الفصل الثالث

تدابير الحماية القانونية لاستخدام الذكاء الاصطناعي في مجال التوقيع الإلكتروني والذكي في التشريع الإماراتي وموقف الشريعة الإسلامية

تمهيد

اتخذت دولة الإمارات العربية المتحدة العديد من التدابير التشريعية والقانونية والإجرائية الهادفة للحماية القانونية لاستخدام الذكاء الاصطناعي في مجال التوقيع الإلكتروني والذكي في التشريع الإماراتي وموقف الشريعة الإسلامية والتي سيتم توضيحها من خلال هذا الفصل وتقسيمة إلى ثلاثة مباحث، خصصت المبحث الأول لمعرفة المصادقة الذكية للتوقيعات وشرعيتها، وافردت المبحث الثاني لإصدار شهادات التوقيع الإلكتروني وتزويد خدمات المصادقة الإلكترونية، أما المبحث الثالث لدراسة توقيع الوكيل الذكي على العقود الذكية.. وهي في التالي:

المبحث الأول: المصادقة الذكية للتوقيعات وشرعيتها

تمهيد

في هذا المبحث سنتناول ونبين المصادقة الذكية على التوقيع الإلكتروني الذكي في سياق الذكاء الاصطناعي واستخداماته من خلال تقسيم هذا المبحث إلى أربعة مطالب، خصص المطلب الأول: لمعرفة ماهية المصادقة الذكية للتوقيع الإلكتروني. ويكون المطلب الثاني: لدراسة موقف التشريعات المقارنة من المصدقة الذكية على التوقيع الإلكتروني، وخصص المطلب الثالث: لبيان أهمية شهادة المصادقة الذكية على التوقيع الإلكتروني، أخيراً المطلب الرابع: لمعرفة الحماية الجنائية للتوقيع الإلكتروني في الفقه الإسلامي وهي التالي:

المطلب الأول: ماهية المصادقة الذكية للتوقيع الإلكتروني

ترتب على التقدم التكنولوجي المعاصر في وسائل الاتصالات ونقل المعلومات وازدياد اللجوء إلى المعاملات الإلكترونية، ظهور طرق ووسائل حديثة في التعامل لا تتفق تماماً مع فكرة التوقيع بالمفهوم التقليدي القائم على دعامات ورقية مادية، ومن ثم لا يستوعب أساليب التعامل الحديث لهذا كان من الضروري الأخذ بالتوقيع بمفهومه الحديث، أي التوقيع الإلكتروني استجابةً لمتطلبات التعامل الحديث وليتوافق وطبيعة المعاملات القانونية وخاصة المعاملات الإلكترونية، فالتوقيع الإلكتروني يعدّ من الأساليب الحديثة سواء في المسائل المدنية أو التجارية أو الإدارية الأمر، الذي دفع التشريعات المختلفة للتدخل لضبط هذه الظاهرة القانونية الجديدة وإعطاء وصف لها من خلال تعريفها وبيان صورها المختلفة(١٩٣).

وبالتطبيق على العقد الإداري الإلكتروني نجد أنّه لا يختلف عن التوقيع الإلكتروني في بقية المعاملات الإلكترونية، فالإدارة تعتبر عن الإرادة بالتعاقد باستخدام التوقيع الإلكتروني على العقد الإلكتروني بعد انتهاء المناقصة الإلكترونية، كما يتم اعتماد التوقيع الإلكتروني لصاحب العطاء المتعاقد مع الإدارة، وبذلك يكون التوقيع الإلكتروني أداة للتعبير عن الإرادة في العقد الإداري الإلكتروني.

كما أدى التطور التقني المذهل في مجال نظم المعلومات والاتصالات إلى ظهور العديد من الصور التي يتخذها التوقيع الإلكتروني التي تختلف تبعاً لاختلاف الطريقة التي يتم بها، كما تختلف أيضاً من حيث توافر الثقة والأمان ووسائل الحماية التي تعتمد عليها الوسيلة التقنية المستخدمة فإذا كان التوقيع التقليدي يتم في صورة إمضاء أو بصمة إصبع أو ختم، فإنّ للتوقيع الإلكتروني أشكالاً متعددة

(١٩٣) عبد العليم، محمد حسين. (٢٠١٩). *إثبات العقد الإداري الإلكتروني*. الإسكندريّة مصر: دار الجامعة الجديدة. ص ١٥٠.

قد تتمثل في صورة حروف أو أرقام أو رموز أو أصوات أو نظام معالجة إلكتروني أو غيرها[١٩٤]،وعلى ذلك يعتبر هذا الشرط هاماً جداً لضمان سلامة المحرر الموقّع إلكترونياً بحيث يتم اكتشاف أي تعديل أو تبديل بالمحرر بعد توقيعه إلكترونياً وبحيث تتيح تقنية استخدام التوقيع الإلكتروني على المحرر من إمكانية كشف أي تلاعب بمضمون المحرر الموقع إلكترونياً[١٩٥].

نخلص مما سبق، أنّ التوقيع الإلكتروني في العقد الإداري الإلكتروني يتمتّع بالحجيّة في الإثبات ويرتبط ارتباطاً وثيقاً بدرجة الأمان والثقة التي يوفرها لدى المتعاقدين في العقد الإداري الإلكتروني (الإدارة والطرف المتعاقد معها)، ولتحقيق ذلك يجب أن يتم كتابة العقد الإداري الإلكتروني والتوقيع عليه باستخدام وسائل ونظم – كالتشفير والاستعانة بمقدمي خدمات التصديق الإلكتروني – من شأنها أن تحافظ على صحة العقد الإداري الإلكتروني المشتمل على التوقيع وتضمّن سلامته وتؤدي إلى كشف أي تعديل أو تبديل في بيانات العقد الإداري الإلكتروني الموقّع إلكترونياً. أي أنّه يتعين لصحة التوقيع الإلكتروني وجود رابطة أكيدة بين التوقيع والعقد الإداري الإلكتروني من شأنها أن تكفل تأمين ارتباط التوقيع بمضمون العقد الإداري الإلكتروني بشكل لا يقبل الانفصال. **أمّا عن** مواصفات التوقيع الإلكتروني الحكومي في العقد الإداري الإلكتروني والتي تحققها منظومة Gov-CA يمكن تلخيصها في النقاط التالية:

أ. أنّ هذا التوقيع على العقد الإداري الإلكتروني غير قابل للتزوير، ويرجع ذلك لاستخدام أنظمة التشفير الهجين التي تعتمد على تكنولوجيا هندسة الشفرة وتكنولوجيا المظاريف الرقمية التي صممت لاستخدام مجموعة من خوارزميات التشفير القياسية عالية السرية في وقت واحد.

---

(١٩٤) الروبي، أسامة روبي عبد العزيز. (٢٠٠٩). *حجيّة التوقيع الإلكتروني في الإثبات والادعاء مدنياً بتزويره*. مؤتمر المعاملات الإلكترونية: الإمارات العربية المتحدة. ص ٥٠٩.

(١٩٥) يوسف أحمد النوافلة. *الإثبات الإلكتروني في المواد المدنية والمصرفية*. مرجع سابق. ص ٨٤.

ب. يحتوي التوقيع الإلكتروني على العقد الإداري الإلكتروني الناتج على البصمة الزمنية الرقمية المؤهلة التي تحدد التوقيت الذي تم فيه على الوثيقة بالإضافة إلى قيام خوارزم التوقيع الإلكتروني بحماية هذه البصمة وإخفائها.

ج. يعتمد التوقيع الإلكتروني على العقد الإداري الإلكتروني في بنائه على تكنولوجيا شفرة المفتاح العام عالية السرية مستخدماً أطوال مفاتيح شفرة تحقق السرية العالية للتوقيع الناتج (لا تقل أطوال المفاتيح عن ٢٠٤٨ بت في الوقت الحالي).

د. لا يتقيد التوقيع الإلكتروني على العقد الإداري الإلكتروني بحجم المعلومات التي تحتويها الوثيقة.

هـ. لا يؤثر استخدام التوقيع الإلكتروني الرقمي على العقد الإداري الإلكتروني بكثافة على سرية نظام التوقيع. يتم تغيير القيمة الحسابيّة للتوقيع الإلكتروني لنفس الرسالة مع تغيير زمن التوقيع.

و. يرتبط التوقيع على العقد الإداري الإلكتروني حسابياً بالفرد نفسه ويتم ذلك من خلال منظومة شفرة التوقيع الإلكتروني الحكومية الخاصة بالفرد.

ز. يمكن التوقيع إلكترونياً على أي نوع من أنواع الملفات المرفقة بالعقد الإداري الإلكتروني مثل الرسائل أو الملفات (ملفات صوت – صور – فيديو – مكاتبات).

ح. القدرة الحسابية على التحقق من صحة التوقيع الإلكتروني على العقد الإداري الإلكتروني والفرد الذي قام به التوقيع(١٩٦).

أمّا مجالات استخدام التوقيع الإلكتروني الرقمي في العقود الإدارية الإلكترونية كثيرة منها:

(١٩٦) أنظر موقع وزارة المالية، سالف الإشارة إليه، متاح على الرابط:
www.Mof.gov.eg/MOFGallerySource/Arabic/E-signature/http://Introduction-E-signature.pdf

١) توقيع الرسائل الخاصة بتطبيقات المعاملات المالية الحكومية المختلفة المرتبطة بالعقد الإداري الإلكتروني وغيرها توقيعاً حكومياً ذات حجيّة قانونية طبقاً للمادة (١٤، ١٨) من قانون التوقيع الإلكتروني المصري.

٢) تشفير الرسائل الإلكترونية الخاصة بالعقد الإداري الإلكتروني إلى شخص بعينه أو مجموعة من الأشخاص والتحقق من شخصية المرسل بالإضافة إلى التحقق من توقيعه.

٣) إجراء التحويلات النقدية والتوقيع على الشبكات وتعاملات الأفراد المتعلقة بالعقد الإداري الإلكتروني مع عمليات البيع والشراء عبر شبكة الإنترنت.

٤) المدفوعات والمتحصلات الإلكترونية الخاصة بالعقد الإداري الإلكتروني شاملاً ذلك المرتبات والأجور والمعاشات ودافعي الضرائب والجمارك.

٥) منح شهادات التوثيق للمواقع التي تقوم بخدمة المتعاقدين مع الإدارة في العقد الإداري الإلكتروني مثل مواقع البنوك – الجامعات والمعاهد – مواقع التوثيق العقاري – مواقع البيع والشراء. أي أن تكون هذه المواقع موثقة بشهادات تصديق إلكتروني حكومية ليعطي كامل الثقة للأفراد للتعامل مع هذه المواقع.

٦) تفعيل تطبيقات الحكومة الإلكترونية فيما يخص العقد الإداري الإلكتروني عبر شبكة الإنترنت شاملاً ذلك كلاً من:

أ. تحرير الإقرارات الضريبية المتعلقة بالعقد الإداري الإلكتروني من خلال التأكد من شخصية صاحب الإقرار.

ب. الحصول على مستندات أو بيانات شخصيّة (مثل شهادة الميلاد أو الشهادة الدراسية) من خلال التأكد من شخصية صاحب المستند أو البيان.

ج. دفع الفواتير الشهرية (تليفون – كهرباء – غاز –..... إلخ).

د. حجز تذاكر السفر (طائرات – قطارات – أتوبيسات) من خلال التأكد من شخصيّة القائم بالحجز.

هـ. تحقيق نظام البنك الشخصي Home Banking من خلال التأكد من الشخص الذي يود الدخول إلى حسابه الشخصي صاحب الحساب وليس شخصاً آخر(١٩٧).

المطلب الثاني: موقف التشريعات المقارنة من المصدقة الذكية على التوقيع الإلكتروني

واشترطت المادة (١٣١٦/ ٤) من قانون التوقيع الإلكتروني الفرنسي رقم (٢٣٠/ ٢٠٠٠ م) الصادر في ١٣ مارس ٢٠٠٠ م: "أن يتم التوقيع باستخدام وسيلة آمنه لتحديد هوية الموقع تضمن صلته بالتصرف "الذي وقّع عليه" وقد أوضحت المادة (٢/١) م، قرار مجلس الدولة الفرنسي في مارس ٢٠٠١ م: "أن التوقيع يوكن صحيحاً إذا تم بوسيلة تكون تحت السيطرة المباشرة للموقع وحده دون غيره". واشترطت المادة (١٨/ ب) من قانون التوقيع الإلكتروني المصري لتمتع التوقيع الإلكتروني بالحجية في الإثبات: (سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني). ونصّت المادة (١٠) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المعدل على أنّه: (تتحقق من الناحية الفنية والتقنية سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني المستخدم في عملية تثبيت التوقيع الإلكتروني عن طريق حيازة الموقع لأداة حفظ المفتاح الشفري الخاص متضمنه البطاقة الذكية المؤمنة والكود السري المعترف بها). ويتّضح من النصوص السابقة أنّه يشترط لتمتع التوقيع الإلكتروني بالحجية في الإثبات أن يسيطر الموقع وحده دون غيره على الوسيط الإلكتروني(١٩٨).

---

(١٩٧) أنظر موقع وزارة المالية، سالف الإشارة إليه، متاح على الرابط:
www.Mof.gov.eg/MOFGallerySource/Arabic/E-signature/http://Introduction-E-signature.pdf

(١٩٨) عرفت المادة من (١/ د) من قانون التوقيع الإلكتروني الوسيط الإلكتروني بأنّه: "أداة أو أدوات أو أنظمة أو إنشاء التوقيع الإلكتروني وتحقق سيطرة الموقع على الوسيط الإلكتروني عن طريق حيازته لأداة حفظ المفتاح الشفري الخاص متضمنة البطاقة الذكية المؤمنة – الكود السري المعترف به".

