الخدمات التي يقدمونها. كما تسمح هذه المادة بتداول منتجات التواقيع الإلكترونية المنطبقة على هذا الإرشاد بكل حرية في الأسواق الداخلية. والهدف هو تشجيع المعاملات الإلكترونية من خلال حرية تداول منتجات التواقيع الإلكترونية.

أما **الباب الثاني** المعنون "السندات والتواقيع الإلكترونية"، فإنه يتناول بالتفصيل السندات والتواقيع الإلكترونية. فالمادة ٤ من القانون تنظّم مسألة مدى انطباق الآليات الآمنة لإنشاء التواقيع الإلكترونية على الشروط المحددة لها في هذا القانون، وتُعطي صلاحية التحقق من ذلك لأجهزة عامة أو خاصة، وتكون نتيجة هذا التحقق مُعترفاً بها من قبل جميع الدول الأعضاء. فآليات إنشاء التواقيع الإلكترونية تشكل الضمانة التقنية لموثوقية التواقيع، وينبغي التحقق منها من قبل جهاز متخصص وموثوق. تجيز المادة ٥ فرض متطلبات إضافية لاستخدام التواقيع الإلكترونية في القطاع العام، على أن تكون موضوعية وشفافة ومتناسبة وغير مميِّزة. وهذه المتطلبات الإضافية مبررة بالنظر للثقة المُفترضة في صحة التعاملات العامة الناجمة عن تدخل طرف رسمي محايد مكلف بمهمة خدمة عامة، ولا يجب تقويض هذه الثقة من خلال تواقيع إلكترونية معرّضة ولو بشكل بسيط للتلاعب.

أما المادة ٥ من القانون، فهي تعرّف الكتابة وتضع الشروط القانونية للاعتراف بالكتابة الإلكترونية وبقوتها الثبوتية. وهذه الشروط تختصر بتحديد الشخص صاحب الكتابة وبإنشاء الكتابة وحفظها في ظروف تضمن سلامتها. إنّ الكتابة على دعامة إلكترونية تتمتع بنفس القوة الثبوتية للكتابة على دعامة ورقية. فمفهوم الكتابة هو واحد، أنّه تدوين سلسلة حروف أو أرقام أو أشكال أو أي رموز لها معنى مفهوم، أياً كانت الدعامة المستعملة ووسائل نقل المعلومات. ويقتضي التفريق بين الدعامة أو الركيزة التي توضع عليها الكتابة، والمختلفة بين ورقية أو إلكترونية، والكتابة بحد ذاتها. وتزيل المادة ٥ الالتباس الحاصل بالخلط بين الكتابة ودعامتها.

تشرّع المادة ٦ من القانون تنظيم السندات الإلكترونية العادية وكذلك الرسمية، إلا أنها تعطي الدول الخيار بحظر السندات الرسمية الإلكترونية أو بعض الفئات منها أو وضع متطلبات إضافية بخصوصها، وذلك تبعاً للاعتبارات التي جرى ذكرها أعلاه في سياق شرح المواد السابقة.

كما تتعرض المادة ٦ في فقرتها الثانية لإشكالية تعدّد النسخ في السندات الإلكترونية، إذ تختلط النسخة بالأصل في حالة السند الإلكتروني. فالنسخة هي تكرار تام للأصل، وهي مطابقة كلياً له، وقد يستحيل التمييز بينهما. لذلك، تُعتبر قاعدة تعدد النسخ الأصلية، المعمول بها بالنسبة للعقود المتبادلة المنظمة بشكل سندات عادية، مُستوفاة عندما تُنظّم وتُحفظ السندات العادية الإلكترونية وفق شروط الموثوقية المنصوص عليها في هذا الإرشاد وعندما تسمح الآليات لكل طرف بالحصول على نسخ عن السندات أو بالوصول إليها.

تقر المادة ٧ من القانون الآثار القانونية للتواقيع الإلكترونية، فهي، إذا كانت موثوقة، معادلة للتوقيع اليدوي. وتكون في جميع الحالات مقبولة أمام القضاء كوسيلة إثبات، إلا أن موثوقيتها تختلف باختلاف الوسائل التي اعتمدت لإنشائها. ويعود للمحكمة تقدير موثوقيتها من خلال الاستعانة بالخبرة الفنية. ويمكن لأشخاص يستعملون نظاماً مغلقاً لتبادل المعلومات أن يبرموا اتفاقات خطية خاصة حول الآثار القانونية لجهة الإثبات للتواقيع الإلكترونية وفق ما يرتأونه، لكن ضمن هذا النظام. وتضع المادة ٨ الشروط الأساسية للتوقيع الإلكتروني[١٩]، فهو يستلزم استخدام وسائل أو إجراءات موثوق بها من شأنها تأمين التعريف بصاحب التوقيع وتأكيد الصلة بين التوقيع والسند الذي يتعلق به. وتعطي المادة ٨ التواقيع الإلكترونية المتقدمة، والمُسندة إلى شهادات موصوفة والمُنشأة بواسطة آلية آمنة لإنشاء التواقيع موثوقية مفترضة، تُعفي من يتمسك بها من عبء

إثبات موثوقيتها. ويجب على الخصم هدم هذه القرينة بإثبات عدم الموثوقية.

تتناول المادة ٨ من القانون موضوع تزوير السندات الإلكترونية. فتنص على أنه في حال أنكر الخصم السند الإلكتروني أو التوقيع الإلكتروني أو ادعى تزويرهما، يتحقق القاضي من توفر شروط الموثوقية المنصوص عليها في هذا الإرشاد. ويمكن للقاضي الاستعانة بالخبرة الفنية من أجل التحقق من توفر هذه الشروط. يستفيد التوقيع الإلكتروني المتقدم من قرينة الموثوقية، إلا أنه يعود للقاضي، في ضوء العناصر التي تتوفر له، تقرير زوال هذه القرينة. فالتحقق من وجود تزوير يتم من خلال التثبت من توفر شروط الموثوقية المنصوص عليها في هذا القانون، والتي تضفي موثوقية مفترضة على التوقيع الإلكتروني، وكذلك من خلال التقنيات المستعملة التي يتم فحصها من قبل خبير فني متخصص.

أما المادة ٩ من القانون، فتعالج مسألة حفظ السندات الإلكترونية والشروط المطلوبة لصحة عملية الحفظ وتلافي أي تلاعب في الحفظ. فعملية الحفظ هي صحيحة عندما يتم التأكد من سلامة المعلومات واكتمالها منذ وقت بدء إنشاء هذه المعلومات لحين حفظها بالشكل الإلكتروني. لا تشكل التعديلات والمستجدات على المعلومات مساساً بسلامتها إذا تم توثيقها وفق الأصول القانونية. كذلك يُشترط لصحة عملية الحفظ أن تتم بشكلٍ يسمح بالرجوع إلى المعلومات لاحقاً وعرضها بشكل مفهوم، وأنه قد تم حفظ البيانات التقنية التي تبين منشأ المعلومات ومصدرها والجهة المرسلة إليها وتاريخ إرسالها ووقته وكذلك استلامها.

تتناول المادة ١٠ من القانون مسألة الآثار الإلكترونية والوثيقة الورقية المطبوعة عن السند الإلكتروني. فهي تعتبر الآثار الإلكترونية الصادرة عن شخص ما بمثابة بدء بينة خطية بوجه الشخص المذكور، وتعتبر الوثيقة الورقية المطبوعة عن السند الإلكتروني كصورة السند الورقي. وتتمتّع الآثار الإلكترونية بأهمية خاصة في مسائل الإثبات الإلكتروني، فكثيراً ما يشغّل المتعامل الحاسوب ويعمل على بعض الأنظمة المعلوماتية، ولكن دون التعبير صراحةً عن مراده بكتابة أو رسالة واضحة، بل يترك آثاراً لدخوله بعض البرامج أو لاستخدامها. وهذه الآثار قد تشكل دليلاً ولو غير كامل ضده.

بالانتقال إلى **الباب الثالث** المعنون "مسؤوليات مزود خدمات المصادقة الإلكترونية وصاحب الشهادة والطرف المعول/المعتمد"، يتبيّن أنه ينظم مسؤولية كل من مزود خدمات المصادقة الإلكترونية وصاحب شهادة المصادقة والطرف المعول/المعتمد. فالمادة ١١ تضع القواعد الخاصة بمزودي خدمات المصادقة الإلكترونية، الذين لا يخضعون في المبدأ لأي ترخيص لممارسة نشاطهم، إلا أنه من الممكن إنشاء أنظمة اختيارية للاعتماد لرفع مستوى خدمات المصادقة الإلكترونية المقدمة، على أن تكون جميع المعايير المتعلقة بهذه الأنظمة موضوعية وشفافة ومتناسبة وغير مميِّزة، وعلى أن يخضع مزوّدو خدمات المصادقة المعتمدون لنظام ملائم للمراقبة. لا يعني نظام الاعتماد الاختياري بالطبع حظر مزودي خدمات المصادقة غير المُعتمدين، بل يبقى هؤلاء مجبرين على تقديم الإثباتات على موثوقية وسائلهم وموثوقية شهادات المصادقة الصادرة عنهم.