أمّا إذا فقد الموقع سيطرته على الوسيط الإلكتروني وأصبحت بيانات إنشاء التوقيع الإلكتروني غير سرية، بحيث يعلمها أشخاص آخرون غير الموقع، فإنّ التوقيع الإلكتروني لا يعتبر حجة في الإثبات لأنّ تمييز هوية الموقّع وتحديد شخصيته بالرجوع إلى هذا التوقيع يكون مشكوكاً فيه(١٩٩)، وتتم عملية التوقيع الإلكتروني بين المتعاقدين في مجال المعاملات الإلكترونية عبر الإنترنت باستخدام تقنية شفرة المفتاحين العام والخاص، فكل طرف من المتعاقدين يجب أن يكون لديه مفتاحين متفردين أحدهما عام والثاني خاص ويجب أن يسيطر على هذين المفتاحين في أثناء قيامه بالتوقيع الإلكتروني. ويقصد بالمفتاح العام: أداة إلكترونية متاحه للكافة تنشأ بواسطة عملية حسابية خاصة وتستخدم في التحقق من شخصية الموقع على المحرر الإلكتروني، والتأكد من صحة وسلامة محتوى المحرر الإلكتروني. طبقاً للمادة (١١/١) من اللائحة التنفيذية.

أمّا المفتاح الشفري الخاص: فيقصد به أداة إلكترونية خاصة بصاحبها، تنشأ بواسطة عملية حسابية خاصة وتستخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية ويتم الاحتفاظ بها على بطاقة ذكية مؤمنه طبقاً لنص المادة (١٢/١) من اللائحة التنفيذية. ويحصل العميل (الموقع) على المفتاحين العام والخاص من جهة التصديق الإلكتروني التي تتولى عادة عملية إصدار هذه المفاتيح بناء على طلب العملاء ولديها نظام لحفظ البيانات الخاصة بالعملاء ومنها بيانات إنشاء التوقيع

(١٩٩) وهو ما أكد عليه القضاء الفرنسي في حكم محكمة استئناف (Besancon) في ٢٠ أكتوبر ٢٠٠٠ م والذي يعتبر أدلة حكم قضائي صدر في فرنسا بعد صدور قانون مارس ٢٠٠٠ م من الخاص بالتوقيع الإلكتروني وتتلخص وقائع هذه القضية وهي ما تعرف بقضية: (Snarl chalets Boasson/- Bernard G.) إنّ محامي أحد الأشخاص (الموقّع) احتج بالتوقيع الإلكتروني لموكله أمام المحكمة، وقدم في صحيفة دعواه بيانات هذا التوقيع السرية، التي من المفترض أنّ الموقّع هو الذي يعلمها وحده دون غيره، كما أنّ هذه البيانات كان يعرفها أيضاً أشخاص يعملون في مكتب المحامي وقد رفضت المحكمة الحكم بصحة هذا التوقيع الإلكتروني لأنّ دوره في إثبات شخصية الموقع أصبح مشكوكاً فيه، ولأنّ بيانات التوقيع خرجت من تحت يد الموقع إلى شخص آخر وهو محامية ومعاونوه في مكتبه. أشار إلى هذا الحكم: أيمن سعد سليم، التوقيع الإلكتروني، مرجع سابق، ص ٢٩.

الإلكتروني ولكنها لا تحفظ البيانات الخاصة بالعملاء ومنها بيانات إنشاء التوقيع الإلكتروني ولكنها لا تحتفظ بمفتاح الشفرة الخاص التي تصدرها للموقّع إلّا بناء على طلب من الموقّع وبموجب عقد مستقل يبرم بين الجهة المرخص لها بالتصديق الإلكتروني والموقّع (العميل) طبقاً لنص المادة (١٢/ ز) من اللائحة التنفيذية.

ويرجع السبب في ذلك إلى أنّ المفتاح الشفري الخاص يجب أن يكون سرياً ويتم تخزينه والاحتفاظ به على بطاقة ذكية مؤمنة ولا يعلمه إلّا الموقّع وحده دون غيره، وقد يحصل العملاء على هذه المفاتيح من خلال المؤسسة المالية التي سيتم بواسطتها تمويل التعاقد الإلكتروني.

وبحصول العميل الموقع على المفتاحين العام والخاص وحيازته لأداة حفظ المفتاح الشفري الخاص وهي البطاقة الذكية التي يخزن عليها المفتاح الشفري الخاص والكود السري المقترن بها، فإنّه يكون مسيطراً على الوسيط الإلكتروني وبالتالي يتحقق هذا الشرط من شروط حجية التوقيع الإلكتروني في الإثبات(٢٠٠).

ويعتبر التوقيع على المحرر بمثابة تعبير عن إرادة الموقّع برضائه بمضمون التصرف القانوني وإقراره به(٢٠١)، فمجرد التوقيع يفيد الرضا والالتزام طالما أمكن نسبة التوقيع إلى من ينسب إليه، وقد نصّت محكمة النقض بأنّ: "ثبوت صحة التوقيع بعد إنكاره صراحة كافية إعطاء الورقة حجيتها في أن صاحب التوقيع قد ارتضى مضمونها والتزم بها. مؤداه إعطاء الورقة حجيتها"(٢٠٢). وبالنسبة للتوقيع الإلكتروني يستفاد رضا الموقّع وقبوله بالالتزام الوارد بالمحرر من مجرد وضع توقيعه بالشكل الإلكتروني على البيانات

---

(٢٠٠) مبروك، ممدوح محمد علي مبروك. *مدى حجية التوقيع الإلكتروني في الإثبات*. مرجع سابق، ص ٦٤ وما بعدها، وابراهيم، خالد ممدوح، *التوقيع الإلكتروني*. مرجع سابق. ص ١٣٦.

(٢٠١) Catherine Guigou (2002). *Les contacts avec les consommateurs un outil de developpement du commerce Electronique*, presses Universitaires D'Aix- Marseille, p. 148.

(٢٠٢) نقض مدني، جلسة ٥ يونيو ٢٠٠١، *الطعن رقم ٥٦٤ لسنة ٧٠ ق*، مجلة المحاماة، العدد ٢ لسنة ٢٠٠٢م، ص ٧٠.

التي يحتويها المحرر الإلكتروني[٢٠٣]، وبالتالي إذا تم التوقيع الإلكتروني باستخدام نظام شفرة المفتاحين العام والخاص الذي يجعل المفتاح الخاص المقترن بالرقم السري محفوظاً على بطاقة ذكية مؤمنة في حوزة الموقّع ولا يعلمها غيره، فإنّه يدل على موافقته على البيانات والمعلومات التي وقّع عليها وأنّه يرغب في الالتزام بها بما يحقق الارتباط بين التوقيع الإلكتروني والموقع وحده دون غيره[٢٠٤].

ولقد ورد هذا الشرط بالمادة (٧/ أ) من قانون الأونسترال النموذجي بشأن التجارة الإلكترونية لعام ١٩٩٦ م، التي تنصّ على أنّ: "والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات" كما ورد نص المادة (٢/ أ) من قانون الأونسترال بشأن التوقيعات الإلكتروني لعام ٢٠٠١ م، التي تنصّ المادة (٢/ ٢) من التوجيه الأوروبي بشأن التوقيعات الإلكترونية لعام ١٩٩٩ م بالنسبة للتوقيع المؤهل" أن يكون مرتبطاً بالبيانات التي يشير إليها على نحو يؤدي إلى اكتشاف أي تغيير لا حق فيها". ونخلص مما سبق إلى أنّ التوقيع الإلكتروني وظيفة هامة في التعبير عن إرادة الموقع في العقد الإداري الإلكتروني بالالتزام والقبول بالبيانات الواردة في المحرر الإلكتروني، وأنّ قيام الموقّع بالتوقيع الإلكتروني يعتبر بمثابة أداة للتعبير عن رضا الموقع بمضمون المحرر الإلكتروني متى كان التوقيع موثقاً مؤمناً[٢٠٥]. ولكي يؤدي التوقيع وظيفته في إثبات إقرار الموقع بما ورد في مضمون المحرر يجب أن يكون هذا التوقيع متصلاً بالمحرر على نحو لا يمكن فصله عنه، وأن يكون هذا الاتصال مستمراً أو يمكن حفظة واسترجاعه بطريقة معلوماتية آمنة[٢٠٦]، وطوال الفترة الزمنية الكافية لاستخدامه في الإثبات[٢٠٧]

(٢٠٣) حجازي، عبد الفتاح بيومي. *إثبات المعاملات الإلكتروني عبر الإنترنت*. مرجع سابق. ص ٣٣٨.

(٢٠٤) مبروك، ممدوح محمد علي. *مدى حجية التوقيع الإلكتروني في الإثبات*. مرجع سابق. ص ١٤١.

(٢٠٥) النوافلة، يوسف أحمد. *الإثبات الإلكتروني في المواد المدنية والمصرفية*. مرجع سابق. ص ١٠٠.

(٢٠٦) عبد العزيز، مير حامد عبد العزيز. *التعاقد عبر تقنيات الاتصال الحديثة*. مرجع سابق. ص ٢٣٤.

(٢٠٧) حازم، صلاح الدين عبد الله. *تعاقد جهة الإدارة عبر شبكة الإنترنت*. مرجع سابق. ص ٣٤٢.

وإذا كان من المستقر عليه هو أن يوضع التوقيع في نهاية الكتابة التي تتضمنها المحرر حتى يكون منسحباً على جميع البيانات المكتوبة الوارد فيه ويعلن عن موافقة الموقع والتزامه بمضمونه[٢٠٨] إلّا أنّ وجود التوقيع في مكان آخر لا ينفى هذه الموافقة[٢٠٩]، وفي الواقع أنّ استخدام التوقيع التقليدي على المحرر الورقي المعدّ للإثبات يتحقق معه ارتباط التوقيع بالمحرر ارتباطاً مادياً وكيميائياً، بحيث لا يمكن فصل أحدهما عن الآخر إلّا بإتلاف الوثيقة أو إحداث تعديل في التركيب الكيمائي لكل من الأحبار ومادة الأوراق المستخدمة، وهو الأمر الذي يمكن كشفه بالمناظرة أو بالاستعانة بأهل الخبرة الفنية في هذا المجال[٢١٠]. أمّا بالنسبة للتوقيع الإلكتروني في العقد الإداري الإلكتروني فقد يبدو للوهلة الأولى أنّ هذا الأمر غير ميسور، حيث أنّ المحررات الإلكترونية تتخذ شكل رموز أو بيانات غالباً ما تكون على دعائم إلكترونية، بحيث يمكن إحداث تعديل وإدخال بيانات أخرى بما تتفق مع مصالح مستعمل جهاز الحاسب الآلي الذي يخضع لسيطرة مستخدمه دون أن يترك ذلك أي أُثر مادي يمكن أن يدل عليه[٢١١].

إلّا أنّ هناك جانباً من الفقه يرى أنّ هذه المخاوف يمكن التغلب عليها في ظل التطور التقني الهائل في مجال الاتصالات وتكنولوجيا المعلومات وما يبذله المختصون في هذا المجال من جهود كبية لتوفير أكبر قدر من الأمان والحماية والسرية للعقود الإدارية الإلكترونية، وأن هذه التقنيات يمكن أن توفر نفس الوظيفة التي يمكن أن يوفرها العقد الإداري التقليدي، حيث يمكن تسجيل وحفظ جميع البيانات الإلكترونية على دعائم الإلكترونية غير قابلة للتعديل وتتيح إمكانية استرجاعها عند الضرورة، وتتيح التوقيع عليها بوسائل مشفرة يصعب الوصول إليها ويمكنها أن تتصل بالعقد الإداري الإلكتروني

---

(٢٠٨) السنهوري، عبد الرزاق. مرجع سابق، ص ١٠٦.

(٢٠٩) عبد الحميد، ثروت. *التوقيع الإلكتروني*، مرجع سابق، ص ٢٩.

(٢١٠) جميعي، حسن عبد الباسط. *إثبات التصرفات التي يتم إبرامها عن طريق الإنترنت*. مرجع سابق، ص ٣١.

(٢١١) زهرة، محمد المرسي. *الحاسوب والقانون*. مرجع سابق. ص ٥٧.

على نحو مستحيل معه نقله أو تعديله، كما يمكن الاستعانة في هذا المجال بجهات التوثيق الإلكتروني التي يمكن أن تحفظ مثل هذه التصرفات بطريقة آمنة وسرية تضفي عليها نوعاً من الحماية والثقة لدى الأطراف المتعاقدة[٢١٢]. كما أشارت المادة (٢) من المرسوم الفرنسي رقم ٢٧٢ لسنة ٢٠٠١ الصادر تطبيقاً لأحكام المادة ١٣١٦ على هذا الشرط وأكدت على ضرورة أن يرتبط التوقيع الإلكتروني بالمحرر الموقعة بحيث أنّ أي تعديل يطرأ على المحرر بعد التوقيع عليه يتم اكتشافه. وفقاً على المادة (٢٠/ د) من القانون الإماراتي رقم (١) لسنة ٢٠٠٢ م بشأن التجارة الإلكترونية فإنّه يشترط في التوقيع الإلكتروني أن يرتبط بالرسالة الإلكترونية ذات الصلة به بطريقة آمنة تضمن سلامة التوقيع. كما أنّه وفقاً للمادة ١٨ من قانون تنظيم التوقيع الإلكتروني المصري رقم ١٥ لسنة ٢٠٠٤ م فإنّه يشترط في التوقيع الإلكتروني لكي تكون له حجية في الإثبات أن يتوافر فيه الشروط الآتية:

أ. ارتباط التوقيع بالموقع وحده دون غيره.

ب. سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.

ج. إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

تحدد اللائحة التنفيذية لهذا القانون الضوابط الفنية والتقنية اللازمة لذلك.

وبالرجوع للائحة التنفيذية نجد أنّ المادة (١١) نصّت على أن ".. يتم من الناحية الفنية والتقنية، كشف أنّ تعديل أو تبديل في بيانات المحرر الإلكتروني الموقع إلكترونياً، باستخدام تقنية شفرة المفتاحين العام والخاص، وبمضاهاة شهادة التصديق الإلكتروني وبيانات إنشاء التوقيع الإلكتروني بأصل هذه الشهادة وتلك البيانات أو بأية وسيلة مشابهة".

(٢١٢) عبد العزيز، سمير حامد. *التعاقد عبر تقنيات الاتصال الحديثة*. مرجع سابق. ص ٢٣٥.

وعلى ذلك يعتبر هذا الشرط هاماً جداً لضمان سلامة المحرر الموقع إلكترونياً بحيث يتم اكتشاف أي تعديل أو تبديل بالمحرر بعد توقيعه إلكترونياً وبحيث تتيح تقنية استخدام التوقيع الإلكتروني على المحرر من إمكانية كشف أي تلاعب بمضمون المحرر الموقع إلكترونياً[٢١٣].

نخلص مما سبق، أنّ التوقيع الإلكتروني في العقد الإداري الإلكتروني يتمتع بالحجية في الإثبات ويرتبط ارتباطاً وثيقاً بدرجة الأمان والثقة التي يوفرها لدى المتعاملين به في مجال العقود الإدارية الإلكترونية، ولتحقيق ذلك يجب أن يتم كتابة العقد الإداري الإلكتروني والتوقيع عليه باستخدام وسائل ونظم – كالتشفير والاستعانة بمقدمي خدمات التصديق الإلكتروني – من شأنها أن تحافظ على صحة العقد الإداري الإلكتروني المشتمل على التوقيع وتضمن سلامته وتؤدي إلى كشف أي تعديل أو تبديل في بيانات العقد الإداري الإلكتروني الموقّع إلكترونياً، أي أنّه يتعين لصحة التوقيع الإلكتروني وجود رابطة أكيدة بين التوقيع والمحرر من شأنه أن تكفل تأمين ارتباط التوقيع بمضمون العقد الإداري الإلكتروني بشكل لا يقبل الانفصال.

المطلب الثالث: أهمية اعتماد شهادة التوقيع الإلكتروني

فيما يتعلق بأحكام الاعتماد على التوقيع الإلكتروني، وكذلك شهادات المصادقة الإلكترونية على هذا التوقيع، فقد فصلت أحكامها في المادة ٢١ من هذا القانون، وتخلص هذه الأحكام في الآتي:

أ. القاعدة أنّ الشخص المعنى بالتوقيع الإلكتروني أو شهادة للصادقة الإلكترونية، يحق له الاعتماد عليهما، شرط أن يكون ذلك الاعتماد معقولاً أو مبرراً، بمعنى أن يكون ذلك الاعتماد له ما يبرره كأن يكون طرفاً في معاملة إلكترونية مع صاحب التوقيع أو صاحب الشهادة.

(٢١٣) النوافلة، يوسف أحمد. *الإثبات الإلكتروني في المواد المدنية والمصرفية*. مرجع سابق، ص ٨٤.

ب. من ناحية أخرى فإنّه يجب على ذلك الشخص الذي يعتمد على التوقيع الإلكتروني لطرف آخر ويكون التوقيع معززاً بشهادة مصادقة إلكترونية، فإنّه يجب على ذلك الشخص اتخاذ إجراءات التوثيق المحكمة أو غيرها من الإجراءات والخطوات اللازمة للتأكد من صحة الشهادة وصحة البيانات الواردة فيها، وما إن كانت لازالت سارية أم أنّها معلقة أو ملغاة، وكذلك بحث أية قيود تعطل قوة وتأثير هذه الشهادة. وعلى ذلك فإذا لم يتخذ هذه الخطوات، ولم ينجح في معرفة أنّ الشهادة ملغاة أو معلقة أو مقيدة بأي قيد آخر، فإنّ النتائج التي ستترتب على ذلك تخصه وحده هو دون غيره، ويتحملها هو دون غيره(٢١٤).

ج. من ناحية أخرى فقد أورد المشرّع بعض المعايير التي تساعد الشخص الذي يعتمد على شهادة المصادقة الإلكترونية أو التوقيع الإلكتروني، وذلك كإجراءات تبرر اعتماده المعقول في الاعتماد على أي منهما، وتخلص هذه الاعتبارات في الآتي:

١. طبيعة المعاملة المعنية، والتي قصد الشخص تعزيزها بالتوقيع الإلكتروني من عدمه لأنّ هناك بعض الصفقات، نظراً لقيمتها وأهميتها تتطلب ذلك التوقيع الإليكتروني وبعضها قد لا يتطلبه، وهناك بعض المعاملات لا تقبل التوقيع الإلكتروني حسب هذا القانون مثل عقود الزواج، وعقود التصرف في العقارات.

٢. قيمة أو أهمية المعاملة المعنية إذا كان ذلك معروفاً، وذلك لأنّ طبيعة بعض المعاملات من الأهمية بحيث أنّها تعتمد على التوقيعات الإلكترونية في إتمامها، وكذلك شهادات المصادقة حتى يستوثق الأفراد من صحة التوقيعات المهور بها هذه العقود فمثلاً في صفقة شراء طائرة أو مجموعة سيارات وقّع على عقدها بطريق التوقيع الإلكتروني يحق للطرف الآخر أن يستوثق

(٢١٤) العبدالله، طارق. (٢٠٢٢). *التوقيع الإلكتروني*. عجمان: الميار القانوني. ص ٢٩٩.

عن مدى صحة هذه التوقيعات، وذلك عن طريق المصادقات الإلكترونية الصادرة من طرف ثالث أو وسيط يضمن صحة التوقيع الإلكتروني عن طريق إصدار هذه الشهادة "شهادة المصادقة الإلكترونية".

د. مدى قناعة الشخص في الاعتماد على التوقيع الإلكتروني أو شهادة المصادقات، إذ يجب كذلك البحث فيما إذا كان ذلك الشخص الذي اعتمد على التوقيع أو شهادة المصادقة الإلكترونية، قد اتخذ الإجراءات المناسبة والمعقولة لكي يقرر بعدها حاجته للاعتماد على هذا التوقيع أو شهادة المصادقة الإلكترونية(٢١٥).

هـ. كذلك فإنّ أي توقيع إلكتروني، لا بد وأن يعزز بشهادة مصادقة على صحة ذلك التوقيع، وهذا الأمر يتطلب بحث من صاحب التوقيع فيما إن كان ذلك التوقيع معززاً بشهادة مصادقة أم لا، وكذلك على الطرف الآخر الذي يعتمد على هذا التوقيع لا بد أن يبحث عن هذه الشهادة، وقد نصّ على شهادة التصديق ضمن قانون الأمم المتحدة النموذجي في شأن التوقيع الإلكتروني.

و. أيضاً فإنّ التوقيع الإلكترونية وشهادة المصادقة الخاصة به قد يكون معرضة للإلغاء، وهنا يتعين بحث ما إن كان الشخص – طرف المعاملة الإلكترونية – كان يعلم بالإلغاء أو كان يجب عليه أن يعلم به أم لا، وذلك لأنّ عملية وجوب العلم بالإلغاء أو عدم وجوبه ترتب أثاراً قانونية هامة في حق ذلك الشخص.

ز. من ناحية أخرى فإنّ المعاملات أو الاتفاقيات السابقة ما بين منشئ الرسالة الإلكترونية –الشخص الذي صدر عنه الإيجاب في العقد – وذلك الشخص الذي اعتمد على التوقيع الإلكترونية أو الشهادة، تؤخذ في الحسبان لتقدير معقولية الاعتماد على أي منهما. كذلك فإنّ أي عرف تجاري

(٢١٥) العبدالله، طارق. التوقيع الإلكتروني. مرجع سابق. ص ٣٠٠.

يحكم معقولية اتخاذ إجراء الاعتماد على التوقيع أو الشهادة يجب كذلك النظر إليه بعين الاعتبار بوصف أنّ العرف مصدراً للتشريع في حالة عدم وجود نص قانوني مكتوب.

ح. وبالإضافة للعوامل السابقة التي تعد معياراً للتعرف على مدى معقولة الاعتماد على التوقيع الإلكتروني أو الشهادة الإلكترونية فقد أجاز المشرّع اللجوء إلى أي عامل آخر ذي صلة لبحث هذه المعقولة.

ومن ناحية أخرى فإنّ الفقرة الرابعة من المادة ٢١ من القانون، أوردت جزاءً على ذلك الشخص الذي يعتمد على التوقيع الإلكتروني أو شهادة التوثيق الإلكترونية، وكان ذلك الاعتماد غير مبرر أو غير معقول في ضوء الظروف المحيطة به، وإصابته أضراراً أو مخاطر من جراء ذلك، فإنّ هذا الشخص دون غيره هو الذي يتحمل مخاطر عدم صحة ذلك التوقيع أو عدم صحة هذه الشهادة.

تلعب جهة التصديق الإلكتروني دوراً مهماً في مجال التوقيع الإلكتروني بحيث تصدر شهادة التصديق الإلكتروني التي تحتوي على بيانات الموقع صاحب المفتاح العام التي يعتمد عليها الطرف الواثق في التعاقد، ولقد بيّنا أنَّ الأخطاء المرتكبة من قبل الموظفين في جهة التصديق ينجم عنها إصدار شهادةٍ فيها بياناتٍ خاطئةٍ عن الموقع مما يؤدي إلى حدوث أضرار قد تصيب الطرف المعول على تلك الشهادة، ويبرز حل هذه المشكلة عبر استخدام خبراء في مجال التقنية الذين تقلّ أخطاؤهم نظراً لخبرتهم في عملهم، وذلك لأنّ المتخصصين في مجال معالجة البيانات تقل أخطاؤهم نتيجة خبرتهم الكبيرة في مجال عملهم، وتعمد غالبية القوانين الناظمة لموضوع التوقيع الإلكتروني إلى إبراز مسؤولية جهة التصديق عن الأخطاء التي تصدر عنها عند ممارستها لمهامها [٢١٧].

(٢١٧) راجع ما تمَّ ذكره سابقاً حول مسؤولية جهة التصديق الإلكتروني، وخاصةً في مجال دقة المعلومات ومدى صحة البيانات المشتملة عليها شهادة التصديق الإلكتروني. ص ١٥٦ من هذه الرسالة.

المطلب الرابع: الحماية الجنائية للتوقيع الإلكتروني في الفقه الإسلامي

اهتمت الشريعة الإسلامية بحفظ الأموال، وأمرت باتخاذ الوسائل الكفيلة بحفظها، وشرعت العقوبات الرادعة لمن يتجرأ أو يحاول الاعتداء عليها بالتزييف أو التزوير أو غير ذلك من طرق الاعتداء. وقد حرم الله عز وجل أكل الأموال بالحيل الماكرة والطرق الملتوية، قال تعالى: (وَلَا تَأْكُلُوٓاْ أَمْوَٰلَكُم بَيْنَكُم بِٱلْبَٰطِلِ وَتُدْلُواْ بِهَآ إِلَى ٱلْحُكَّامِ لِتَأْكُلُواْ فَرِيقا مِّنْ أَمْوَٰلِ ٱلنَّاسِ بِٱلْإِثْمِ وَأَنتُمْ تَعْلَمُونَ) (البقرة، الآية: ١٨٨)، وأباحت الشريعة الإسلامية للإنسان المدافعة عن ماله إذا اعتدى عليه ولو باستعمال القوة وأن "من قتل دون ماله فهو شهيد"(٢١٨). وجعلت كل من تسبب في إتلاف مال منقوم بغير حق فإنّه يضمنه حتى لو كان ذلك بطريق الخطأ(٢١٩).

وهذه الأحكام وغيرها تبيّن مدى حرص الشريعة الإسلامية على إيجاد الحماية الجنائية للأموال ذاتها وعلى وسائل حفظها أيضاً. وبما أنّ الاعتداء على التوقيع الإلكتروني أو محاولة القيام بذلك يترتب عليه مخاطر كبيرة على المجني عليه خاصة، وعلى التجارة الإلكترونية عامة، حيث يؤدي إلى استخدام هذا التوقيع في المعاملات والحقوق المالية مما يسبب سرقة الأموال وضياعها فإنّ وضع الحماية الجنائية للتوقيع الإلكتروني يتفق مع مقاصد الشريعة الإسلامية في حفظ الأموال والحقوق الخاصة وحرمة الاعتداء عليها بأي وجه كان. والعقوبات في الشريعة الإسلامية ثلاثة أقسام:

١) **الحدود**: وهي العقوبات المقدرة شرعاً لحق الله تعالى، وهي حد الزنا والقذف والشرب والسرقة والحرابة والردة.

(٢١٨) متفق عليه، أخرجه البخاري في كتاب *المظالم باب من قتل دون ماله* برقم ٢٣٠٠، ومسلم في كتاب الإيمان برقم ٢٠٢.

(٢١٩) أنظر: في حفظ المال وأهميته: الإسلام مقاصده وخصائصه. لمحمد عقله ص ٢٠٩ – ٢٢٤.

٢) **القصاص**: وهي عقوبة مقدرة شرعاً لحق الأفراد، فمن حق المجني عليه أو ورثته أن يستوفيه أو يعفو عنه، وهو قسمان: في النفس، وفي الأطراف.

٣) **التعزيزات**: وهي عقوبات غير مقدرة شرعاً، وإنّما ترك شأنها وتقديرها إلى ولي أمر المسلمين[٢٢٠] فمن حكم الشارع أن جعل لولي الأمر مجالاً لينظر الجرائم التي تقع في عصره والتي تكون مخالفة لأحكام الشريعة ومقاصدها، فيضع لها العقوبات الرادعة الزاجرة مراعياً في ذلك نوع الجريمة والآثار المترتبة عليها[٢٢١]

والاعتداء على التوقيع الإلكتروني أو محاولة القيام بذلك يعتبر جريمة بحد ذاته، سواء كان بصنع برنامج لإعداد توقيع إلكتروني بدون إذن الجهة صاحبة الصلاحية، أو تزوير وتقليد التوقيع الإلكتروني، أو الدخول بطريق الغش على قاعدة بيانات تتعلق بالتوقيع الإلكتروني، أو غير ذلك من الجرائم التي تقع على التوقيع الإلكتروني. ووضع عقوبة محددة على هذه الجرائم هو من باب التعزير الموكول إلى ولي أمر المسلمين سواء بنفسه أو عن طريق السلطة التنظيمية في الدولة الإسلامية التي تتولى تحديد الجرائم ووضع العقوبات المناسبة لها. ويرى البعض أن الفقه الإسلامي يقرُّ صحة استخدام التوقيع الالكتروني وخاصة الرقمي منه لإثبات العقود الالكترونية، وهذا الأمر متفقٌ مع مبادئ الإثبات في الشريعة إذ أنها غير محصورةٍ بعددٍ معينٍ أو بشكلٍ محددٍ، وإنما يشمل كل وسيلةٍ يبين فيها الحق [٢٢٤]، فوسائل الإثبات

---

(٢٢٠) أنظر: في حفظ المال وأهميته: الإسلام مقاصده وخصائصه – لمحمد عقله ص ٢٠٩ – ٢٢٤.