تحدد المادة ١٢ من القانون مسؤوليات مزود خدمات المصادقة الإلكترونية الذي يصدر شهادة مصادقة موصوفة باعتبار أنها تتمتع بقرينة الموثوقية. فمزود خدمات المصادقة مسؤول في هذه الحالة عن الضرر الواقع على كل شخص طبيعي أو معنوي، يثق بشكل معقول بهذه الشهادة في ما خص صحة جميع المعلومات الواردة فيها وكفايتها. وهو مسؤول عن تكامل بيانات إنشاء التوقيع الإلكتروني وبيانات التحقق منه، إلا إذا أثبت أنه لم يرتكب أي إهمال. تنشأ مسؤولية مزود خدمات المصادقة من واقع أنه يتوجب عليه جمع كل المعلومات المطلوبة لإصدار شهادة المصادقة الإلكترونية وكذلك التحري عن صحة المعلومات الواردة في شهادة المصادقة وأخيراً المصادقة على أن بيانات التحقق من التوقيع تعود لشخص معين يحوز بيانات إنشاء توقيع مقابلة للنوع الأول من البيانات. كما يكون مزود خدمات المصادقة الإلكترونية الذي يصدر شهادة مصادقة موصوفة، مسؤولاً عن الضرر الواقع على كل شخص طبيعي أو معنوي، يستند بشكل معقول على هذه الشهادة، وذلك من أجل عدم تسجيل إلغاء الشهادة، إلا إذا أثبت مزود خدمات المصادقة أنه لم يرتكب أي إهمال. فإلغاء شهادة المصادقة يرتب زوال الموثوقية عن كل توقيع إلكتروني يتم بالاستناد إلى بيانات إنشاء التوقيع، ويفترض بالمتعامل مع الموقّع أن يكون على علم بهذا الأمر حتى يحتاط له. من هنا ينشأ موجب مزود خدمات المصادقة بتسجيل إلغاء الشهادة فوراً ونشر ذلك. كذلك يعود لمزود خدمات المصادقة الإلكترونية، وفق المادة ١٢ من القانون، أن يذكر في شهادة موصوفة القيمة القصوى للمعاملات التي يمكن استعمال الشهادة فيها، بشرط أن تكون هذه القيمة القصوى ظاهرة للغير. ولا يكون مزود خدمات المصادقة الإلكترونية مسؤولاً عن الأضرار التي تنتج عن تخطي هذه القيمة القصوى. فقد يرغب شخص معنوي بتحديد الصلاحيات المالية لممثليه بالتوقيع عنه وفق سقوف معينة كما هي حال المديرين في الشركات التجارية.

أو قد يحتاط شخص في تعامله على الإنترنت مخافة إساءة استعمال توقيعه ويفرض سقفاً لقيمة معاملاته. وفي جميع الأحوال يجب أن تظهر للمتعاملين بشكل واضح القيمة القصوى لأي معاملة إلكترونية للمُوقِّع يرغب بتوقيعها إلكترونياً، وذلك لحماية مصالحهم.

في المقابل، وفق المادة ١٣ من القانون تترتب مسؤولية على صاحب شهادة المصادقة عن صحة المعلومات المتعلقة به المقدمة إلى مزود خدمات المصادقة وتحديثها، وعن عدم اتخاذ التدابير الضرورية، كإعلام مزود خدمات المصادقة، في حال تعرض بيانات إنشاء التوقيع لما يثير الشبهة أو للانكشاف، وعن استعمال شهادة مصادقة إلكترونية موقوفة أو مُلغاة أو عن استعمال شهادة خلافاً لشروطها. ففي هذه الحالات، يكون الضرر عائداً بشكل واضح إلى فعل خاطئ صادر عن صاحب شهادة مهمل أو سيء النية.

تتعرض المادة ١٤ من القانون إلى مسؤولية الطرف المعوّل/المعتمد، فهو يكون مسؤولاً عن عدم اتخاذ خطوات معقولة للتحقق من موثوقية التوقيع الإلكتروني أو للتحقق من صلاحية الشهادة أو وقفها أو إلغائها أو وجود قيود عليها. ففي هذه الحالات يكون الطرف المعوّل/المعتمد قد ارتكب خطأً كبيراً أو إهمالاً فاضحاً يشكل مانعاً لمسؤولية أي طرف آخر كمزود خدمات المصادقة الإلكترونية. فمن أولى البديهيات قيام الطرف المعوّل/المعتمد بالتحقق من موثوقية التوقيع الإلكتروني ومن الشهادة العائدة له، إذ أن آلية التوقيع الإلكتروني كلها، من بيانات إنشاء التوقيع إلى بيانات التحقق من التوقيع، قد صُمّمت لتمكين الطرف المعوّل/المعتمد من إجراء التحقق.

يتطرق **الباب الرابع** المعنون "الاعتراف القانوني بشهادات المصادقة الإلكترونية الأجنبية" إلى مفعول شهادات المصادقة الإلكترونية الصادرة في دولة أجنبية. وتعتبر المادة ١٥ من القانون شهادات المصادقة الإلكترونية الأجنبية الموصوفة معادلة من الناحية القانونية لشهادات المصادقة الصادرة عن مزود خدمات مصادقة وطني في إحدى ثلاث حالات: حالة تلبية الشهادة ومزود خدمات المصادقة الإلكترونية الشروط المذكورة في هذا الإرشاد مع وجود ترخيص للمزود في إحدى الدول الأعضاء، وحالة ضمان الشهادة من قبل مزود خدمات مصادقة إلكترونية وطني يلبي المتطلبات الواردة في هذا الإرشاد، وحالة كون الشهادة أو مزود خدمات المصادقة الإلكترونية معترفاً بهما تطبيقاً لاتفاق ثنائي أو متعدد الأطراف بين الدولة العضو ودول أخرى أو منظمات دولية. إن توضيح الوضعية القانونية لشهادة مصادقة إلكترونية أجنبية هو ضروري لحل الإشكاليات الناشئة عن تجاوز التعاملات الإلكترونية الحدود الوطنية بفعل الإنترنت، كما أن من شأن ذلك المساهمة في توحيد المتطلبات التي يخضع لها مزودو خدمات المصادقة وشهادات المصادقة.

ينظم **الباب الخامس** المعنون "العمليات المصرفية" هذه العمليات، أي تلك المتعلقة بأوامر الدفع والتحويل الإلكتروني للأموال النقدية وبالبطاقات المصرفية وبالنقود الإلكترونية وبالشيكات الإلكترونية.

تتناول المادة ١٦ مسألة إصدار أوامر الدفع والتحويل الإلكتروني للأموال النقدية. فحتى يكون كل طرف على بينة من حقوقه وموجباته ومن الجدوى الاقتصادية من العقد، ولحماية العميل الطرف غير الممتهن في العقد وهو الأضعف، توجب المادة ١٦ أن يتم إبرام اتفاق واضح ومفصل مسبق بين العملاء والمصارف والمؤسسات المالية على الشروط التنظيمية لأوامر الدفع الإلكترونية أو التحاويل الإلكترونية للأموال النقدية[٢٠]. ويجب أن تتضمن هذه الشروط تعيين تاريخ نفاذ أوامر التحويل الصادرة والواردة والعمولات المستوفاة وقيمة العملية المنجزة وحقوق فريقي العقد وموجباتهما والقواعد المختصة بالأخطاء في القيود أو القيود غير المشروعة وطرق الاعتراض المتاحة للعميل والإجراءات المتبعة في حال الدخول غير المشروع على حساب العميل وسعر الصرف المعتمد للعملة الأجنبية والقيود على العمليات. وضمانةً لحقوق فرقاء العقد وتجنباً لحدوث أي إلباس في بيان موجبات وحقوق كل طرف، تشترط المادة ١٦ أن يكون الأمر بتحويل الأموال النقدية خطياً على دعامة ورقية أو إلكترونيةً، وإذا كان الأمر صادراً بالصورة الإلكترونية، يجب التصديق عليه من قبل هيئة رسمية أو خاصة تعتمدها كل دولة عضو.

تحدد المادة ١٧ مواصفات الأنظمة الإلكترونية المستعملة في العمليات المتعلقة بأوامر الدفع والتحاويل الإلكترونية، والضمانات التقنية والقانونية المقدمة لسلامة هذه العمليات. فالأنظمة الإلكترونية يجب أن تكون قادرة على نقل أمر دفع إلكتروني أو تحويل إلكتروني للأموال النقدية مع قدرتها على تخزين البيانات المتعلقة بالأمر للتمكن من الرجوع إليه. ويجب أن تتضمن هذه البيانات تحديداً للجهة المُرسلة وإسم العميل وقيمة المبالغ وغيرها من العناصر المهمة. كما يجب أن تتيح هذه الأنظمة الإلكترونية للطرف الآمر بالدفع أو بالتحويل معرفة نتيجة هذا الأمر فوراً لجهة القبول أو الرفض وأسباب هذا الرفض.

تتكلم المادة ١٨ من القانون عن مسؤولية العميل عن أوامر الدفع أو التحاويل الإلكترونية. فلا يكون العميل مسؤولاً عن أي قيد جرى على حسابه ناتج عن تحويل إلكتروني للأموال النقدية، بعد قيامه بإبلاغ المصرف أو المؤسسة المالية عن وجود إمكانية لدخول الغير إلى حسابه دون وجه حق، أو عن فقدان بطاقته المصرفية أو احتمال معرفة الغير لرمز التعريف الخاص به. وعلى العميل اتباع الأصول والإجراءات المتفق عليها مع المصرف أو المؤسسة المالية بشأن معاملة التبليغ. لا يستطيع العميل أن يلغي أو يرجع أمر تحويل إلكتروني للأموال النقدية صادر عنه بعد سحب المبلغ من حسابه. فالعميل المتنبه إلى مصالحه يفترض أن يبادر إلى إبلاغ المصرف في حال وجود خطر عليها وذلك عبر إتباع طرق التبليغ المتفق عليها، ويكون حينها قد أتم واجباته، ويعود للمصرف أو للمؤسسة المالية التصرف على أساس التبليغ الحاصل.

تتعرض المادة ١٩ لمسؤولية المصرف أو المؤسسة المالية عن عدم تنفيذ أمر تحويل عميله، ولاعتراض العميل ولموجب تقديم معلومات مفصّلة له. ففي الحالة الأولى، يتحمل المصرف أو المؤسسة المالية مسؤولية عدم تنفيذ أمر التحويل كلياً أو جزئياً أو سوء تنفيذه. يتوجب عليه حينها، بالإضافة إلى التعويضات، إعادة المبالغ إلى العميل الآمر بالتحويل، إلا إذا كان عدم التنفيذ ناجماً عن خطأ أو نقص في التعليمات المعطاة من قبل الأخير.