(٢٢١) التشريع الجنائي الإسلامي. عبد القادر عودة ١٠/ ١٢٩.

(٢٢٤) الناصر عبد الله بن إبراهيم، *العقود الالكترونية* (دراسة فقهية مقارنة) بحث منشور على الموقع التالي (facu -faculty.ksu.edu.sa/11434/DocLib3/)، آخر زيارة في ٢٠١٠/١٠/٢٠

في الشريعة الإسلامية غير محصورةٍ في عددٍ معينٍ أو بشكلٍ محددٍ حسب القول الراجح، بل تشمل أي وسيلة يبين فيها الحق(٢٢٥) .

ولم تحدد الشريعة الإسلاميّة شكلاً ملزماً للكتابة، وكل ما اشترطته فيها أن تكون ظاهرة، واضحة، معبرة عن الإرادة، مرسومة بالطريقة التي جري بها العرف. ومن ثمّ فقد اتفق الفقهاء في الجملة على صحة العقود وانعقادها بالكتابة.(٢٢٦) وعرفها الإمام ابن تيميّة بأنها تتعدد بكل ما دل على مقصدها وتتنوّع بتنوّع اصطلاح الناس وكما تتنوّع لغاتهم. والدليل الكتابي يجد سنده في كتابه يقول الله تعالى ﴿يَا أَيُّهَا الَّذِينَ آمَنُوا إِذَا تَدَايَنتُم بِدَيْنٍ إِلَى أَجَلٍ مُّسَمًّى فَاكْتُبُوهُ ۚ وَلْيَكْتُب بَّيْنَكُمْ كَاتِبٌ بِالْعَدْلِ ۚ وَلَا يَأْبَ كَاتِبٌ أَن يَكْتُبَ كَمَا عَلَّمَهُ اللَّهُ ﴾ (سورة البقرة، الآية: ٢٨٢). صدق الله العظيم.

يمكن القول إنّ الشريعة الإسلاميّة، تستوعب تقنية التوقيع الإلكتروني. ذلك أنّ التوقيع بالإمضاء على المحرر حجة على الموقع (فمن كتب على نفسه أكبر حق وكتب في أسفل بخطة، فهلك الشهود فشهد رجلانْ عن أن ذلك خطة كان حجّة عليه) كما أنّ التوقيع بالختم على المحررات من شأنه أن يسبغ عليها الحجيّة، فقد كان النبي – صلّى الله عليه وسلّم – يبعث كتبه إلى الملوك وغيرهم

(٢٢٥) يعدد قانون البينات السوري أدلة الإثبات وهي ست أدلة: الكتابة . الشهود . الإقرار . القرائن . اليمين . الخبرة. أما في الفقه الإسلامي فيرى بعضهم أن وسائل الإثبات ليست محددةً ويجوز اللجوء إلى أي وسيلةٍ يبين فيها الحق أي اعتماد المذهب الحرفي حين يميل جانبٌ من الفقه إلى اعتماد المذهب المختلط الذي يعدد ويبين طرق الإثبات ويترك للقاضي الحرية في تقدير الأدلة ولن ندخل في النقاش حول أيّ رأي هو الأولى بالاعتبار وما هي حجج كل رأي ولكن نميل إلى الاتجاه الذي يمثله ابن القيم الذي يستند إلى عدم تحديد وسائل الإثبات، ولاشك أنَّ موقف قانون البينات السوري المعدد لطرق الإثبات المقبولة لا يتيح المجال مبدئيا للأخذ بالمحررات الالكترونية الموقعة الكولونيا . راجع في كل ما تقدم : علي محمد أحمد أبو العز، المرجع السابق، ص ٢٩٥ . ٢٩٦ . وأيضا محمد واصل، شرح قانون أصول المحاكمات، الكتاب الأول، الجزء الأول، منشورات جامعة دمشق،٢٠٠٦، ص ٥٤٣ وما يليها.

(٢٢٦) ممدوح مبروك. ٢٠٠٥. *مدى حجيّة التوقيع الإلكتروني في الإثبات*. دار النهضة العربيّة. طبعة. ص ٢٦، طه، أحمد حسام. ٢٠٠٠. *الجرائم الناشئة عن الحاسب الآلي*. كليّة الحقوق: جامعة طنطا. ص ٤٢٢، الفهوجي، *علي عبد القادر. الحماية الجنائيّة للبيانات المعالجة الكترونيّاً*. دراسة مقدمة إلى المؤتمر الذي عقدته كليّة الشريعة والقانون بجامعة الإمارات العربية المتحدة في موضوع "القانون والكومبيوتر والإنترنت"، وذلك بفندق هيلتون، العين، في الفترة من ١-٣ مايو ص ٣٨٦.

وتقوم بها حجته ولم يشاقه رسولاً بكتابه، ولا جري هذا في مدى حياته بل يدفع الكتاب مختوماً ويأمر بدفعه إلى المكتوب إليه.(٢٢٧)بل إنّ بعض الفقهاء رأى وجوب الختم على المحرر الرسمي ككتاب القاضي، وبما يحول دون تغييره أو تبديله(٢٢٨). وقد اتفق الفقهاء على حجيّة الرسائل في الإثبات بين الغائبين سواء أشهد عليها، أو لم يشهد، أخذا بالقاعدة المشهورة أن الكتاب بين الغائبين كالخاطب بين الحاضرين(٢٣٩).

ومؤدى ما تقدم أنّ أحكام الشريعة الإسلاميّة في عمومها تستوعب فكرة التوقيع الإلكتروني فلم تحدد الشريعة الإسلاميّة شكلاً محدداً للكتابة أو المحرر، كما أنها أجازت التوقيع بالإمضاء أو الختم وأسبغت عليه الحجيّة، ما لم ينكره صاحبه، وهنا لم يكن من بديل في ظل مقتضيات ذلك العصر إلا الاستعانة بالعدل من الشهود للشهادة عما إذا كان ذلك هو خط الموقع من عدمه. ولما كان التوقيع الإلكتروني هو تعبير عن تطوّر تكنولوجي، ومن شأنه أن يحقق وظائف التوقيع التقليدي، ومن ثمّ، فإن أحكام الشريعة الإسلاميّة لا تتعارض على الإطلاق مع تلك الفكرة.

المبحث الثاني: إصدار شهادات التوقيع الإلكتروني وتزويد خدمات المصادقة الإلكترونية

تمهيد

حيث نهدف في هذا المبحث لبيان إصدار شهادات التوقيع الإلكتروني وتزويد خدمات المصادقة على التوقيع الإلكتروني الذكي عبر برامج وتقنيات المصادقة الإلكترونية من خلال الثلاثة المطالب التالية: فأتناول في المطلب الأول لبيان الحماية عن طريق تزويد خدمات المصادقة على العقود

(٢٢٧) التاج والأكليل للموافق. بهامش مواهب الجليل ج ٦، ص ١٨٧، الطرق الحكمية، الجزء السادس، ص ٢٠٥، ٢٠٠٦ م.

(٢٢٨) الهذايب للمرغيناني. (١٩٦٥). *شرح بداية المتنبي*. ج ٣. ص ١٠٦. والميسوط للسرخسي، ج ١٨، ص ١٧٣.

(٢٣٩) مبروك، ممدوح. (٢٠٠٥). *مدى حجيّة التوقيع الإلكتروني في الإثبات*. مصر: دار النهضة. ص ١١٨.

الإلكترونية التي تحتوي التوقيع الذكي. وأخصص المطلب الثاني لتوضيح الالتزامات الشركات بتأمين البيانات اللازمة لحماية التوقيع الإلكتروني، ويكون المطلب الثالث لدراسة موقف التشريعات المقارنة، وهي في التالي:

المطلب الأول: الحماية عن طريق تزويد خدمات المصادقة على العقود الإلكترونية التي تحتوي التوقيع الذكي

لا شكّ أنّ أحد أهم عناصر الحماية الوقائيّة للتوقيع الإلكتروني هو تنظيم التزامات قانونيّة على عاتق الأطراف ذات الصلة به سواء تعلق الأمر بطرفي المعاملة أو بالجهات التي تلعب دوراً في إنشائه وإدارته. فبقدر التزام كل طرف من الأطراف المتعاملة بقدر ما تتضاءل المخاطر الناجمة عن التوقيع الإلكتروني(٢٢٢).

وبديهي أنّنا عندما نتناول تلك الالتزامات إنّما نعوّل على ما لها من أثر وقائي في تجنب تعرض التوقيع الإلكتروني للاعتداء، فضلاً عمّا يحققه ذلك من تحقيق مبدأ حماية المستهلك خاصة في الأحوال التي يكون فيها أيّاً من طرفي العقد غير متخصص، حيث يجب حمايته من الشروط التي ينفرد بها الطرف المتخصص.(٢٢٣) ولذلك، ليس غريباً أن نجد التشريعات الوطنيّة وقد سايرت القانون النموذجي والتوجيه الأوروبي في فرض التزامات على عاتق مقدمي خدمات التصديق وضبط القواعد القانونيّة لمسؤوليتهم عند مخالفتها.(٢٢٤)، وأخيراً، فإنّ على الموقع والمتعاقد معه التزامات قانونيّة يتعيّن

(٢٢٢) رمضان، مدحت. (٢٠٠١). *الحماية الجنائيّة للتجارة الإلكترونيّة*. مصر: دار النهضة العربيّة. ص ١٢٢ – ١٢٤.

(٢٢٣) سليم، أيمن سعد. (٢٠٢١). *التوقيع الإلكتروني، دراسة مقارنة*. مصر: دار النهضة العربيّة. ص ٢٢.

(٢٢٤) قنديل، سعيد. (٢٠٠٦)، *التوقيع الإلكتروني ماهيّته صورة وحجيته في الإثبات بين التداول والاقتباس*. مصر: دار الجامعة الجديدة.ص ٩٥.

مراعاتها، وفي المجمل يمكن أن نطلق على تلك الالتزامات وصـــف التدابير الوقائيّة للحماية من مخاطر التوقيع الإلكتروني وسنتناول ذلك تفصيلاً على النحو التالي:

أولاً/ التزامات مقدمي خدمات التصديق(٢٢٥):

نصّت المادة التاسعة من القانون النموذجي بشأن التوقيع الإلكتروني ٢٠٠١ على أنّه حيثما يوفر مقدمي خدمات التصديق خدمات لتأييد توقيع إلكتروني يجوز استخدامه لإعطاء مفعول قانوني بصفته توقيعاً، يتعيّن على مقدم خدمات التصديق (أ) أن يتصرّف وفقاً للتأكيدات التي يقدمها بخصوص سياساته وممارساته. (ب) وأن يولي قدراً معقولاً من العناية لضمان دقة واكتمال كل ما يقدمه من تأكيدات جوهرية ذات صلة بالشهادة طيلة دورة سريانها (ج) وأن يوفر وسائل يكون الوصول إليها متيسراً بقدر معقول وتمكن الطرف المعول من التأكد من الشهادة ومما يلي: (١) هويّة مقدم خدمات التصديق. (٢) أنّ الموقع المعينة هويته في الشهادة كان يتحكم في بيانات إنشاء التوقيع في وقت إصداره الشهادة (٣) أنّ بيانات إنشاء التوقيع كانت صحيحة في وقت إصدار الشهادة أو قبله. (د) وأن يوفر وسائل يكون الوصول إليها متيسراً بقدر معقول وتمكن الطرف المعوّل من التأكد عند الاقتضاء من الشهادة أو مما يلي:

(١) الطريقة المستخدمة في تعيين هوية الموقع. (٢) وجود أي تقييد على القرض أو القيمة التي يجوز أن تستخدم من أجلها بيانات إنشاء التوقيع أو أن تستخدم من أجلها الشهادة. (٣) أنّ بيانات إنشاء التوقيع صحيحة ولم تتعرّض لما يثير الشبهة. (٤) وجود أي تقييد على نطاق أو مدى المسؤوليّة التي اشترطها مقدم خدمات التصديق. (٥) ما إذا كانت هناك وسائل متاحة للموقع لتقديم شعار بمقتضى

(٢٢٥) Theo Hassler**.** 1999**:** *Droit de l'audio visuol l'internet Dalloz* – A.V.. P1188 et. Ss.

الفقرة أ/ ب من المادة الثامنة من هذا القانون وأن يستخدم في أداء خدماته نظماً وإجراءات وموارد بشريّة جديرة بالثقة[٢٢٦]

كما أوجبت المادة العاشرة على مقدمي خدمات التصديق ضرورة مراعاة الثقة في الموارد البشرية وجودة نوعية نظم المعدات والبرمجيات وإجراءات تجهيز الشهادات وطلبات الحصول على الشهادات والاحتفاظ بالسجلات وإتاحة المعلومات للموقعين المعينة هويتهم في الشهادات وللأطراف المحتمل تعويلها.

وقد ساير التوجيه الأوروبي ٩٣ لسنة ٩٩ بشأن التوقيع الإلكتروني[٢٢٧] ذلك النهج حيث نصّت المادة الثامنة من أنّه يجب أن تتعهد الدول الأعضاء بالتزام مقدمي خدمات التصديق بالسريّة والثقة لكل المعلومات ذات الطابع الشخصي، كما استعرضت المادة ٩/٢ ضرورة أن تتضمن الشهادة الإلكترونيّة بيانات مقدم خدمات التصديق والدول التي أنشأ بها لممارسة اختصاصه (٢) واسم الموقع الفعلي أو اسمه المستعار الذي يمكن التحقق منه. (٣) المفتاح العام الذي يمكن الوصول من خلاله إلى المفتاح الخاص للموقع والذي يخضع لرقابة هذا الأخير (٤) تحديد مدة صلاحيّة الشهادة (٥) تحديد قيمة الصفقات التي يمكن استخدام الشهادة بشأنها. ووفقاً للتوجيه الأوروبي ٢٠٠٠/ نصت المادة ٤٠ على التزام الدول الأعضاء بتوحيد المعاملة القانونية بالنسبة لمسؤوليّة الوسطاء الذين يقدمون خدمة الإنترنت وأنّه يجب على الوسطاء الكف عن أي أعمال غير مشروعة ووقفها.[٢٢٨]

---

(٢٢٦) UNCITRAL Model Law Electronic Signatures with Guide to Enactment 2001 UNITED NATIONS New York, 2002 Article 9. Conduct of the certification service provider.