في الحالة الثانية، أي في حال اعتراض العميل على عملية دفع إلكتروني أو تحويل إلكتروني للأموال النقدية، يتوجب على المصرف أو المؤسسة المالية أن تثبت أنه قد جرى قيد هذه العملية أصولاً وأنها لم تتعرض لأي خلل تقني في النظام المعلوماتي. ويُمنع تحميل العميل أية فوائد أو عمولات بغية تصحيح الأخطاء في قيود عمليات الدفع الإلكترونية أو قيود التحاويل الإلكترونية للأموال النقدية.

وفي جميع الأحوال، يجب على المصرف أو المؤسسة المالية تقديم معلومات منتظمة مفصلة لعملائها عن عمليات الدفع الإلكترونية أو التحاويل الإلكترونية للأموال النقدية.

تتناول المادة ٢٠ مسألة تعديل شروط التعاقد. فقد اشترطت قيام المصرف أو المؤسسة المالية قبل ١٠ أيام على الأقل بإبلاغ العميل صراحةً بأي تعديل مُقترح على شروط التعاقد. إلا أنه في الحالات الاستثنائية، مثل تلك المتعلقة بالحفاظ على سلامة حساب العميل أو نظام الدفع الإلكتروني، يمكن للمصرف أو المؤسسة المالية فرض قيود على الخدمة المقدمة للعميل شرط أن يصار إلى إبلاغه فوراً بالقيود ودون تحميله أية أعباء مالية من جراء ذلك. وتوازن هذه المادة من جهة بين مبدأ حماية العميل وعدم مفاجأته بشروط جديدة دون أن يكون لديه الوقت الكافي لدراستها ومن جهة ثانية بين ضرورات حماية حساب العميل بفرض قيود فورية على خدمة العميل، على أن يصار إلى إعلامه فوراً بهذه القيود. ولا ينتظر المصرف أو المؤسسة المالية في الحالات الاستثنائية موافقة العميل على فرض الإجراءات بسبب ضرورة الإسراع بالتصرف صوناً لسلامة حسابه.

تفرض المادة ٢١ من القانون أن يكون طلب الحصول على بطاقة مصرفية أو على العقد العائد لإصدارها خطياً على دعامة ورقية أو إلكترونية، وذلك منعاً لأي التباس حول مضمون العقد.

تفصل المادة ٢٢ من القانون مسؤوليات المصرف أو المؤسسة المالية عند إصدار بطاقات مصرفية، فكلاهما ملزم بموجب الإعلام تجاه أصحاب البطاقات المصرفية، وبإعطاء معلومات التعريف لأصحاب البطاقات لتمكينهم من استخدامها مع الحفاظ على السرية، وبحفظ كشوفات مفصلة عن عشر سنوات، بوضع وسائل ملائمة للإبلاغ عن فقدان البطاقة أو سرقتها، وبمنع استخدام البطاقة بعد حصول هذا الإبلاغ. كذلك، يكون المصرف أو المؤسسة المالية مسؤولين عن عدم تنفيذ الأوامر الصادرة عن صاحب البطاقة أو عن سوء تنفيذها، وكذلك عن العمليات المنفذة دون موافقته وعن الأخطاء في قيود حسابه. وعلى المصرف أو المؤسسة المالية أن يدفعا لصاحب البطاقة المبالغ المسحوبة من حسابه دون مبرر مشروع.

تفصل المادة ٢٣ من القانون مسؤوليات صاحب البطاقة المصرفية لجهة كيفية استعمال البطاقة ولجهة الاعتراض على عمليات الدفع ولجهة إبلاغ المصرف بفقدان البطاقة أو بسرقتها. فقد ورد فيها أنّ صاحب البطاقة المصرفية يلتزم باستعمال بطاقته وفق الشروط المتفق عليها ويتخذ كل الاحتياطات اللازمة لحماية البطاقة ومعلومات التعريف التي تتيح استعمالها. ولا يمكن لصاحب البطاقة المصرفية أن يرجع عن أمر الدفع الإلكتروني الصادر بواسطة هذه البطاقة. ولا يحق لصاحب البطاقة المصرفية أن يعترض على أي عملية دفع إلا في حال تعرضت بطاقته أو معلومات التعريف التي تتيح استعمالها للفقدان أو السرقة أو الاستعمال غير المشروع أو الاحتيالي أو في حال الخطأ الحاصل من قبل الجهة المصدرة للبطاقة. ويجب على صاحب البطاقة المصرفية، فور معرفته، إبلاغ المصرف أو المؤسسة بفقدانه بطاقته أو بسرقتها، وبأي عملية تمت دون موافقته.

وبأي خطأ في كشف حسابه. ويتحمل صاحب البطاقة المصرفية، حتى تاريخ إبلاغه المصرف أو المؤسسة المالية، نتائج فقدان البطاقة أو سرقتها، وذلك في حدود سقف تعينه كل دولة. لكن هذا السقف لا يطبق في حال ارتكاب صاحب البطاقة المصرفية خطأ فادحاً أو إهمالا كبيراً، أو في حال عدم قيامه بالإبلاغ وفق الفقرة السابقة ضمن مهلة معقولة.

وقد أعفت المادة ٢٣ من القانون صاحب البطاقة المصرفية من المسؤولية في عدة حالات: حالة حصول عمليات دفع بعد تقدمه باعتراض، حالة عمليات الدفع غير المشروعة المنفذة عن بعد دون تقديم البطاقة مادياً، حالة تزوير البطاقة المصرفية. وفي مثل هذه الحالات، يتولى المصرف أو المؤسسة المالية إعادة قيد المبالغ المعترض عليها في حساب صاحب البطاقة دون استيفاء أي عمولة أو نفقة، وذلك في خلال مهلة شهر من تاريخ استلام اعتراض صاحب البطاقة.

تنظم المادة ٢٤ من القانون النقود الإلكترونية، فتنص على أنها تصدر عن المصرف المركزي في دولة عضو أو عن مؤسسة مالية مرخص لها بذلك، وذلك بناءً على عقد يبرم مع العميل، على أن يتضمن العقد حقوق والتزامات الفريقين بشكل واضح. وتشكل وحدات النقود الإلكترونية ديناً على مُصدرها، يسقط بانقضاء مدة صلاحيتها، ويبرئ بالتالي ذمة مُصدرها.

تتناول المادة ٢٥ الشيك الإلكتروني محددةً مشتملاته والضمانات الخاصة به. إذ يجب أن يتضمن جميع البيانات المطلوبة قانوناً، ويعود لكل دولة عضو أن تحدد ضمانات تقنية لضمان موثوقية الشيك الإلكتروني وصحته وكذلك أن تضع قواعد تنظيمية مفصلة لكيفية استعماله. ويمكن للمصارف في الدول الأعضاء التعامل بالشيكات الإلكترونية.

تحدد المادة ٢٦ الأخيرة تحت عنوان أحكام ختامية مبدأ حق الوصول إلى المعلومات العامة. وعلى الدولة أن تضمن هذا الحق شريطة أن لا يؤدي ذلك إلى التعرض للأمن الوطني أو سلامة الدولة أو الحياة الخاصة للأفراد أو الأسرار المحمية بموجب نصوص قانونية خاصة أو أن ينتهك النظام العام في الدولة."

هوامش

1- Information Privacy in Cyberspace Transactions by Jerry Kang 1998: http://www.ntia.doc.gov/ntiahome/privacy/files/cprivacy.pdf
«Cyberspace transaction» means an interaction with an individual through cyberspace for the purposes of satisfying, accepting, or completing an individual's request, offer, lease, financing, rental, purchase, sale, or exchange of information, services, or goods. A «cyberspace transaction» specifically includes the browsing of a World Wide Web page through the hypertext transfer protocol and its subsequent extensions, regardless of whether any money is exchanged. A «cyberspace transaction» specifically excludes any portion of an interaction that is a message from an individual to an individual in a noncommercial context, or to a publicly accessible forum.

٢- أي قبل وضع تشريع ينظم المعاملات إلكترونيا"

٣ - يراجع الإثبات الالكتروني، للقاضي وسيم شفيق حجار: "ان التشفير هو من أقدم العلوم التقنية، يعود على الأقل لأربعة آلاف سنة، وقد بدأ على الأرجح حوالي عام ٢٠٠٠ قبل الميلاد في مصر الفرعونية، حيث استعمل لتزيين قبور الحكام والملوك، ليس بغرض إخفاء محتوى النصوص، بل بهدف جعلها أكثر فخامة وقدسية. في الهند استخدمت رموز سرية في العصور الغابرة للتواصل بين الحكام وجواسيسهم. كما طور اليونانيون والاسبرطيون أنظمة التشفير، ولجأت الجيوش الرومانية إلى تقنيات معينة في الكتابة من اجل تبادل رسائل مشفرة غير مفهومة من العدو. تقدم التشفير في العصور الوسطى خصوصاً في ايطاليا فينيس، حيث كرس لأهداف الاتصال بالسفراء، ووضع الكاهن الألماني Trithemius نظاماً جديداً للتشفير وترك خمس كتب حول هذا الموضوع عام ١٥١٨. في القرن السابع عشر، أنشئت في معظم الدول الأوروبية ما يعرف بالغرف السوداء Black Chambers لاستنباط تقنيات التشفير وتفكيك شيفرات الدول الأخرى. ومن ثم عرف علم التشفير خطوات أخرى، منها ابتكار دولاب التشفير الذي يتكون من عدة دوائر برّامة في قالب واحد تحتوي كل منها على الأحرف الأبجدية. وظهر بعد ذلك الدوار الكهربائي Rotor، الذي يتلقى النص غير المشفر من لوحة المفاتيح لينتج الموجة الكهربائية المناسبة على لوحة التشفير التي تخرج النص المشفر. ومع اختراع التلغراف عام ١٨٤٤، وأجهزة البث اللاسلكية عام ١٨٩٥، تم اللجوء إلى تقنيات التشفير لتوفير سرية الاتصالات".
كمثال على التشفير البدائي في تلك الحقبة، كانت الرسالة تكتب على ورق يلف حول دعامة، وحتى تفك الرسالة، يقتضي إعادة وضعها على دعامة بنفس القطر، لتأمين ترابط الكلمات والجمل وتسلسلها.