(٢٢٧) تمام، حسام طه. (٢٠٠٠). *الجرائم الناشئة عن استخدام الحاسوب – (الحماية للحاسوب). دراسة مقارنة*. مصر: دار النهضة القاهرة. ص ١٥٦.

(٢٢٨) رمضان، مدحت رمضان. (٢٠٠١). الحماية *الجنائيّة للتجارة الإلكترونيّة*. مصر: دار النهضة العربية. ص ١٢٢ – ١٢٤.

ومؤدي ما تقدم أن أخص التزامات مقدم خدمات التصديق في ضوء القانون النموذجي والتوجيه الأوروبي، تتعلق بمراعاة الدقة والثقة عند إصدار الشهادة الإلكترونيّة وفترة سريانها، وأن يراعى في ذلك اعتبارات الحيطة والحذر، وأن يتخذ من التدابير ما يخوّل للمعمول الوقوف على صحة الشهادة وجهة إصدارها ومدة سريانها وشخص الموقع وكذا وجود قيود محددة على التزامات مقدم الخدمات تحدد نطاق مسؤوليته على وجه الدقة. ومن ثمّ فقد حظر المشرّع على مقدم خدمات التصديق إفشاء سرية البيانات الشخصية للموقع. غير أنّ هذا الالتزام محدود بما نصّ عليه المشرّع من بيانات خاصة بالموقع، يتعيّن الإفصاح عنها دون أن يشكّل ذلك إخلالاً بالتزام السريّة، كما أنّ من الأحوال الجائز فيها إفشاء أسرار الموقع حالة صدور حكم قضائي بإفشاء بيانات الشهادة والموقع، بل إنّ المشرّع التونسي قد عاقب جنائيّاً على الإخلال بذلك الالتزام.

ومن الالتزامات التي استلزمها المشرّع التونسي على مقدّم خدمات التصديق، أن يسلم صاحب شهادة المصادقة الإلكترونيّة تلك الشهادة بعد التحقق من توافر الشرائط التي تطلبها في كراس شروط الشهادة، وهي عبارة عن، ملف بطلبات الشهادات وآجال لدراسة الملفات، والتحقق من توافر الإمكانيات الماليّة والبشريّة، وتأمين التفاعل المتبادل للأنظمة، والإفصاح عن المعلومات فيما لا يشكّل إخلالاً بالسريّة[٢٢٩].

كما أوجب الفصل ١٣ على مزوّد خدمات التصديق التزاماً باستعمال وسائل موثوق بها تقنياً عند إصدار وتسليم وحفظ الشهادات وكذا اتخاذ الوسائل اللازمة لحمايتها من التقليد والتدليس. بل إنّه اعتبر الإخلال بذلك الالتزام جريمة عاقب عليها بموجب الفصل ٤٥.

(٢٢٩) أبـو هيبـة، نجـوى. (٢٠٠٣). *التوقيـع الإلكـتروني، تعريفـه، حجيّتـه. دراسـة مقدمـة لمـؤتمر الأعمـال المصـرفيّة*. دبي: المجلّد الأوّل ص ٤٧٨.

ثانياً/ موقف المشرّع المصري من التزامات مقدمي خدمات التصديق:

عالجت المادة ١٩ من قانون التوقيع الإلكتروني المصري الالتزامات التي تقع على عاتق من يزاول نشاط إصدار شهادات التصديق الإلكتروني. وأجملتها في أن يكون قد رخص له من الهيئة بذلك(٢٣٠). ووضعت ضوابط عامة لتلك الالتزامات وأحالت إلى اللائحة التنفيذيّة في تحديد الإجراءات والقواعد والضمانات وأهمها عدم إبرام أي عقد مع العملاء إلّا بعد اعتماد نموذج العقد من الهيئة المختصة. وأن يقدّم الضمانات والتأمينات لتغطية أي أضرار أو أخطار تتعلّق بذوي الشأن في حالة إنهاء الترخيص لأي سبب أو لتغطية أي إخلال بالتزام تضمنه الترخيص وأن تكون شهادة التصديق الإلكتروني(٢٣١) متضمنة:

١- ما يفيد صلاحيّة هذه الشهادة للاستخدام للتوقيع الإلكتروني.

٢- موضوع الترخيص الصادر للمرخص له موضحاً فيه نطاقه ورقمه وتاريخ إصداره وفترة سريانه.

٣- اسم وعنوان الجهة المصدرة للشهادة ومقرها الرئيسي وكيانها القانوني والدولي التابعة له إن وجد.

٤- اسم الموقع الأصلي أو اسمه المستعار أو اسم شهرته وذلك في حالة استخدامه لأحداها.

٥- صفة الموقع.

٦- المفتاح الشفري العام الحائز للشهادة المناظرة للمفتاح الشفري الخاص.

٧- تاريخ بدء صلاحية الشهادة وتاريخ انتهائها.

٨- رقم مسلسل الشهادة.

---

(٢٣٠) فهمي، خالد مصطفى. (٢٠٠٧). *النظام القانوني للتوقيع الإلكتروني في ضوء التشريعات العربية والاتفاقات الدولية*. مصر: الجامعة الجديدة. ص ٨٨.

(٢٣١) نفس المرجع السابق. ص ٨٨.

٩- التوقيع الإلكتروني المخصص لقائمة الشهادات الموقوفة أو الملغاة ويجوز أن تشمل على أي من البيانات الآتية عند الحاجة:

أ. ما يفيد اختصاص الموقع عند الحاجة.

ب. حد قيمة التعاملات المسموح بها في الشهادة.

ج. مجالات استخدام الشهادة.

ومن الالتزامات الملقاة على عاتقه أيضاً الالتزام بتأمين المعلومات وحماية سريّة البيانات وخصوصيتها بمستوى حماية لا يقل عن المستوى المذكور في المعايير والقواعد المشار إليها في الفقرة/ د من الملحق الفني والتقني(٢٣٢). وأن يكون من شأن الشهادة أن تحقق الربط بين التوقيع وبين الموقع على نحو يطمئن إلى سيطرته على التوقيع، كما يجب أن يلتزم بسلامة شهادات التصديق الإلكتروني وتوافقها ١- مع بيانات إنشاء التوقيع. ٢- مكان ومضمون المحرر الإلكتروني الموقع بدقة. ٣- سهولة العلم بشخص الموقع الأصلي أو المستعار أو الشهرة. والالتزام بما عساه يفرض عليها في الترخيص من شرائط أخرى. ومن أهم الالتزامات التي أشارت إليه اللائحة التنفيذيّة هذا الالتزام مزود خدمات التصديق بإيقاف الشهادة حال فقدها أو تعييبها أو سرقتها والاستعانة بالكوادر الفنيّة والبشريّة الماليّة اللازمة لإسباغ الثقة والأمان والسريّة والخصوصيّة على تلك الشهادة(٢٣٣)

ثالثاً/ التزام الجهة مانحة التصديق:

تلتزم السلطة المختصة بمنح الترخيص وفقاً لقانون الأونسترال النموذجي بضمان الشروط التي تقتضيها سياسته العامة في إنشاء وإدارة التوقيع الإلكتروني والتي من شأنها أن تحقق شرائط ووظائف

(٢٣٢) عبد الغني، شيماء. (٢٠٠٥). *الحماية الجنائيّة للتعاملات الإلكترونيّة*. (رسالة دكتوراه). كليّة الحقوق. مصر: جامعة المنصورة. ص ١١٤.

(٢٣٣) مادة ٧ من اللائحة التنفيذيّة للقانون ١٤ لسنة ٢٠٠٥.

التوقيع. ففي حين أنّ اختيار مقدمي خدمات التصـــديق قد يتوقف على عوامل عديدة منها قوّة المفتاح العمومي الذي يجري اسـتعماله وهوية مسـتعمله، فإنّ السـلطة المختصـة يجب أن توفر نظام للمعاملة بالمثل بالنسبة لمقدم خدمات التصديق فيما يتعلق باستمرار الامتثال لشروط السياسة العامة والأمان الصادر منها.(٢٣٤)

وفي ضوء ذلك، فإنّ قانون الأونسترال يلزم السلطة المختصة بالترخيص بإسباغ الرقابة على مقدمي خدمات التصديق، للتحقق من توافر الكوادر البشرية والمالية والتقنية ومدى التزام جهات التصديق بالشرائط الواردة بالترخيص وأخصها السرية والأمان(٢٣٥). كما ساير التوجيه الأوروبي ذلك النهج، حيث نصّت المادة الثالثة من الباب السادس منه على ضرورة أن يكون للدولة أو للسلطة المختصة أن تراقب مقدمي خدمات التصديق التي نشأت على إقليم هذه الدولة، إلّا أنّها تركت للدول الأعضاء اتخاذ التدابير اللازمة لإسباغ الرقابة وفقاً للقانون الداخلي.

بينما أنشأ المشرّع المصري بمقتضى نص المادة الرابعة من القانون ١٥ لسنة ٢٠٠٤ م هيئة تنمية تكنولوجيا المعلومات وخولها الترخيص لأي شخص طبيعي أو معنوي بمزاولة نشاط التصديق الإلكتروني، وأياً ما كان الأمر، فإنّ التزامات هذه الهيئة تتمثل في:

أ. إصدار وتحديد التراخيص اللازمة لمزاولة خدمات التصديق.

ب. تحديد الضوابط الفنيّة والمواصفات القياسيّة لإصدار وإدارة التوقيع الإلكتروني.

ج. اتخاذ الإجراءات اللازمة بشأن الشكاوى بأنشطة التوقيع الإلكتروني وتكنولوجيا المعلومات.

د. تقييم الجهات العاملة بأنشطة تكنولوجيا المعلومات وتحديد مستوياتها بحسب نتائج التقييم.

---

(٢٣٤) فهمي، خالد مصطفى. مرجع سابق. ص ٨٨.

(٢٣٥) IRS Rev. Proc. 98-25, Section 8.01 The notice must identify the affected records and include a plan that describes how, and what time frane, the taxpayer proposes to replace or restore the affected records in a way that assures that they will be capacle of being processed. Rev Proc. 98-25, Sectinv 8,02.

وقد نصّ المشرّع التونسي في الفصل ٥٢ من قانون المبادلات الإلكترونيّة على أنّه يعاقب طبقاً لأحكام الفصل ٢٥٤ من المجلة الجنائيّة مزود خدمات المصادقة الإلكترونية وأعوانه الذين يفشون أو يحثون أو يشاركون في إفشاء المعلومات التي عهدت إليهم في إطار تعاطي نشاطاتهم باستثناء تلك التي رخص صاحب الشهادة كتابياً أو إلكترونياً في نشرها أو الإعلام بها أو في الحالات المنصوص عليها في التشريع الجاري به العمل.

رابعاً/ موقف المشرع الإماراتي من التزامات مزود خدمة التصديق:

عرف المشرع الإماراتي في المادة الأولى من المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ مزود الخدمة بأنه:" مزود الخدمة: كل شخص طبيعي أو اعتباري عام أو خاص يزود المستخدمين بخدمات الوصول بواسطة تقنية المعلومات إلى الشبكة المعلوماتية."

وتنص المادة (٤٠) من القانون الإماراتي على أنه:" يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (١,٠٠٠,٠٠٠) مليون درهم، أو بإحدى هاتين العقوبتين، كل من استولى لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند، وذلك بالاستعانة بأي طريقة من الطرق الاحتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات."

المطلب الثاني: التزامات الشركات بتأمين البيانات اللازمة لحماية التوقيع الإلكتروني

تبرز مسألة تأمين البيانات كنتيجة منطقيّة للكثير من عمليات خرق التأمين. ذلك أنّ الاعتماد على بنية تحتية من أجهزة الكمبيوتر قد يؤدي إلى نقاط ضعف ملحوظة يمكن بدورها أن يلحق أضراراً بالغة.

ومن هنا برزت أهميّة فرض التزامات على جميع جهات العمل لتنفيذ تدابير تأمين المعلومات لحماية بياناتها الخاصة والإفصاح عن أي خرق قد يحدث لنظم التأمين، ونتيجة للالتزام بتوفير التأمين، قد تجد الشركات العامة نفسها ملزمة بواجب الإفصاح عن مدى استعداد نظم التأمين بها.(٢٣٦)

وقد كان السبب الرئيسي المذكور وراء عدم الإبلاغ عن تلك الخروقات لجهات إنفاذ القانون، خوفاً من الآثار السلبيّة للإعلان عنها. ويعدّ ذلك من المخاوف الخاصة للشركات العامة. فعلى سبيل المثال، تعرّضت شركة Choice point لتراجع بما يزيد على ٢٠٪ في سعر أسهمها دفعة واحدة عقب ما تمّ الإفصاح عنه في حادث اختراق نظم التأمين مما قلّل من حافز الشركة في تنفيذ تدابير تأمين جيدة.(٢٣٧) وبناء على ذلك، فإنّ هناك التزامين قانونيين أساسيين على كافة الأعمال اليوم فيما يتعلّق بتأمين المعلومات:

- واجب توفير نظم تأمين معقولة لجميع بيانات الشركة.
- واجب الإفصاح عن أي خرق لنظم التأمين التي تتضمن بيانات شخصيّة حساسة.

وفي ضوء ذلك سوف نتناول واجب توفير نظم تأمين معلومات الشركات والمعيار القانوني لتأمين المعلومات، وسبل وضع برنامج تأمين لإدارة المخاطر والسيطرة عليها، وواجب الإفصاح عن مدى استعداد نظم التأمين وذلك على النحو التالي:

---

(٢٣٦) IRS Rev. Proc. 98-25, Section 8.01 *The notice must identify the affected records and include a plan that describes how*, and what time frane, the taxpayer proposes to replace or restore the affected records in a way that assures that they will be capacle of being processed. Rev Proc. 98-25, Sectinv 8,02.