– نرفق بهذا الإرشاد رسومات لعملية التشفير بهدف مساعدة المشترع في فهم التقنية الدقيقة لهذه العملية،

-How encryption works: http://computer.howstuffworks.com/encryption1.htm

The Greek historian Plutarch wrote, for example, about Spartan generals who sent and received sensitive messages using a scytale, a thin cylinder made out of wood. The general would wrap a piece of parchment around the scytale and write his message along its length. When someone removed the paper from the cylinder, the writing appeared to be a jumble of nonsense. But if the other general receiving the parchment had a scytale of similar size, he could wrap the paper around it and easily read the intended message.

٤ – راجع:

– نظام DES-Data Encryption Standard http://www.itl.nist.gov/fipspubs/fip46-2.htm

DES – Data Encryption Standard http://www.cypher.com.au/crypto_history.htm
In 1972 the US National Bureau of Standards began the search for an encryption algorithm that could be tested and certified. After several false starts in 1974 IBM offered the US government an algorithm which was based on the early 1970's LUFICER algorithm. The offer was accepted and the algorithm was tested and 'adjusted' by the NSA and eventually released as a federal standard in 1976.

DES is a Symmetric block cypher based on a 64 bit block. The user feeds in a 64 block of plain text and is returned 64 bits of cyphertext. The same algorithm and key are used for the encrypt and decrypt operations.

Since its release in 1976 the key has remained fixed at 56 bits (reduced from a 128 bit key as part of the NSA 'adjustment') although it was possible to 'build' DES with a 128 bit key, exporting it from the US was banned. Recently however this key length restriction was removed by the US Government.

– نظام AES-Advanced Encryption Standard المرفق بهذا التقرير http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

AES - Advanced Encryption Standard, The Latest Encryption Algorithm http://cyberstephanians.blogspot.com/2008/02/advanced-encryption-standard-latest.html
Advanced Encryption Standard (AES) is the latest encryption standard used to protect confidential information like financial data for government and commercial use. It is a stronger symmetric encryption algorithm that was approved by NIST (National Institute of Standards and Technology) to replace the Data Encryption Standard (DES) and Triple DES encryption algorithm. DES is arguably the most important and widely used cryptographic algorithm in the world. However, its usefulness is now quite limited after years of advances in computational technology. A DES key can now be easily cracked after several hours of number crunching. By using dedicated hardware, Electronic Frontier Foundation manages to break it in 22 hours (http://www.rsasecurity.com/rsalabs/des3/).

Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. It has been analyzed extensively and is now used worldwide, as was the case with its predecessor,[3] the Data Encryption Standard (DES). AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001 after a 5-year standardization process (see Advanced Encryption Standard process for more details). It became effective as a standard May 26, 2002. As of 2006, AES is one of the most popular algorithms used in symmetric key cryptography. It is available by choice in many different encryption packages.

– بالإضافة الى الغوريتميات Algorithms أخرى مثال:

3-Way • ABC • Akelarre • Anubis • ARIA • BaseKing • BassOmatic • BATON • BEAR and LION • CAST-256 • CIKS-1 • CIPHERUNICORN-A • CIPHERUNICORN-E • CLEFIA • CMEA • Cobra • COCONUT98 • Crab • Cryptomeria/C2 • CRYPTON • CS-Cipher • DEAL • DES-X • DFC • E2 • FEAL • FEA-M • FROG • G-DES • GOST • Grand Cru • Hasty Pudding cipher • Hierocrypt • ICE • IDEA NXT • Intel Cascade Cipher • Iraqi • KASUMI • KeeLoq • KHAZAD • Khufu and Khafre • KN-Cipher • Ladder-DES • Libelle • LOKI97 • LOKI89/91 • Lucifer • M6 • M8 • MacGuffin • Madryga • MAGENTA • MARS • Mercy • MESH • MISTY1 • MMB • MULTI2 • MultiSwap • New Data Seal • NewDES • Nimbus • NOEKEON • NUSH • Q • RC6 • REDOC • Red Pike • S-1 • SAFER • SAVILLE • SC2000 • SHACAL • SHARK • SMS4 • Spectr-H64 • Square • SXAL/MBAL • Threefish • Treyfer • UES • Xenon • xmx • XXTEA • Zodiac.

5- The legal and market aspects of electronic signature, Study for the European Commission- DG Information Society http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

٦– لقد ظهرت عدة آليات معلوماتية (بروتوكولات) Protocole للتعامل الآمن في السوق التجاري في السنوات الأخيرة، نذكر منها:
١ . نظام PGP (Pretty good Privacy) الذي ابتكره Phil Zimmermann، وهو بسيط وسهل، إلا أن استعماله يخضع لقيود في أوروبا وأميركا. ٢ . نظام S-HTTP الذي يعتمد عدة تقنيات تشفير، ويسمح بتوقيع الرسالة البيانية بعد تشفيرها. ٣ . نظام SSL (Secure Socket layer) الذي تم تطويره من قبل شركة Netscape، وهو قابل للتطبيق فقط على المعاملات عبر شبكة الانترنت. ٤ . نظام SET (Secure Electronic Transaction) الذي وضع عام ١٩٩٦ من قبل شركتي Visa وMasercard بالاشتراك مع شركات Microsoft وIBM وNetscape، حيث يهدف هذا النظام إلى تأمين التعامل عبر استعمال البطاقة المصرفية. Francis Balle، Laurent Cohen-Tanugi، Dictionnaire du Web، 2001، Dalloz، p70

7- See Authentication Protocols, available: http://www.comptechdoc.org/independent/networking/protocol/protauthen.html
An authentication protocol is a type of cryptographic protocol with the purpose of authenticating entities wishing to communicate securely:

CHAP - Challenge Handshake Authentication Protocol is a three way handshake protocol which is considered more secure than PAP. Authentication Protocol.
EAP - Extensible Authentication Protocol is used between a dial-in client and server to determine what authentication protocol will be used.
PAP - Password Authentification Protocol is a two way handshake protocol designed for use with PPP. Authentication Protocol Password Authentication Protocol is a plain text password used on older SLIP systems. It is not secure.
SPAP - Shiva PAP. Only NT RAS server supports this for clients dialing in.
DES - Data Encryption Standard for older clients and servers.
RADIUS - Remote Authentication Dial-In User Service used to authenticate users dialing in remotely to servers in a organization's network.
S/Key - A one time password system, secure against replays. RFC 2289. Authentication Protocol.
TACACS - Offers authentication, accounting, and authorization. Authentication Protocol.
MS-CHAP (MD4) - Uses a Microsoft version of RSA message digest 4 challenge and reply protocol. It only works on Microsoft systems and enables data encryption. Selecting this authentification method causes all data to be encrypted.
SKID - SKID2 and SKID3 are vulnerable to a man in the middle attack.

8- UNCITRAL Model Law on Electronic Signatures (2001), available: http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf

- "Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message;

- A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later. A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211953,00.html

- Methods, software programs, and systems for electronic information security http://www.freepatentsonline.com/7395436.html FIG. 3A shows a diagram of digital signature creation

9- European law (directive n.93/1999) provides three kinds of electronic signatures, each with different juridical value: 1- electronic signature (also called a weak electronic signature or light electronic signature); 2- advanced electronic signature; 3- advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device (also called a secure digital signature, strong digital signature, or qualified digital signature).
http://www.symantec.com/connect/articles/digital-signatures-and-european-laws

10- OECD Guidelines for Cryptography Policy:
«Cryptography» means the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorized use.

«Encryption» means the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality. http://www.oecd.org/document/11/0,3343,en_2649_34255_1814731_1_1_1_1,00.html

١١- راجع كتاب الإثبات الالكتروني للقاضي وسيم حجار:
يفترض التشفير عنصرين: آلية التشفير Algorithm ومفتاح التشفير Clé، وإن هناك نوعين من التشفير، أو من آلية التشفير بتعبير أدق:
١. التشفير عبر المفتاح السري Clé Secrète à، أو المفتاح المتماثل Symétrique وهو يتم بتشفير المعلومات وفك تشفيرها عبر استعمال مفتاح واحد. لذا، يصبح هذا النظام أكثر عرضة للاختراق عند تعدد المستخدمين، حيث سيشترك في مفتاح التشفير هؤلاء المستخدمون جميعاً. يتم تشفير النص المنوي تشفيره مقطعاً تلو الآخر، حيث يُقسم هذا النص الى وحدات ذات حجم معين. تجدر الإشارة أخيراً إلى ان النظام الأكثر شهرة بالنسبة لهذه التقنية هو نظام DES (Data Encryption Standard) وRC4. يرتكز هذا النوع من التشفير على عمليتي استبدال حرف بآخر وتغيير تسلسل الأحرف، حيث يكون مفتاح التشفير عبارةً عن أرقام جزافية ذات طول معين Nombres Pseudoaléatoires، تنتج من برنامج معلوماتي بالاستناد الى نواة محددة Semence مثل ساعة وتاريخ إنتاج المفتاح. يُفترض هذا الأسلوب أن يكون المفتاح سرياً وغير معروف إلا من المرسل والمستقبل، وتكمن الصعوبة في نقل المفتاح الى المرسل إليه، وتتم عملية النقل هذه عادةً وفق آلية متفق عليها.

٢. التشفير عبر المفتاح العمومي (العام) Clé Publique à، أو المفتاح غير المتماثل: Asymétrique. في هذه الحالة، يُستعمل مفتاحان، واحدٌ للتشفير وآخر لفك التشفير. المفتاحان مرتبطان حسابياً، فما يمكن تشفيره بأحدهما يُمكن فكه بالآخر. يعمد المُرسِل الى تشفير الرسالة مستعملاً المفتاح العمومي للمُستقبل (هذا المفتاح معلومٌ من الجميع)، في حين يقوم المرسل إليه بحل التشفير، بعد استلامه الرسالة المُشفرة، بواسطة مفتاحه الخاص المحفوظ لديه، والذي لا يتشاركه مع احد، ولا يمكن فك التشفير إلا بواسطة المفتاح المذكور المملوك فقط من المُرسل إليه. هكذا، لا يعود ضرورياً تبادل المفاتيح عبر الشبكة المشرعة للعموم وتحمُل إمكانية اعتراض هذه المفاتيح من قبل الغير وكشفها. يستعمل هذا التشفير معادلاتٍ حسابية مقعدة، ولتبسيط الأمور يرتكز نظام إنتاج المفاتيح على حاصل ضرب رقمين أوليين بحجم كبير p و q ضمن شروطٍ حسابية معينة.

ترتبط مناعة نظام التشفير بطول المفتاح المُستعمل، الذي يُقاس بوحدة، تُسمى بيت Bit، وكلما كبُر المفتاح ازدادت صعوبة اختراقه، إلا أن إطالة المفتاح دونها سلبيات، فالمعلومات المُشفرة تكون في المبدأ أكبر حجماً من المعلومات الأساسية قبل تطبيق التشفير عليها، وتنعكس زيادة طول مفتاح التشفير على حجم المعلومات المُشفرة، فكلما ازداد طول المفتاح زاد حجم المعلومات، وبما ان نقل المعلوماتٍ يتم بوتيرة معينة b/s هي سعة خط النقل الممكنة، فإن إطالة مفتاح التشفير تستلزم وقتاً أطول لإتمام عملية نقل المعلومات بعد تشفيرها، مما يعني بطءاً في الأنظمة المعلوماتية، وارتفاعاً في كلفة النقل عبر الشبكات.

- Methods, software programs, and systems for electronic information security: http://www.freepatentsonline.com/7395436.pdf

12- An encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret. This methodology is usually only used by a small group. www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html

A system of encryption where both the encoding and decoding keys are privately held by the sender and receiver.
www.utexas.edu/lbj/21cp/ebt/glossary.htm

13- Digital Signature Guidelines Tutorial http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html
Digital signatures are created and verified by cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. Digital signatures use what is known as «public key cryptography,» which employs an algorithm using two different but mathematically related «keys;» one for creating a digital signature or transforming data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original form. Computer equipment and software utilizing two such keys are often collectively termed an «asymmetric cryptosystem.»

14- The European Commission welcomes new legal framework to guarantee security of electronic signatures, Brussels, 30 November 1999
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/99/915&format=HTML&aged=1&language=EN&guiLanguage=en

15- Public key cryptography is a widely adopted cryptographic system used to encrypt data. Unlike symmetric cryptography, which utilizes a single key, this type of system is considered asymmetric because it relies on a pair of keys. Public key cryptography was originally introduced in the 1970s by cryptographers Whitfield Diffie and Martin Hellman. Such cryptography systems are often referred to as Diffie-Hellman encryption as a way of paying homage to the inventors.
http://www.wisegeek.com/what-is-public-key-cryptography.htm

16- Digital Signature Guidelines Tutorial http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html
Verification of a digital signature is accomplished by computing a new hash result of the original message by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the verifier checks: (1) whether the digital signature was created using the corresponding private key; and (2) whether the newly computed hash result matches the original hash result which was transformed into the digital signature during the signing process. The verification software will confirm the digital signature as «verified» if: (1) the signer's private key was used to digitally sign the message, which is known to be the case if the signer's public key was used to verify the signature because the signer's public key will verify only a digital signature created with the signer's private key; and (2) the message was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the digital signature during the verification process.

17- Entrust Securing Digital Identities & Information: http://www.entrust.com/digital-certificates.htm
Digital certificates are the evolving, current-day standard to help solve the growing concerns regarding secure online communication and the protection of sensitive data. This is particularly the case with transactions where financial institutions and their clients similarly contend that the leading impediment to online banking is security. Since traditional security measures like firewalls, anti-virus software, and login/password user authentication are no longer sufficient to address the increasing number of sophisticated online attacks, digital certificates were implemented as an alternative to basic authentication security practices

18- Entrust Securing Digital Identities & Information: http://www.entrust.com/certification-authority.htm
A certification authority is a trusted third party organization that issues digital certificates to requesting organizations after a process of verifying (or certifying as the name implies) their credentialing information. As a part of this process, an issued digital certificate contains some of that information for identification purposes: such as the certificate holder's name, organization, address, etc. By issuing the digital certificate, the certification authority attests to the organization's identification contained therein, confirming that it is a legitimate entity.

19- Digital Signature Guidelines Tutorial http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html
To sign a document or any other item of information, the signer first delimits precisely the borders of what is to be signed. Then a hash function in the signer's software computes a hash result unique (for all practical purposes) to the message. The signer's software then transforms the hash result into a digital signature using the signe's private key. The resulting digital signature is thus unique to both the message and the private key used to create it.

20- 97/489/EC: Commission Recommendation of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997H0489:EN:HTML

نص الإرشاد المتعلق بالمعاملات الإلكترونية والتواقيع الإلكترونية

الباب الأول: أحكام عامة

المادة ١: نطاق التطبيق

إن الهدف من الإرشاد هو تسهيل استخدام التواقيع الإلكترونية والسندات والكتابة الإلكترونية والاعتراف القانوني بها. ويشكل الإرشاد بالتالي إطاراً قانونياً للتواقيع الإلكترونية وبعض خدمات المصادقة من أجل ضمان حسن سير المعاملات.

لا يغطي الإرشاد الجوانب المتعلقة بإبرام وبصحة العقود أو غيرها من الموجبات القانونية عندما يكون هناك متطلبات شكلية بموجب القوانين الوطنية. ولا يمس هذا الإرشاد بالقواعد والقيود التي تنظم استخدام المستندات الواردة في القوانين الوطنية.

المادة ٢: تعاريف

١. **السند الإلكتروني:** هو القيد أو العقد أو المراسلة التي تنشأ أو ترسل أو تسجل أو تسلم أو تحفظ بوسائل إلكترونية أو على وسيط إلكتروني ويمكن استخراجها بشكل مفهوم.

٢. **التوقيع:** هو علامة مميزة تسمح بتحديد هوية الشخص الموقع وتعبر عن رضاه والتزامه بمضمون السند المُوقّع.

٣. **توقيع إلكتروني[1]:** هو بيانات بشكل إلكتروني متصلة أو مرتبطة منطقياً ببيانات إلكترونية أخرى، وهي تخدم كوسيلة لتأكيد الموثوقية.

٤. **توقيع إلكتروني متقدم:** هو توقيع إلكتروني يلبي المتطلبات التالية مجتمعةً:
- أن يكون مرتبطاً فقط بالمُوقّع.
- أن يسمح بتحديد المُوقع.
- أن يُنشأ بوسائل تكون تحت رقابة المُوقّع الحصرية.
- أن يكون مرتبطاً بالبيانات المُوقّعة بشكل أن كل تعديل لاحق في البيانات المُوقّعة يكون قابلاً للاكتشاف.

٥. **مُوقّع:** هو كل شخص يحوز آلية لإنشاء توقيع ويتصرف إما لحسابه الخاص أو لحساب شخص طبيعي أو معنوي يمثّله.

٦. **طرف معوّل/معتمد:** هو كل شخص يجوز أن يتصرف استنادا إلى شهادة مصادقة إلكترونية أو إلى توقيع إلكتروني.

٧. **بيانات لازمة لإنشاء توقيع إلكتروني:** هي بيانات فريدة، مثل رموز أو مفاتيح تشفير خاصة، يستخدمها المُوقّع لإنشاء توقيع إلكتروني.

٨. **آلية لإنشاء توقيع إلكتروني:** هي برنامج معلوماتي أو تجهيزات معلوماتية معدة لتضع موضع التطبيق البيانات اللازمة لإنشاء توقيع إلكتروني.

٩. **آلية آمنة لإنشاء توقيع إلكتروني:** هي آلية لإنشاء توقيع إلكتروني تلبي المتطلبات التالية مجتمعةً، بحيث تضمن على الأقل بوسائل تقنية وبإجراءات ملائمة أن:
- البيانات المستخدمة لإنشاء توقيع إلكتروني لا يمكن عملياً مصادفتها إلا مرة واحدة وأن سريتها هي مؤمنة بصورة معقولة.
- تكون هناك ضمانة كافية أن البيانات المستخدمة لإنشاء توقيع إلكتروني لا يمكن إيجادها بالاستنتاج وأن يكون التوقيع محمياً من أي تزوير أو تقليد بوسائل تقنية متاحة فعلياً.
- البيانات المستخدمة لإنشاء توقيع إلكتروني هي محمية بطريقة موثوقة من قبل المُوقّع الشرعي من أي استخدام من قبل الغير.
- الآلية الآمنة للتوقيع الإلكتروني لا تعدل البيانات الموقّعة، ولا تمنع أن تعرض هذه البيانات على الموقّع قبل التوقيع.

١٠. **بيانات لازمة للتحقق من التوقيع الإلكتروني:** هي بيانات، مثل رموز أو مفاتيح تشفير عامة، تستخدم للتحقق من توقيع إلكتروني.

١١. **آلية للتحقق من توقيع إلكتروني:** هو برنامج أو تجهيزات معلوماتية معدة من أجل وضع بيانات التحقق من التوقيع الإلكتروني موضع التطبيق عند التحقق من توقيع إلكتروني، من المناسب التأكد مما يلي:
- أن البيانات المُستخدمة من أجل التحقق من توقيع، تُطابق البيانات المعروضة بوجه المُتحقِّق المُتعامل الآخر.