(٢٣٧) Thomas J .2005. *Smedinghoff "Security Breach Notification Law – Defining a New Corporate Obligation*," World Data Protection Report (October).

أولاً/ واجب توفير نظم تأمين معلومات الشركات:

وفقاً للقانون الأمريكي فإنّ الالتزامات القانونيّة للشركات بتنفيذ تدابير تأمين المعلومات، منصوص عليها في مجموعة من القوانين الفيدراليّة وقوانين الولايات، واللوائح، وأوامر الإنفاذ الحكوميّة. والتي تلزم الشركات بتنفيذ تدابير تأمين المعلومات لحماية بيانات شخصيّة خاصة بالأفراد يحتفظ بها في تلك الشركات.[٢٣٨] وخلاصة القول، فإنّ واجب الشركة – في توفير التأمين – قد يتمّ من خلال عدّة مصادر، ربما يؤكد كل منها على دائرة اختصاص بعينها من الجوانب المختلفة لبيانات الشركات في ظل التزام عام بتوفير التأمين لبيانات الشركات ونظم المعلومات.

ثانياً/ المعيار القانوني لتأمين المعلومات:

نادراً ما تحدّد القوانين واللوائح أي تدابير تأمين يعيّن على الشركة تنفيذها لتفي بالتزاماتها القانونيّة، فأغلبها عادة ما تلزم الشركات بوضع وتنفيذ إجراءات، أو ضوابط، أو ضمانات، أو تدابير تأمين "معقولة" أو "ملائمة" ولكن غالباً دون تقديم المزيد من التوجيه أو الإرشاد. وتوجد بالطبع العديد من المعايير التي تسعى لتحديد نطاق متطلبات تأمين البيانات من المنظور "الفني"[٢٣٩]، ويتضمّن المعيار القانوني منهجاً معقداً نسبيّاً للالتزام[٢٤٠]، ويتمثل جوهر منهج الالتزام بالتأمين القائم على العملية في تنفيذ تأمين شامل مكتوب يتضمن:

أ. تقييم الأصول: تحديد النظم والمعلومات التي تحتاج إلى حماية.

---

(٢٣٨) الحسيني، عمر الفروق الحسيني. (٢٠١٥). *المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دراسة تحليليّة نقديّة لنصوص التشريع المصري مقارناً بالتشريع الفرنسي*، مصر: دار الجامعة الجديدة الطبعة الثانية. ص ١٥٥.

(٢٣٩) تتضمن تلك المعايير، وغيرها. أنظر:

Jody Westby (Ed.0, International Strategy for Cyberspace Security, at Chapter 4 American Bar Association, Section of Science & Technology Law, 2004).

(٢٤٠) Guinn V. Brazos Higher Education Servo**.** 2006 , CSV, No. 05668, 2006 U.S Dist. Lei 4846 (D. Mann February 7,).

ب. تقييم المخاطر: إجراء عمليات تقييم دوريّة للمخاطر التي تتعرض لها تلك النظم والمعلومات والتي تواجهها الشركة.

ج. تنفيذ تدابير تأمين تقوم على الاستجابة للمخاطر وتنفيذ تدابير تأمين يتمّ تصميمها لإدارة المخاطر المحددة التي تمّ التعرف عليها والسيطرة عليها.

د. مخاطبة أطراف ثالثة والإشراف على ترتيبات تقديم الخدمات من أطراف ثالثة.

هـ. التثقيف وتنفيذ دورات تدريبيّة وتثقيفيّة حول التوعية بالتأمين.

و. المتابعة والاختبار لضمان أنّ البرنامج تمّ تنفيذه بشكل ملائم ويعمل بفعاليّة(٢٤١).

ثالثاً/ وضع برنامج تأمين لإدارة المخاطر والسيطرة عليها: ويعنى ذاك ضرورة تصميم وتنفيذ برنامج تأمين يتكون من معايير التأمين المادية والفنية والإدارية اللازمة للسيطرة على المخاطر التي يتمّ تحديدها خلال تقييم المخاطر. ذلك أنّ نظم الحماية firewalls وبرامج تتبع التدخل هي عادة طرق فعالة لوقف القراصنة hackers ولحماية قواعد البيانات الحساسة من الهجوم الخارجي، ولكن إذا كانت بالإفصاح عن كلمات السر أو البيانات المعقدة للتأمين الفني، على أهميتها، غير قادرة على معالجة المشكلة(٢٤٢).

ولا شك أنّ القيام بتقييم المخاطر ثمّ القيام بنشر تدابير التأمين المصممة لتحديد المخاطر المختلفة، قد تساعد في إعفاء الشركة من المسؤوليّة في حالة وقوع اختراق لنظم التأمين. ووفقاً لقرار المحكمة الفيدراليّة الأخير في دعوى جبن ضد برازوس، تمّ القيام بتقييم للمخاطر بشكل ملائم، وتمّ تنفيذ تدابير التأمين الملائمة، ومن ثمّ، فإن عدم القدرة على التنبؤ أو ردع خرق ما لنظام التأمين، لا

---

(٢٤١) Thomas J. 2005. Smedinghoff "Sec*urity Breach Notification Law – Defining a New Corporate Obligation,*" World Data Protection Report (October).

(٢٤٢) فهمي، خالد مصطفى. مرجع سابق. ص ٨٨.

تشكل فشلاً في الوفاء بواجب توفير نظم تأمين معقولة[٢٤٣]، ومن تدابير التأمين الملائمة، المقترحة في هذا المقام:

١. **حماية الوحدات الماديّة:** وهي عبارة عن تدابير للحماية ضدّ التدمير، أو الفقد، أو تعطل الأجهزة أو المعلومات نتيجة مخاطر بيئيّة محتملة، مثل الأعطال بسبب الحرائق أو المياه أو الأعطال التكنولوجيّة، وإجراءات رقابة تحكم استلام وإزالة الأجهزة والوسائل الإلكترونيّة داخل وحدة ما أو خارجها، وإجراءات تحكم استخدام وتأمين الأجهزة الماديّة.[٢٤٤]

٢. **ضوابط دخول المباني:** وهي قيود على دخول المباني، ووحدات الحاسب الآلي، ووحدات حفظ السجلات، للسماح بالوصول فقط للأفراد المصرّح بهم بذلك[٢٤٥].

٣. **ضوابط الدخول الفني:** وتتمثل في سياسات وإجراءات لضمان دخول الأشخاص المصرح لهم على الأنظمة بطريقة ملائمة، وكذا أولئك الذين يجب ألّا يدخلوا على الأنظمة ويتمّ منعهم من الولوج على تلك الأنظمة، وتتضمّن أيضاً إجراءات لمنح الدخول على الأنظمة والتحكم فيه، وإجراءات التصديق للتحقق من أن الشخص أو الهيئة التي تسعى للولوج على الأنظمة هو الشخص المعني، وإجراءات لإنهاء إمكانيّة الوصول إلى الأنظمة.

٤. **إجراءات تتبع التدخل في الأنظمة:** وهي عبارة عن إجراءات لتتبّع محاولات الدخول على الأنظمة وتقارير بالمخالفات، وإجراءات لتتبّع الهجمات الفعليّة ومحاولات الهجوم على نظم

---

(٢٤٣) جهنمي، منير محمد. المرجع السابق، ص ١٣٢.

(٢٤٤) E. France .1998. '*Using Design to Deliver Privacy'*, in One World, One Privacy, Towards an Electronic Citizenship, 22nd International Conference on Privacy and Personal Data Protection, Venice, 28-30 September 2000, p. 216; see also J. Borking, 'Privacy Protecting Measures in IT Environment Necessary', Information Management, 10, , pp. 6-11. http://www.truste.org

(٢٤٥) Thomas J. 1996. S*medinghoff Guide to Contracts and the Legal Protection of Software* (Software Publishers Association,; 570 pages).

معلومات الشركة أو محاولة التدخل فيها، وإجراءات لمنع وتتبّع وإعداد التقارير بشأن النظم والبرامج الضارة (مثل: برامج الفيروسات، وحصان طروادة، إلخ).[٢٤٦]

٥. **إجراءات تعديل النظم**: في معنى أن تكون التعديلات التي تتمّ على النظم متسقة مع برنامج التأمين بالشركة.

٦. **سلامة البيانات، وسريتها، وحفظها**: وهي مجموعة من التدابير الواجب مراعاتها لحماية المعلومات من الولوج غير المصرح به، أو التبديل، أو الإفصاح، أو التلف أثناء تخزينها أو نقلها.

٧. **تدمير البيانات والتخلّص من الأجهزة والوسائط**: وهي عبارة عن إجراءات تتعلّق بالتخلص النهائي من البيانات أو الأجهزة التي توجد عليها تلك البيانات.

٨. **ضوابط المراجعة**: ومؤدى ذلك ضرورة حفظ سجلات لتوثيق الإصلاحات والتعديلات التي تتمّ على المكوّنات الماديّة للوحدة المتعلقة بالتأمين (مثل: الجدران، الأبواب، الأقفال، إلخ)، والأجهزة والنظم والبرامج، أو آليات التحكم في المراجعة الإجرائيّة التي تسجل وتختبر عمل الأنظمة[٢٤٧].

٩. **خطة للطوارئ**: ويستلزم ذلك اتخاذ التدابير اللازمة لضمان القدرة على مواصلة العمل في حالة حدوث طوارئ، مثل خطة عمل نسخ احتياطيّة من البيانات، خطة معالجة الكوارث، وخطة للعمل في ظل الطوارئ.[٢٤٨]

---

(٢٤٦) Thomas J. 2005 **.***Smedinghoff "Security Breach Notification Law* – Defining a New Corporate Obligation," World Data Protection Report (October).

(٢٤٧) فهمي، خالد مصطفى. مرجع سابق. ص ٨٨.

(٢٤٨) Jody Westby 2004.(*Ed.0, International Strategy For Cyberspace Security*, at Chapter 4 American Bar Association, Section Of Science & Technology Law,).

١٠. المتابعة والاختيار: أنّ مجرّد تطبيق تدابير التأمين يعدّ غير كافي، فيجب أن تكفل الشركات أيضاً تنفيذ تدابير التأمين على النحو الملائم وتنفيذها بفعاليّة. ويتضمن ذلك إجراء تقييم لمدى كفاية تدابير التأمين المنفذة للسيطرة على المخاطر التي يتمّ تحديدها، وإجراء اختبار دوري أو متابعة لفعاليّة تلك التدابير.

١١. المراجعة والتعديل: ربما من أهم الأمور التي يقرها المعيار القانوني لتأمين المعلومات هو أنّ التأمين يعدّ هدفاً متحركاً. فيجب أن يتواكب التطوّر التقني مع جميع التهديدات، والمخاطر، ونقاط الضعف، وتدابير التأمين المتغيرة المتاحة للاستجابة لها[٢٤٩].ونتيجة لذلك، يجب أن تقوم الشركة بمراجعات داخليّة دوريّة لتقييم وتعديل برامج تأمين المعلومات في ضوء:

أ. نتائج الاختبار والمتابعة.

ب. أي تغييرات ماديّة في النشاط أو الترتيبات.

ج. أي تغييرات في التكنولوجيا.

د. أي تغييرات في التهديدات الداخليّة أو الخارجيّة.

هـ. أي تغيرات بيئيّة أو تشغيليّة محتملة.

و. أي ظروف أخرى قد يكون لها تأثير مادي.

رابعاً/ واجب الإفصاح عن مدى استعداد نظم التأمين:[٢٥٠]

نتيجة للالتزام بتوفير التأمين، قد تجد الشركات نفسها ملزمة بواجب الإفصاح عن مدى استعداد نظم التأمين بها[٢٥١]. إلّا أنّ أحدث التشريعات قد غلبت عليها مخاوف تتعلق بانتحال

---

(٢٤٩) Thomas J .2006. *Smedinghoff Seven Key Legal Requirements for Creating Enforceable Electronic Transactions*, "to be published by The Computer & Internet Lawyer (April).

(٢٥٠) Thomas J .2005. *Smedinghoff "Security Breach Notification Law* – Defining a New Corporate Obligation," World Data Protection Report (October).

(٢٥١) IRS Rev. Proc. 98-25, Section 8.01 The notice must identify the affected records and include a plan that describes how, and what time frane, the taxpayer proposes to replace or restore the affected records in a way that assures that they will be capacle of being processed. Rev Proc. 98-25, Sectinv 8,02.

الشخصيّة، وركزت على الالتزام بالإفصاح عن حوادث الاختراق التي تؤثر على المعلومات الشخصيّة الحساسة. وقد كان السبب الرئيسي المذكور وراء عدم الإبلاغ عن تلك الخروقات لجهات إنفاذ القانون، هو الخوف من الآثار السلبيّة للإعلان عنها.

وقد كان أول القوانين التي تقتضي الإفصاح عن خرق نظم التأمين التي تتضمن معلومات شخصيّة هو قانون كاليفورنيا بشأن معلومات خرق نظم التأمين (S.B. 1386) والذي دخل حيّز التنفيذ في ١ يوليو ٢٠٠٣ م.[٢٥٢] ويلزم ذلك القانون جميع الشركات التي تمارس أعمالها في كاليفورنيا بالكشف عن أي عمليّة خرق لنظم التأمين تؤدي إلى حصول شخص غير مصرح له على أنواع بعينها من المعلومات الشخصيّة لأحد المقيمين بولاية كاليفورنيا. ويجب أن يتمّ الإفصاح لجميع الأشخاص الذين تعرضت معلوماتهم للخرق، ويحق للمتضرر بسبب فشل الشركة في الوفاء بذلك الالتزام، أن يقاضى الشركة مطالباً بتعويض[٢٥٣].