- إمكانية التحقق من التوقيع بطريقة أكيدة والتأكد من أن نتيجة التحقق تُعرض بطريقة صحيحة.
- أن المُتحقِّق المُتعامل الآخر يستطيع بشكل أكيد، عند الاقتضاء، تحديد مضمون البيانات الموقّعة.
- إمكانية التحقق من مصداقية الشهادة وصحتها، وهو أمر ضروري للتحقق من التوقيع الإلكتروني.
- إمكانية تعرض نتيجة عملية التحقق من التوقيع الإلكتروني وهوية الموقّع بشكل صحيح.
- أن يتم التنويه وبشكل واضح أنه تم عن استعمال اسم مستعار.
- أن كل تعديل له تأثير على الأمان قابل للاكتشاف.

١٢. **شهادة مصادقة إلكترونية:** هي شهادة إلكترونية تربط بين بيانات التحقق من التوقيع الإلكتروني وبين شخص معين وتؤكد هوية هذا الشخص.

١٣. **شهادة مصادقة إلكترونية موصوفة:** هي شهادة إلكترونية تشتمل على التالي:
- إشارة إلى أنها شهادة موصوفة.
- تحديد مزود خدمات المصادقة الإلكترونية والبلد الذي يقيم فيه.
- اسم الموقّع.
- صفة خاصة للموقّع عند الاقتضاء في ضوء كيفية استخدام شهادة المصادقة.
- بيانات التحقق من التوقيع الإلكتروني والتي تقابل بيانات إنشاء التوقيع الإلكتروني. الموضوعة تحت رقابة الموقّع.
- تحديد بداية مدة صلاحية الشهادة وانتهائها.
- رقم الشهادة.
- التوقيع الإلكتروني المتقدم لمزود خدمات المصادقة الإلكترونية الذي أصدر الشهادة.
- حدود استخدام الشهادة.
- القيمة القصوى للمعاملات التي يمكن استخدام الشهادة فيها.

كما يجب أن تكون الشهادة صادرة من قبل مزود خدمات مصادقة إلكترونية يلبي الشروط التالية:
- أن يقدم الإثبات أنه موثوق كفاية لتقديم خدمات المصادقة الإلكترونية.
- أن يتقيد بالقواعد القانونية الموضوعة لحماية البيانات ذات الطابع الشخصي.
- أن يؤمن خدمة سريعة وأكيدة لدليل الشهادات وخدمة أكيدة وآنية لإلغاء الشهادات.
- أن يسهر على أنه يمكن تحديد تاريخ ووقت إصدار الشهادة وإلغائها بشكل دقيق.
- أن يتحقق، بوسائل ملائمة ومتوافقة مع القوانين الوطنية، من هوية ومن الصفات الخاصة للشخص الذي صدرت له الشهادة.
- أن يستخدم عناصر بشرية، تكون لديها المعارف المتخصصة والخبرات والمؤهلات الضرورية لتقديم الخدمات، وعلى وجه الخصوص، مؤهلات على مستوى الإدارة، معارف متخصصة في تكنولوجيا التواقيع الإلكترونية وممارسة جيدة لإجراءات الأمان الملائمة. وكذلك أن يطبق إجراءات وطرقاً إدارية منطبقة على المعايير المتعارف عليها.
- أن يستخدم أنظمة ومنتجات موثوقاً بها، تكون محمية من التعديلات وتوفر الأمان التقني والتشفيري للوظائف التي تنفذها.
- أن يتخذ تدابير ضد تزوير وتقليد الشهادات، وفي حالة كان ينتج بيانات لإنشاء التوقيع الإلكتروني، أن يؤمن السرية خلال عملية الإنتاج.
- أن تكون لديه موارد مالية كافية للعمل وفق متطلبات هذا الإرشاد، وعلى وجه الخصوص لتحمل المسؤولية عن الأضرار من خلال توفير ضمانات مناسبة.
- أن يسجّل جميع المعلومات الملائمة المتعلقة بشهادة موصوفة خلال المدة المفيدة، ولاسيما من أجل تقديم الدليل على الشهادة أمام القضاء. هذه التسجيلات ممكن أن تتم بطرق إلكترونية.
- أن لا يحفظ أو ينسخ بيانات إنشاء التوقيع الإلكتروني التي قدم لها خدمات إدارة المفاتيح.
- قبل التعاقد مع شخص يطلب شهادة، أن يعلم فيها هذا الشخص بشروط وبكيفية استخدام الشهادة، ولاسيما القيود على الاستخدام، وبإجراءات المطالبة وتسوية النِزاعات. هذه المعلومات، التي من الممكن نقلها بوسائل إلكترونية، يجب أن تكون خطية وفي لغة مفهومة بسهولة. إن بعض هذه المعلومات الملائمة يجب - أن توضع بتصرف الغير، بناءً لطلب، واستناداً إلى الشهادة.
- أن يستخدم أنظمة موثوق بها من أجل حفظ الشهادات في شكل قابل للتحقق منه وفق الشروط التالية:
- وحدهم الأشخاص المرخص لهم قادرون على إدخال معلومات وتعديلها.
- المعلومات تخضع للرقابة لجهة مصداقيتها.

الشهادات لا تكون متاحة لأبحاث الجمهور إلا بعد موافقة صاحب الشهادة.
- كل تعديل تقني يتعرّض لمتطلبات الأمان يكون ظاهراً للمشغل.

١٤. **مزود خدمات مصادقة إلكترونية[٢٢]:** هو كل هيئة أو شخص طبيعي أو معنوي يسلّم شهادات إلكترونية أو يقدم خدمات إلكترونية أخرى مرتبطة بالتواقيع الإلكترونية.

١٥. **منتوج توقيع إلكتروني:** هو كل منتوج تجهيزات أو برامج أو عنصر خاص من هذا المنتوج، معدّة للاستخدام من قبل مزود خدمات مصادقة إلكترونية من أجل تقديم خدمات التواقيع الإلكترونية، أو معدّة للاستخدام من أجل إنشاء التواقيع الإلكترونية أو التحقق منها.

١٦. **الاعتماد الاختياري:** هو كل ترخيص يحدد الحقوق والموجبات الخاصة بتقديم خدمات المصادقة الإلكترونية، يُعطى، بناءً لطلب مزود خدمات المصادقة الإلكترونية المعني، من قبل هيئة عامة أو خاصة مكلفة بوضع هذه الحقوق والموجبات وبمراقبة احترامها.

١٧. **أمر الدفع الإلكتروني أو التحويل الإلكتروني للأموال النقدية:** هو الأمر الذي ينظم كلياً أو جزئياً بوسيلة إلكترونية، ويفوض بموجبه العميل مصرفاً أو مؤسسة مالية، بإجراء دفع إلكتروني أو تحويل إلكتروني للأموال النقدية أو إتمام قيد دائن أو مدين على حسابه.

١٨. **بطاقة الدفع أو السحب المصرفية:** هي أداة صادرة عن مصرف أو عن مؤسسة مالية، وهي تتيح لصاحبها سحب الأموال وتحويلها، أو سحبها فقط.

١٩. **النقود الإلكترونية:** تتكون من وحدات تسمى وحدات نقد إلكتروني يمكن حفظها على دعامة إلكترونية لمدة محددة، وتصدر مقابل نقد تتم مبادلته فوراً، بنفس القيمة ونفس العملة، وتتيح للغير دون المصدر إتمام عمليات دفع.

٢٠. **الشيك الإلكتروني:** هو الشيك الذي يتم إنشاؤه والتوقيع عليه وتداوله إلكترونياً.

المادة ٣: مبادئ متعلقة بالأسواق الداخلية

تطبق كل دولة عضو التشريعات الوطنية التي تقرها وفقاً لهذا الإرشاد، على مزودي خدمات المصادقة الإلكترونية العاملين على أراضيها وعلى الخدمات التي يقدمونها.
تسهر الدول الأعضاء على إمكانية تداول منتجات التواقيع الإلكترونية المنطبقة على هذا الإرشاد بكل حرية في الأسواق الداخلية.

الباب الثاني: السندات والتواقيع الإلكترونية[٢٣]

المادة ٤: الآليات الآمنة لإنشاء التوقيع الإلكتروني

إن انطباق الآليات الآمنة لإنشاء التواقيع الإلكترونية على الشروط المبيّنة في التعاريف أعلاه تحدد من قبل أجهزة مختصة، عامة أو خاصة، تعيّن من قبل الدول الأعضاء.

إن التحقق من انطباق الآليات الآمنة لإنشاء التواقيع الإلكترونية على الشروط المعينة في التعاريف أعلاه يكون معترفاً به من قبل مجموع الدول الأعضاء في الإسكوا[٢٤].
يمكن أن تخضع الدول الأعضاء استخدام التواقيع الإلكترونية في القطاع العام لمتطلبات إضافية، هذه المتطلبات يجب أن تكون موضوعية وشفافة ومتناسبة وغير مميِّزة.

المادة ٥: مفهوم الكتابة الإلكترونية والآثار القانونية للسندات والكتابة الإلكترونية

الكتابة هي تدوين سلسلة حروف أو أرقام أو أشكال أو أي رموز لها معنى مفهوم، أياً كانت الدعامة المستعملة ووسائل نقل المعلومات. تعتمد الكتابة والسندات بالشكل الإلكتروني تماماً كالكتابة والسندات على دعامة ورقية، شرط تحديد الشخص الصادرة عنه؛ على أن تُنشأ وتحفظ في ظروف من شأنها أن تضمن سلامتها. ويكون للكتابة والسندات على دعامة إلكترونية نفس القوة الثبوتية للكتابة والسندات على دعامة ورقية.

المادة ٦: السندات العادية والرسمية الإلكترونية

يمكن تنظيم السندات العادية والسندات الرسمية بالشكل الإلكتروني، إلا أنه يعود للدول الأعضاء عدم اعتماد السندات الرسمية الإلكترونية أو بعض الفئات منها، كما يعود لها فرض متطلبات إضافية بالنسبة لها.

إن قاعدة تعدد النسخ الأصلية المعمول بها بالنسبة للعقود المتبادلة المنظمة بشكل سندات عادية تُعتبر مستوفاة عندما تُنظّم وتُحفظ السندات العادية الإلكترونية وفق شروط الموثوقية المنصوص عليها في هذا الإرشاد وعندما تسمح الآليات المعتمدة لكل طرف بالحصول على نسخ عن السندات أو بالوصول إليها.