المطلب الثالث: موقف التشريعات المقارنة

ونصّت المادة رقم من القانون الكويتي رقم ٣. السنة ٢٠١٤ في شأن المعاملات الإلكترونية على أن يكون كل من السجل الإلكتروني والمستند الإلكتروني والرسالة الإلكترونية والمعاملة الإلكترونية والتوقيع الإلكتروني في مجال المعاملات المدنية والتجارية والإدارية منتجة لذات الأثار القانونية المترتبة على الوثائق والمستندات والتوقيعات الكتابية من حيث إلزامه لأطرافه. أو قوته في الإثبات أو حجيته متي أجري وفقاً لأحكام هذا القانون". ونصّت المادة ١٠ من القانون الاتحادي الإماراتي رقم ١ لسنة ٢٠٠٦ بشأن المعاملات والتجارة الإلكترونية على أن:

---

(٢٥٢) Cal. Civil code Section 1798.82. wwwleginfo.ca.gov/calaw.html

(٢٥٣) Thomas J. 2005 .*Smedinghoff "Security Breach Notification Law* – Defining a New Corporate Obligation," World Data Protection Report (October).

١) لا يحول دون قبول الرسالة الإلكترونية أو التوقيع الإلكتروني كدليل إثبات:

أ. أن تكون الرسالة أو التوقيع قد جاء في شكل إلكتروني.

ب. أن تكون الرسالة أو التوقيع ليس أصلياً أو في شكله الأصلي، متى كانت هذه الرسالة أو التوقيع الإلكتروني أفضل دليل يتوقع بدرجة معقولة أن يحصل عليه الشخص الذي يستشهد به.

٢) في تقدير حجية المعلومات الإلكترونية في الإثبات، تراعي العناصر الآتية:

أ. مدى إمكانية الاعتداد بالطريقة التي تم بها تنفيذ واحدة أو أكثر من عمليات إدخال المعلومات أو إنشائها أو تجهيزها أو تخزينها أو تقديمها أو إرسالها.

ب. مدى إمكانية الاعتداد بالطريقة التي استخدمت في المحافظة على سلامة المعلومات.

ج. مدى إمكانية الاعتداد بمصدر المعلومات إذا كان معروفاً.

د. مدى إمكانية الاعتداد بالطريقة التي تم بها التأكد من هوية المنشئ.

هـ. أي عنصر آخر يتصل بالموضوع.

٣) ما لم يتم إثبات عكس ذلك. يفترض أن التوقيع الإلكتروني المحمي:

أ. يمكن الاعتداد به.

ب. هو توقيع الشخص الذي تكون له صله به.

ج. قد وضعه ذلك الشخص بنية توقيع أو اعتماد الرسالة الإلكترونية المنسوب إليه إصدارها.

٤) ما لم يتم إثبات عكس ذلك يفترض أن السجل الإلكتروني المحمي:

أ. لم يتغير منذ أن أنشئ.

ب. معتد به.

ونصّت المادة ١١ من القانون ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات على أن يكون للأبلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو من النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات ذات قيمة وحجية الأبلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا

القانون". ونصت المادة (٧) من المرسوم سلطاني العماني رقم (٢٠٠٨/٦٩) بإصدار قانون المعاملات الإلكترونية على أن تنتج الرسالة الإلكترونية أثرها القانوني وتعتبر صحيحة وقابلة للتنفيذ شأنها في ذلك شان الوثيقة المكتوبة إذا روعي في إنشائها واعتمادها الشروط المنصوص عليها في هذا القانون واللوائح والقرارات الصادرة تنفيذاً لأحكامه".

المبحث الثالث: توقيع الوكيل الذكي على العقود الذكية

تمهيد

حقيقة أن العقد بالمعنى التقليدي هو بين شخص وآخر وأن الصفقة تحكمها القواعد العامة للعقد. يتم التنفيذ دون تدخل عنصر بشري أو من خلال وكلاء إلكترونيين تحكمها قواعد خاصة بالبيئة الإلكترونية، وفي حال وجود هذه القواعد، إضافة إلى مسألة المصطلحات، "عقد ذكي" نخطط لتوضيح النظام القانوني للتوقيع الذكي. وكيل في هذه الدراسة.

من خلال تقسيم المبحث إلى خمسة مطالب خصص في الأول ماهية توقيع الوكيل الذكي وسكون المطلب الثاني لدراسة أنماط الحماية التقنية للتوقيع الإلكتروني اما المطلب الثالث لبيان القواعد الجزائية لحماية التوقيع الإلكتروني وأحدد في المطلب الرابع مدلول المصلحة محل الحماية في جرائم الاعتداء على التوقيع الإلكتروني والذي يتمحور في ثلاثة فروع يكون في الفرع الأول بيان تطبيقات المصلحة محل الحماية في جرائم التوقيع الإلكتروني والفرع الثاني: لتوضيح حماية سرية وخصوصيه تداول البيانات في جرائم التوقيع الإلكتروني والفرع الثالث: الاستعمال غير المشروع في جرائم التوقيع الإلكتروني وأخيراً يكون المطلب الخامس لبيان نطاق الحماية الجنائية للتوقيع الإلكتروني وهذه المطالب والذي يتمحور أيضاً في ثلاثة يكون في الفرع الأول بيان حماية التوقيع الإلكتروني في مجال الإدارة

الإلكترونية والفرع الثاني: لتوضـــيح حماية التوقيع الإلكتروني في مجال المعاملات المدنية والفرع الثالث: لمعرفة حماية التوقيع الإلكتروني في مجال التجارة الإلكترونية نناقشها في التالي:

المطلب الأول: ماهية توقيع الوكيل الذكي

ويقصد بأتمتة النظام الإلكتروني أن تتم الأعمال من تلقاء ذاتها دون تدخل العنصر البشري وهذا يعدّ تطوراً إلكترونياً في العمل غير مسبوق، وانطلاقاً من ذلك يمكن للحاسب الآلي أن يلعب دور الوكيل الإلكتروني وينجز عملاً مع إنسان أو حاسب آلي آخر، وبهذا يحدث الإيجاب والقبول آليا وبشكل تلقائي ارتكازاً إلى عناصر ومعلومات مبرمجة بين الحواسب الآلية تنتقل عبر شبكة الاتصال الدولية، ويضاف إلى ذلك كونه متقيداً بالتعليمات التي لديه.

القانون الأونسترال النموذجي بشأن التجارة الإلكترونية الصادر سنة ١٩٩٦ يجيز استخدام المتعاقدين الأجهزة الإلكترونية لإبرام العقود في المادة ١١/ ١ منه التي تتعلق بصحة العقود، ويؤكد ذات القانون في مادته رقم ١٢ على الاعتراف بالعقود المبرمة باستخدام الوسائل الإلكترونية، أمّا أمريكا فقد قامت سنة ١٩٩٨ بإصدار قانون يلغي الأعمال الورقية من الجهات الحكومية وسنة ١٩٩٩ اعترف قانون المعاملات الإلكترونية الموحد بجواز التعاقد إلكترونياً والتعاقد بواسطة الوكلاء الإلكترونيين.

وكان المشرّع الفرنسي أول من سارع إلى الاستفادة من أدوات التكنولوجيا الحديثة، عندما أصدر عام ٢٠٠٠ القانون رقم ٢٠ بخصوص تحديث قانون تكنولوجيا المعلومات المعني بالتوقيع الإلكتروني، كما تبنى تحديث إبرام العقود الإدارية عن طريق إدخال التعديلات على قانون الصفقات العمومية في مادته (٥٦)، وبخصوص دولة الإمارات العربية المتحدة، فلقد كانت دبي أول من بادر إلى الاعتراف بنظام التعاقد الإلكتروني في عقود السلطات الإدارية، حيث أعلنت حكومة دبي سنة ٢٠٠١

أنّها سوف تجري جميع مشترياتها إلكترونياً عبر شبكة الاتصال الدولية، وانطلاقاً من ذلك سمح قانون إمارة دبي للمعاملات الإلكترونية لعام ٢٠٠٢ بالتعاقد بوساطة الوكيل الإلكتروني تبعاً للمادة ١٤/ ١ منه التي تنص على أنّه: "يجوز أن يتم التعاقد بين وسائط إلكترونية مؤتمتة متضمنة معلومات إلكترونية أو أكثر تكون معدة ومبرمجة مسبقاً للقيام بمثل هذه المهمات، ويتم التعاقد صحيحاً ونافذاً ومنتجاً آثاره القانونية على الرغم من عدم التدخل الشخصي أو المباشر لأي شخص طبيعي في عملية إبرام العقد في هذه الأنظمة".

كما تنصّ الفقرة الثانية من ذات المادة على أنّه: "كما يجوز أن يتم التعاقد بين نظام معلوماتي إلكتروني مؤتمت يعود إلى شخص طبيعي إذا كان الأخير يعلم أو من المفترض أن يعلم ذلك، سيتولى مهمة إبرام العقد أو تنفيذه"، ومنه يتّضح لنا أنّ المشرّع الإماراتي يأخذ بفكرة أن التعبير عن الإرادة الذي يتم عبر الوسائل الإلكترونية أو الوسيط الإلكتروني هو تعبير يصدر عن المستخدم الذي يسيطر على النظام المؤتمت بشكل مباشر.

ويمكننا القول أنّ المشرّع الإماراتي لم يمنح الوسيط الإلكتروني شخصية قانونية مستقلة، بل على العكس من ذلك فقد اعتبر أنّ التعبير عن الإرادة بواسطة وسيط إلكتروني هو بمثابة تعبير عن الإرادة صادر من مستخدم الوسيط الإلكتروني، وهو ما يمكننا أن نطلق عليه أنّ الوسيط الإلكتروني في نظر المشرّع الإماراتي هو بمثابة وسيلة اتصال يستخدمها المتعاقد مع الإدارة في العقد الإداري الإلكتروني مثلها مثل الهاتف أو الفاكس وغيرها من الوسائل الحديثة، حيث أنّ اتجاه المشرّع الإماراتي هو اعتبار التعبير عن الإرادة عبر الوسائل الإلكترونية هو تعبير صادر بشكل مباشر عن الشخص الذي يسيطر عليه ويستخدمه.

المطلب الثاني: أنماط الحماية التقنية للتوقيع الإلكتروني

تتعدّد صور التوقيع الإلكتروني بحسب الطريقة التي يتم بها هذا التوقيع، كما تتباين هذه الصور من حيث درجة الثقة، ومستوى ما تقدمه من ضمان، بحسب الإجراءات المتبعة في إصدارها وتأمينها، والتقنيات التي تتيحها(٢٥٤).

ومن ثم، فإنّ تقييم جدوى وسيلة الحماية التقنية ترتبط بمدى استيعابها لعناصر أمن المعلومات والتي تتلخص في الآتي:

١. **السرية**: وتعني التحقق من أنّ المعلومات لا يتسنى الاطلاع عليها لغير المخول له بذلك(٢٥٥).

٢. **تكامل البيانات**: في معنى أنّ رسالة البيانات تكون بمنأى عن أي عبث بأي جزء من محتواها(٢٥٦).

٣. **التوثيق**: أي ضرورة وجود آلية للاحتفاظ برسالة البيانات بحيث يمكن الرجوع إليها عند الحاجة.

٤. **عدم الإنكار**: ويعني ذلك ضرورة إسباغ الحجية في الإثبات على مضمون التصرف محل الرسالة، وبحيث لا يكون بوسع الموقع عليها إنكار توقيعه(٢٥٧).

ومن ناحية أخرى، فيجب أن تتوافر آلية يكون من شـأنها تحقق طرفي التعاقد من أنّ التوقيع المنسوب للطرف الآخر قد صدر عن يد صحيحة منه ودون أن يداخله شبهة تنال من حجيته.

---

(٢٥٤) عبد الحميد، ثروت. (٢٠٠١). *التوقيع الإلكتروني ماهيته مخاطره وكيفية مواجهتها ومدى حجيته في الإثبات*. مصر: دار النيل للطباعة والنشر. ص ٥٤.

(٢٥٥) *Guide to Electronic Commerce*, Regulation, 2002. http://www.diffuse.org/commerce.html .

(٢٥٦) الجنيهي، ممدوح. (٢٠٠٥). *أمن المعلومات الإلكترونية*. مصر: دار الفكر الجامعي. ص ١٣.

(٢٥٧) حازم، شريف. (٢٠٠٦). *حجية التوقيع الإلكتروني*. مركز الدراسات القضائية. دولة الإمارات العربية المتحدة: بحث مقدم لمؤتمر التوقيع الإلكتروني. ص ٧.

التوقيع الإلكتروني بواسطة أدوات القياس الحيوي

يعتبر التشفير من أهم السبل الوقائية لإسباغ الحماية على التوقيع الإلكتروني، وإزاء ذلك بات ملحاً أن تتوافر آلية يكون من شأنها تحقق طرفي التعاقد من أنّ التوقيع المنسوب للطرف الآخر قد صدر عن إرادة صحيحة منه ودون أن يداخلها شبهة تنال من حجيته. ومن صور الحماية الوقائية التوقيع الإلكتروني باستخدام أدوات القياس الحيوي وتتم هذه الصورة من خلال استخدام أساليب علمية متطورة تدخل ضمن تكنولوجيا البصمات والخواص الحيوية والطبيعية، وهي تعتمد على الخصائص الفيزيائية والطبيعية والسلوكية للأفراد[٢٥٨] والتي تعتمد على بصمة الإبهام أو حدقة العين أو بصمة الصوت هي في التالي:

أولاً/ أجهزة استخدام بصمة الإبهام:

وهي عبارة عن خطوط حلمية بارزة ومتحاذية ومنخفضة تتخذ أشكالاً مختلفة على جلد أصابع اليدين. حيث تركن الكثير من المؤسسات الأمنية إلى استحالة التطابق بين بصمة الإصبع الأكثر من شخص، ومن ثم يتم تجهيز الحاسب بوضع خاص في لوحه المفاتيح أو من خلال جهاز يتم توصيله استقلالاً بالحاسب الإلكتروني، وما على الجهاز إلّا أن يلتقط صورة الثنايا الموجودة ليحولها لرسالة بيانات وعند التوقيع يقوم الحاسب بإجراء المضاهاة بين التوقيع المخزن والتوقيع الجديد المعرفة مدي التطابق بينهما[٢٥٩].

---

(٢٥٨) قضت محكمة النقض أنّ حالة ضياع الشيك وما يدخل في حكمها والتي يتحصل جنيها على الشيك عن طريق جرائم سلب المال كالسرقة البسيطة والسرقة بطريق آخر والنصب والتبديد وأيضاً الحصول عليه بطريقة التهديد والتي تبيح للسارق أن يتخذ من جانبه ما يعون به مال غير توقف عل يحكم القضاء تقرير أمنه معلومتي الساحب في تلك الحال على حق المستفيد استناداً إلى سبب من أسبابه الإباحة (طعن ٢٧٧ لسنة ٥٥ ق ج ١٩٨٥/٢/٢٨).