المادة ٧: الآثار القانونية للتواقيع الإلكترونية

يستلزم التوقيع الإلكتروني استخدام وسائل أو إجراءات موثوق بها من شأنها تأمين التعريف بصاحب التوقيع وتأكيد الصلة بين التوقيع والسند الذي يتعلق به. تسهر الدول الأعضاء على أن تكون التواقيع الإلكترونية المتقدمة، والمُسندة إلى شهادات موصوفة والمُنشأة بواسطة آلية آمنة لإنشاء التواقيع:

- تلبي متطلبات القانون لناحية وجود توقيع في ما خص البيانات الإلكترونية، تماماً كالتوقيع اليدوي في ما خص البيانات المكتوبة أو المطبوعة على الورق.
- تكون مقبولة كوسيلة إثبات أمام القضاء.
- تستفيد من قرينة الموثوقية.

بخصوص التوقيع الإلكتروني، تسهر الدول الأعضاء على أن لا ترفض فعاليته القانونية وقبوله كوسيلة إثبات لمجرد:

- أن التوقيع هو بشكل إلكتروني.
- أو أن التوقيع لا يستند إلى شهادة موصوفة.
- أو أن التوقيع لا يستند إلى شهادة موصوفة صادرة عن مزود خدمات مصادقة إلكترونية مُرخص له.
- أو أن التوقيع غير مُنشأ بواسطة آلية آمنة لإنشاء التواقيع.

المادة ٨: التحقق من صحة وموثوقية السندات والتواقيع الإلكترونية

في حال أنكر الخصم السند الإلكتروني أو التوقيع الإلكتروني أو ادعى تزويرهما، يتحقق القاضي من توفر شروط الموثوقية المنصوص عنها في هذا الإرشاد. ويمكن للقاضي الاستعانة بالخبرة الفنية من أجل التحقق من توفر هذه الشروط.

يستفيد التوقيع الإلكتروني المتقدم من قرينة الموثوقية، إلا أنه يعود للقاضي القول، في ضوء العناصر التي تتوفر له، بزوال هذه القرينة.

المادة ٩: حفظ السندات الإلكترونية

عندما يشترط القانون حفظ سند أو معلومات، تكون عملية الحفظ بالشكل الإلكتروني صحيحة إذا:

- تم التأكد من سلامة المعلومات واكتمالها منذ وقت بدء إنشاء هذه المعلومات لحين حفظها بالشكل الإلكتروني. لا تشكل التعديلات والمستجدات على المعلومات مساساً بسلامة المعلومات إذا تم توثيقها وفق الأصول القانونية.
- تم حفظ المعلومات بشكلٍ يسمح بالرجوع إليها لاحقاً وعرضها بشكل مفهوم.
- تم حفظ البيانات التقنية التي تبين منشأ المعلومات ومصدرها والجهة المرسلة إليها وتاريخ إرسالها ووقته وكذلك استلامها.

المادة ١٠: الآثار الإلكترونية والوثيقة الورقية المطبوعة عن السند الإلكتروني

تعتبر الآثار الإلكترونية الصادرة عن شخص ما بمثابة بدء بينة خطية بوجه الشخص المذكور.

تكون للوثيقة الورقية المطبوعة عن السند الإلكتروني الآثار القانونية نفسها لصورة السند الورقي.

الباب الثالث: مسؤوليات مزود خدمات المصادقة الإلكترونية وصاحب الشهادة والطرف المعول/ المعتمد

المادة ١١: مزودو خدمات المصادقة الإلكترونية

لا تُخضع الدول الأعضاء تقديم خدمات المصادقة لأي ترخيص مسبق. مع مراعاة الفقرة الأولى، يمكن للدول المتعاقدة أن تعتمد أنظمة اختيارية تهدف إلى رفع مستوى خدمات المصادقة الإلكترونية المقدمة. جميع المعايير المتعلقة بهذه الأنظمة يجب أن تكون موضوعية وشفافة ومتناسبة وغير مميِّزة.

تسهر كل دولة عضو على وضع نظام ملائم لمراقبة مزودي خدمات المصادقة الإلكترونية العاملين على أراضيها والذين يصدرون شهادات مصادقة إلكترونية موصوفة للجمهور.

المادة ١٢: مسؤوليات مزود خدمات المصادقة الإلكترونية

تسهر الدول الأعضاء على أن مزود خدمات المصادقة الإلكترونية الذي يصدر شهادة مصادقة موصوفة أو يضمن مثل هذه الشهادة، يكون مسؤولاً عن الضرر الواقع على كل شخص طبيعي أو معنوي، يثق بشكل معقول بهذه الشهادة في ما خص:

- صحة جميع المعلومات الواردة في الشهادة الموصوفة في التاريخ الذي صدرت فيه، وتضمن الشهادة جميع المعلومات المفروضة قانوناً.
- ضمان أن بيانات إنشاء التوقيع الإلكتروني وبيانات التحقق منه قابلة للاستعمال بشكل متكامل، في الحالة التي ينتج مزود خدمات المصادقة هذين النوعين من البيانات، إلا إذا أثبت مزود خدمات المصادقة أنه لم يرتكب أي إهمال.

أن مزود خدمات المصادقة الإلكترونية الذي يصدر شهادة مصادقة موصوفة، يكون مسؤولاً عن الضرر الواقع على كل شخص طبيعي أو معنوي، يستند بشكل معقول على هذه الشهادة، وذلك من أجل عدم تسجيل إلغاء الشهادة، إلا إذا أثبت مزود خدمات المصادقة أنه لم يرتكب أي إهمال.

يعود لمزود خدمات المصادقة الإلكترونية أن يذكر في شهادة موصوفة القيمة القصوى للمعاملات التي يمكن استعمال الشهادة فيها، بشرط أن تكون هذه القيمة القصوى ظاهرة للغير.

لا يكون مزود خدمات المصادقة الإلكترونية مسؤولاً عن الأضرار التي تنتج عن تخطي هذه القيمة القصوى.

المادة ١٣: مسؤولية صاحب شهادة المصادقة

يكون صاحب شهادة المصادقة مسؤولاً:
- عن صحة المعلومات المتعلقة به والتي قدمها لمزود خدمات المصادقة وكذلك عن تحديثها عند الاقتضاء.
- عن عدم اتخاذ التدابير الضرورية في حال تعرض بيانات إنشاء التوقيع لما يثير الشبهة أو للانكشاف، ولاسيما عن إعلام مزود خدمات المصادقة بذلك.
- عند استعماله شهادة مصادقة إلكترونية موقوفة أو مُلغاة أو عن استعمال شهادة خلافاً لشروطها.

المادة ١٤: مسؤولية الطرف المعوّل/المعتمد

يكون الطرف المعوّل/المعتمد مسؤولاً:
- عن عدم اتخاذ خطوات معقولة للتحقق من موثوقية التوقيع الإلكتروني.
- عن عدم اتخاذ خطوات معقولة، إذا كان التوقيع الإلكتروني مُسنداً إلى شهادة مصادقة إلكترونية، لأجل التحقق من صلاحية الشهادة أو وقفها أو إلغائها وكذلك من وجود أي قيود على استعمال الشهادة.

الباب الرابع: الاعتراف القانوني بشهادات المصادقة الإلكترونية الأجنبية

المادة ١٥: الاعتراف القانوني بشهادات المصادقة الإلكترونية الأجنبية

إن شهادات المصادقة الإلكترونية المُسلَّمة على أنها موصوفة من قبل مزود خدمات مصادقة إلكترونية في بلد أجنبي، تُعتبر معادلة من الناحية القانونية لشهادات المصادقة الصادرة عن مزود خدمات مصادقة وطني:
- إذا كانت الشهادة ومزود خدمات المصادقة الإلكترونية يلبيان الشروط المذكورة في هذا الإرشاد وقد جرى الترخيص للمزود اختيارياً في إحدى الدول الأعضاء.
- أو إذا ضمنت الشهادة من قبل مزود خدمات مصادقة إلكترونية وطني، يلبي المتطلبات الواردة في هذا الإرشاد.
- أو إذا كانت الشهادة أو مزود خدمات المصادقة الإلكترونية معترفاً بهما تطبيقاً لاتفاق ثنائي أو متعدد الأطراف بين الدولة العضو ودول أخرى أو منظمات دولية.

الباب الخامس: العمليات المصرفية

المادة ١٦ : إصدار أوامر الدفع والتحويل الإلكترونية للأموال النقدية

يجب أن يسبق أية عملية دفع أو تحويل إلكتروني وضع اتفاق واضح ومفصل بين العملاء والمصارف والمؤسسات المالية على الشروط التنظيمية لأوامر الدفع الإلكترونية أو التحاويل الإلكترونية للأموال النقدية. ويجب أن تتضمن هذه الشروط تعيين تاريخ نفاذ أوامر التحويل الصادرة والواردة والعمولات المستوفاة وقيمة العملية المنجزة وحقوق فريقي العقد وموجباتهما والقواعد المختصة بالأخطاء في القيود أو القيود غير المشروعة وطرق الاعتراض المتاحة للعميل والإجراءات المتبعة في حال الدخول غير المشروع على حساب العميل وسعر الصرف المعتمد للعملة الأجنبية والقيود على العمليات.

يجب أن يكون الأمر بتحويل الأموال النقدية خطياً على دعامة ورقية أو إلكترونية. وإذا كان الأمر صادراً بالصورة الإلكترونية، يجب التصديق عليه من قبل هيئة رسمية أو خاصة تعتمدها كل دولة عضو.

المادة ١٧: الأنظمة الإلكترونية لأوامر الدفع أو التحاويل الإلكترونية

يجب أن تكون الأنظمة الإلكترونية المُستعملة قادرة على نقل أمر الدفع الإلكتروني أو التحويل الإلكتروني للأموال النقدية وعلى تخزين البيانات المتعلقة بالأمر للتمكن من الرجوع إليه. ويجب أن تتضمن هذه البيانات تحديداً للجهة المُرسلة واسم العميل وقيمة المبالغ وغيرها من العناصر المهمة اللازمة للتأكد من صحة أمر الدفع. كما يجب أن تتيح هذه الأنظمة الإلكترونية للطرف معطي الآمر بالدفع أو بالتحويل معرفة نتيجة هذا الأمر فوراً لجهة القبول أو الرفض وأسباب هذا الرفض.

المادة ١٨: مسؤولية العميل عن أوامر الدفع أو التحاويل الإلكترونية

لا يكون العميل مسؤولاً عن أي قيد جرى على حسابه

ناتج عن تحويل إلكتروني للأموال النقدية، بعد قيامه بإبلاغ المصرف أو المؤسسة المالية عن وجود إمكانية لدخول الغير إلى حسابه دون وجه حق، أو عن فقدان بطاقته المصرفية أو احتمال معرفة الغير لرمز التعريف الخاص به. وعلى العميل اتباع الأصول والإجراءات المتفق عليها مع المصرف أو المؤسسة المالية بشأن معاملة التبليغ. لا يستطيع العميل أن يلغين يرجع أأ أمر تحويل إلكتروني للأموال النقدية صادراً عنه بعد سحب المبلغ من حسابه.

المادة ١٩: مسؤولية المصرف أو المؤسسة المالية عن أوامر الدفع أو التحاويل الإلكترونية

يتحمل المصرف أو المؤسسة المالية مسؤولية عدم تنفيذ أمر التحويل كلياً أو جزئياً أو سوء تنفيذه، يتوجب عليه حينها، بالإضافة إلى التعويضات، إعادة المبالغ إلى العميل الآمر بالتحويل، إلا إذا كان عدم التنفيذ ناجماً عن خطأ أو نقص في التعليمات المعطاة من قبل الأخير.

في حال اعتراض العميل على عملية دفع إلكتروني أو تحويل إلكتروني للأموال النقدية، يتوجب على المصرف أو المؤسسة المالية أن تثبت أنه قد جرى قيد هذه العملية أصولاً وأنها لم تتعرض لأي خلل تقني في النظام المعلوماتي. ويُمنع تحميل العميل أية فوائد أو عمولات بغية تصحيح الأخطاء في قيود عمليات الدفع الإلكترونية أو قيود التحاويل الإلكترونية للأموال النقدية.

يجب على المصرف أو المؤسسة المالية تقديم معلومات منتظمة مفصلة لعملائها عن عمليات الدفع الإلكترونية أو التحاويل الإلكترونية للأموال النقدية.

المادة ٢٠: تعديل شروط التعاقد

يجب على المصرف أو المؤسسة المالية أن يبلغ العميل صراحة، قبل ١٠[٢٥] أيام على الأقل، عن رغبته بإجراء أي تعديل على شروط التعاقد لا سيما تلك المتعلقة بالعمولات أو القيود على العمليات.

إلا أنه في الحالات الاستثنائية، مثل تلك المتعلقة بالحفاظ على سلامة حساب العميل أو نظام الدفع الإلكتروني، يمكن للمصرف أو المؤسسة المالية فرض قيود على الخدمة المقدمة للعميل شرط أن يصار إلى إبلاغه فوراً بالقيود ودون تحميله أية أعباء مالية من جراء ذلك.

المادة ٢١: إصدار بطاقة مصرفية

يجب اعتماد الصيغة الخطية على دعامة ورقية أو إلكترونية لطلب الحصول على بطاقة مصرفية أو على العقد العائد لإصدارها.

المادة ٢٢: مسؤوليات المصرف أو المؤسسة المالية في ما خص البطاقات المصرفية

يجب على المصرف، أو المؤسسة المالية التي تصدر بطاقات مصرفية:

١- أن تُعلم صاحب البطاقة المصرفية بخصائص هذه البطاقة وبنظام استعمالها.

٢- أن تعطي صاحب البطاقة المصرفية معلومات التعريف التي تخوله استعمالها، مع ضمان سرية هذه المعلومات.

٣- أن تحفظ كشوفات مفصلة عن العمليات المنجزة بواسطة البطاقة في السنوات العشر الأخيرة.

٤- أن تتيح لصاحب البطاقة المصرفية إبلاغها عن فقدان البطاقة أو سرقتها وذلك بوسائل ملائمة.

٥- أن تمنع أي استخدام للبطاقة المصرفية فور الإبلاغ عن فقدانها أو سرقتها.

يقوم صاحب البطاقة بالتأشير على حسن إعلامه واستلامه الخصائص والمعلومات الخاصة بالبطاقة عبر توقيعه على وثيقة تفيد بذلك، وعليه أن يضع عبارة "عُلم مع الموافقة" بخط يده.

يكون المصرف أو المؤسسة المالية مسؤولين عن عدم تنفيذ الأوامر الصادرة عن صاحب البطاقة أو عن سوء تنفيذها، وكذلك عن العمليات المنفذة دون موافقته وعن الأخطاء في قيود حسابه. وعليهما أن يدفعا لصاحب البطاقة المبالغ المسحوبة من حسابه دون مبرر مشروع، أو بخلاف ما هو متفق عليه بالعقد.

المادة ٢٣: مسؤوليات صاحب البطاقة المصرفية

يلتزم صاحب البطاقة المصرفية باستعمال بطاقته المصرفية وفق الشروط المتفق عليها وبأن يتخذ كل الاحتياطات اللازمة لحماية البطاقة ومعلومات التعريف التي تتيح استعمالها.

لا يمكن لصاحب البطاقة المصرفية أن يرجع عن أمر الدفع الإلكتروني الصادر بواسطة هذه البطاقة.

لا يحق لصاحب البطاقة المصرفية أن يعترض على أي عملية دفع إلا في حال تعرضت بطاقته أو معلومات التعريف التي تتيح استعمالها للفقدان أو السرقة أو الاستعمال غير المشروع أو الاحتيالي أو في حال الخطأ الحاصل من قبل الجهة المصدرة للبطاقة.

يجب على صاحب البطاقة المصرفية، فور معرفته بذلك، إبلاغ المصرف أو المؤسسة بفقدانه بطاقته المصرفية أو بسرقتها، وبأي عملية تمت دون موافقته، وبأي خطأ في كشف حسابه . يتحمل صاحب البطاقة المصرفية، حتى تاريخ إبلاغه المصرف أو المؤسسة المالية، نتائج فقدان البطاقة أو سرقتها، وذلك في حدود سقف يتم تعيينه في التشريع الوطني. لكن هذا السقف لا يطبق في حال ارتكاب صاحب البطاقة المصرفية خطأ فادحاً أو إهمالا كبيراً، أو في حال عدم قيامه بالإبلاغ وفق الفقرة السابقة ضمن مهلة معقولة. لا يكون صاحب البطاقة المصرفية مسؤولاً عن:

١- عمليات الدفع المجراة بعد اعتراضه على استخدام البطاقة المصرفية.
٢- عمليات الدفع المنفذة عن بعد بشكل غير مشروع أو احتيالي، دون تقديم البطاقة المصرفية مادياً أو تحديد هوية الآمر بالدفع.
٣- تزوير البطاقة المصرفية إذا كانت مادياً في حيازته لدى إجراء العملية المعترض عليها.

وفي مثل هذه الحالات، يتولى المصرف أو المؤسسة المالية إعادة قيد المبالغ المعترض عليها في حساب صاحب البطاقة دون استيفاء أي عمولة أو نفقة، وذلك في خلال مهلة شهر من تاريخ استلام اعتراض صاحب البطاقة.

المادة ٢٤: النقود الإلكترونية

تصدر النقود الإلكترونية عن المصرف المركزي في الدولة أو عن مؤسسة مالية مرخص لها بذلك، وذلك بناءً لعقد يبرم مع العميل، على أن يتضمن العقد حقوق والتزامات الفريقين بشكل واضح.

تشكل وحدات النقود الإلكترونية ديناً على مُصدرها، يسقط بانقضاء مدة صلاحيتها، ويبرئ بالتالي ذمة مُصدرها.

المادة ٢٥: الشيك الإلكتروني

يجب أن يتضمن الشيك الإلكتروني جميع البيانات المطلوبة قانوناً بحسب القوانين المالية أو المصرفية، ويعود لكل دولة عضو أن تحدد ضمانات تقنية لضمان موثوقية الشيك الإلكتروني وصحته، وكذلك وضع قواعد تنظيمية مفصلة لكيفية استعماله. يمكن للمصارف العاملة في الدولة التعامل بالشيكات الإلكترونية.

المادة ٢٦: أحكام ختامية

على الدولة أن تضمن للإفراد حق الوصول إلى المعلومات العامة والمستندات الموجودة لدى المؤسسات والإدارات العامة، شرط أن لا يؤدي ذلك إلى التعرض للأمن الوطني أو سلامة الدولة أو علاقاتها الخارجية لدولة ذات الطابع السري أو مصالحها الاقتصادية العليا أو الحياة الخاصة للأفراد أو الأسرار المحمية بموجب نصوص قانونية خاصة أو أن ينتهك ذلك النظام العام في الدولة.

هوامش

٢١- التوقيع الالكتروني = التوقيع الرقمي

٢٢- مزود خدمات مصادقة الكترونية = مقدم خدمات التصديق (السعودية/سلطنة عمان/دبي)؛ مزود خدمات التصديق الالكتروني (سوريا)، مزود خدمة شهادات معتمد (البحرين)

٢٣- إن الإرشاد الحاضر هو في الأصل موجه إلى الدول الأعضاء في الإسكوا حتى تلك التي وضعت تشريعات خاصة بها للفضاء السيبراني

٢٤- ١٠ أيام هي المدة المُقترحة ويمكن تعديلها زيادةً او نقصاناً على ألا تقل عن الفترة اللازمة لتمكين صاحب العلاقة من تعديل شروط التعاقد.