٢٥٩ شريف، عادل. (٢٠١٧). *ضمانات الأمن والأمانة في شبكة الإنترنت*، مصر: مؤتمر في القانون. ص ٣٥.

ثانياً/ أجهزة استخدام حدقة العين:

حيث يتم تعيين الخواص البيولوجية للعين المتمثلة في الشرايين والعلامات الموجودة في الشبكية والقرنية، ثم تحلل على ذاكرة الحاسب الذي يتصل بجهاز مزود بشرائح إلكترونية صغيرة الحجم، والذي يقوم بدوره بتحديد هوية الأشخاص عند التعامل من خلال التقاط صورة للعين ومضاهاتها بما هو مخزن في الذاكرة، وبالتالي يسمح لصاحب البصمة بالدخول على البرنامج وتلك الطريقة تعرف "إيريكس كود"(٢٦٠).

ثالثاً/ أجهزة استخدام بصمة الصوت:

تختلف خصائص الأشخاص في الذبذبات الصوتية من حيث درجتها ونوعها، حيث يتم تحويل نبرة الصوت إلى خطوط أفقية تترجم إلى رسالة بيانات، ثم يقوم الحاسب المزود بجهاز البرنامج يحتوي تلك الخاصية بالمقارنة بين صوت الشخص المصرح له باستخدام الجهاز وبين البصمة الصوتية السابق تسجيلها(٢٦١). وفي الوقت الحالي تدخل معظم الشركات المصنعة لهذه الأجهزة البيومترية هذه الوسائل ضمن جهاز الفارة ولوحة المفاتيح.

وبالرغم من أنّ معظم المؤسسات الأمنية المصنعة للنظام البيومتري ترى أنّ الدقة في تحقيق الشخصية تتراوح بين ٩٩ و٩٩,٩٪، إلّا أنّه ممّا يؤخذ على تلك الوسائل أنّ الصورة البيومترية المسجلة على القرص عرضة للنسخ أو فك شفرتها أو إتلافها، فضلاً عن عدم إمكانية استخدام تلك الخاصية في كل الحاسبات، نظراً لاختلاف نظم التشغيل وأساليب التخزين وخصوصيات حزم البرامج المتنوعة،

---

(٢٦٠) حجازي، عبد الفتاح (٢٠٠٤). *التوقيع الإلكتروني في النظم المقارنة*، مصر: دار الفكر الجامعي. ص ١٣٣.

(٢٦١) أبو هيبة، نجوى (٢٠٠٣). *التوقيع الإلكتروني، تعريفه، حجيته*، الإمارات: دراسة مقدمة لمؤتمر الأعمال المصرفية دبي– المجلد الأول ص ٤٦٦ عادل شريف، عبد الله إسماعيل. *ضمانات الأمن والأمانة في شبكة الإنترنت مؤتمر القانون* ص ٣٥.

وكذا فقدان سرية وكفاءة هذه التقنية لما قد تعمد إليه الشركات المصنعة لها من الاتفاق على طريقة موحدة لها.(٢٦٢) فقد تم اكتشاف حالات احتيال باستخدام البصمة الشخصية المقلدة وعدم استطاعة بعض أجهزة التحقق البصرية المصنوعة من رقائق السيليكون من كشفها أو تمييزها، كما أنّ التكلفة المرتفعة نسبياً التي يتطلبها وضع نظام آمن في شبكات المعلومات – باستخدام وسائل بيو مترية – حدت من انتشاره إلى درجة كبيرة وجعلته قاصراً على بعض الاستخدامات المحدودة(٢٦٣).

ووفقاً لقانون الولايات المتحدة الأمريكية للتوقيع الإلكتروني هناك العديد من الطرق لتوقيع الوثيقة الإلكترونية. وبالرغم من أنّه يتم التعبير عن التوقيعات الإلكترونية بالصورة الرقمية (أي في شكل سلسلة من الأصفار والرقم واحد)، فإنّها قد تأخذ عدة أشكال باستخدام العديد من الطرق التكنولوجية. ومن أمثلة التوقيعات الإلكترونية المعتمدة بموجب قانون التوقيعات الإلكترونية وقانون المعاملات الإلكترونية الموحد:

أ. اسم المرسل مطبوع في نهاية الرسالة الإلكترونية(٢٦٤).

ب. صورة رقمية من التوقيع الخطي ملحقاً بالوثيقة الإلكترونية.

ج. شفرة أو كلمة سرية حتى يتمكن المستقبل من تمييز شخصية المرسل مثال تلك الشفرات المستخدمة في حالة بطاقات الائتمان وبطاقات الصرف الآلي).

---

(٢٦٢) Electronic Patient Management, - About TERP 2003 : http://www.medrecinst.com/index.about.shtml.

(٢٦٣) سليم، أيمن سعد. (٢٠٠٢). *التوقيع الإلكتروني دراسة مقارنة*. مصر: دار النهضة العربية، ص ٢٢

(٢٦٤) Rosenfeld v. Zern, 2004 N.Y. Slip Op. 24143 (2004); *Shattuck v. Klotzbach, 2001 Mass*. Super .48 LEXIS 642 (December 11, 2001)

يضع كلاً من قانون التوقيعات الإلكترونية وقانون المعاملات الإلكترونية لفظ "عملية" كجزء من التعريف البيان أنّ عملية النقر على زر الفأرة يصلح لتوقيع إذا تحققت الشروط الأخرى؛ فكما ورد في الملاحظات على قانون المعاملات الإلكترونية يتضمّن هذا التعريف عملية النقر على زر الفأرة التي تسمح بولوج المستخدم إلى مواقع الشبكة باعتبارها توقيعاً إلكترونياً. فعلى سبيل المثال، إذا طلب أحد الأشخاص شراء السلع أو الخدمات من أحد المواقع على الشبكة، يطلب من هذا الشخص تقديم كافة المعلومات كجزء من العملية التي تؤدي في النهاية إلى استلام البضائع أو الخدمات. عندما يصل المستهلك إلى الخطوة الأخيرة ويقوم بالنقر على زر "أقبل"، فقد أجرى العملية بنية ربط الشخص بكافة سجلات تلك العملية. قانون المعاملات البند ٢ التعليق ٧.

د. طرق الاستدلال البيولوجي، مثل بصمة اليد أو بصمة الصوت أو بصمة العين.

هـ. النقر على زر الفارة (مثال ذلك النقر على زر "أقبل")[٢٦٥].

و. الصوت (مثل الصوت الذي يصدر عند الضغط على رقم "٩" في جهاز التليفون للموافقة)

ز. التوقيع الرقمي (من خلال التشفير بالمفتاح العام)[٢٦٦].

المطلب الثالث: القواعد الجزائية لحماية التوقيع الإلكتروني

بالرغم من أهمية التدابير الوقائية للحد من ارتكاب الجرائم الناشئة عن التوقيع الإلكتروني، إلّا أنّ ذلك لن يؤدي إلى منع ارتكابها. لذلك، كان ضرورياً أن تتناول التشريعات – إضافة إلى التدابير الوقائية – تنظيماً الجزاء الجنائي لمن تسول له نفسه الاعتداء على التوقيع الإلكتروني[٢٦٧]. غير أنّ دراسة ذلك التنظيم، يستلزم الوقوف على المصلحة محل الحماية في جرائم الاعتداء على التوقيع الإلكتروني وصولاً لطبيعة السلوك المادي الذي يشكل اعتداء على تلك المصلحة. وتتمثل المصالح المحمية في شرعية تداول البيانات، وسريتها وخصوصيتها، وإسباغ الحجيه على التوقيع الإلكتروني ومساواته بالتوقيع التقليدي[٢٦٨].

وتأكيداً لحرص مشرعي الدول المختلفة على وضع الضمانات الكفيلة بحرية التجارة الإلكترونية وإسباغ الحماية الجنائية على المستند الإلكتروني، تم تجريم أفعال الاعتداء على التوقيع الإلكتروني، سيما

---

(٢٦٥) لا يتّضح إذا كانت عملية النقر على زر "أوافق" تستوفي تعريف التوقيع كما ورد في توجيهات الاتحاد الأوروبي، إذ يتطلب هذا التعريف أن يتضمّن التوقيع بيانات في الصورة الإلكترونية. المادة ٢ (١) من التوجيهات.

(٢٦٦) للمزيد من المعلومات حول هذه *التكنولوجيا والعملية التي تتم بها إنشاء التوقعات الرقمية أنظر لجنة تأمين المعلومات قسم التجارة الإلكترونية*، "التوجيهات العامة حول التوقيع الإلكتروني" www.abanet.org/scitech/ec/isc/dsgfree.htm1.

(٢٦٧) حسن إبراهيم. *الحماية الجنائية لحق المؤلف عبر الإنترنت*. (رسالة دكتوراه). مصر: دار النهضة العربية. ص ٦٥.

(٢٦٨) La Loi Type de la CUNDCI sur le commerce électronique – la commission des Nations Unies pour le droit comercial international CNUDCI-1996.

أنظر أيضاً: شمس الدين، أشرف توفيق. (٢٠٠٦). *الحماية الجنائية للمستند الإلكتروني – دراسة مقارنه*. الطبعة الأولى. مصر: دار النهضة العربية ص ١٤٠.

وقد بدأ الدخول على الإنترنت وسيله سهله في ارتكابها[٢٦٩]. وقد يرتبط السلوك المادي لجرائم الاعتداء على التوقيع الإلكتروني بتداول بيانات المحرر الإلكتروني، كما هو الحال بالنسبة لجريمة التعامل غير المشروع في نشاط التصديق أو انتهاك سريه وخصوصية البيانات، كما أنّه من المتصور أن يكون محل الجريمة هو المساس بحجيه التوقيع الإلكتروني في الإثبات كما هو الحال في جريمة تزوير التوقيع الإلكتروني وجريمة صنع برنامج لإعداد توقيع إلكتروني.

وتعرف الجريمة بصفة عامة بأنّها عدوان على مصلحة يحميها القانون، ويختص القانون الجنائي بالنص عليها وبيان أركانها والعقوبة المقررة لفاعلها[٢٧٠]. ويستلزم ذلك بطبيعة الحال الوقوف على وجه الدقة على مدلول المصلحة محل الحماية في جرائم الاعتداء على التوقيع الإلكتروني.

ومن ناحية أخرى يتعين الوقوف على نطاق المصلحة محل الحماية في هذا الصدد، ذلك أنّ الصلة وثيقة بين التوقيع الإلكتروني والحكومة الإلكترونية بحيث تتداخل الحماية المقررة لكل منهما كما أنّ المصلحة محل الحماية في التوقيع الإلكتروني ترتبط بالتجارة الإلكترونية عبر الإنترنت[٢٧١]، ومن جهة أخرى، فإنّ دائرة الحماية المقررة لحقوق الملكية الفكرية والذهنية قد تتداخل مع دائرة الحماية المقررة للتوقيع الإلكتروني[٢٧٢].

---

(٢٦٩) العتيق، السيد. (٢٠١٧). *جرائم الإنترنت*. مصر: دار النهضة العربية. ص٢٨. قورة، نائلة. (٢٠٠٥). *جرائم الحاسب الاقتصادية*، مصر: دار النهضة العربية. ص ٥٧. رشدي، محمد السعيد. (٢٠٠٤). الإنترنت *والجوانب القانونية لنظم المعلومات*. مصر: دار النهضة العربية. ص ٧٧.

(٢٧٠) حسنين. إبراهيم عبيد. (١٩٧٩). *الجريمة الدولية* دراسة تحليلية تطبيقية. مصر: دار النهضة العربية. الطبعة الأولى. ص ٥.

(٢٧١) Guide to Electronic Commerce Regulation, 2002, op-cit.

(٢٧٢) شرف الدين، أحمد. (٢٠٠٢). *عقود التجارة الإلكترونية. تكوين العقد وإثباته*. مصر: كلية الحقوق جامعة عين شمس. ص١١٠.

المطلب الرابع: مدلول المصلحة محل الحماية في جرائم الاعتداء على التوقيع الإلكتروني

تمهيد

يمكن القول إنّ المصالح محل الحماية في التوقيع الإلكتروني متعددة وإن كانت تصب في حماية حرية ممارسة وتداول السلع والخدمات عبر الإنترنت(٢٧٣). قد ينطوي النص القانوني على أكثر من مصلحه يرى أنّها جديرة بالحماية، ذلك أنّ المقرر أنّ النص الواحد قد يحمي مصلحه واحدة أو مصالح متعددة(٢٧٤) وتتمثل المصالح المحمية في مشروعية البيانات، وسرية تداولها وإسباغ الخصوصية والحجيه على التوقيع الإلكتروني(٢٧٥):

فحماية الخصوصية في مجال التوقيع الإلكتروني، يجب أن ترتبط بمنظومة متكاملة تحدد عناصر الحماية ونطاقها، وهناك خمسة مبادئ أساسية تحكم ما يسمى بالممارسات العادلة والمقبولة أو النزيهة في نطاق خصوصية المعلومات أو حماية البيانات الشخصية وهذه المبادئ هي: الإخطار Notice والاختيار Choice، والوصول للبيانات، والأمن، وتطبيق القانون٢٧٦. ولا شك أنّ الاستعمال غير المشروع لنظم الحاسب الإلكتروني من خلال شبكة الإنترنت هي أحد أهم صور المصلحة محل الحماية في جرائم الاعتداء على التوقيع الإلكتروني. لذلك، سوف نقسم هذا المطلب إلى ثلاث فروع على النحو التالي:

---

(٢٧٣) قشوش، هدى. (٢٠٠٠). قشقوش *الحماية الجنائية للتجارة الإلكترونية*. مصر: دار النهضة العربية. ص ١٥.

(٢٧٤) عبيد، حسنين إبراهيم. (١٩٩٩). *فكرة المصلحة في قانون العقوبات. مصر:* المجلة الجنائية القومية. المجلد ١٧ ع ٢ يوليو رقم ٨ ص ٢٥٠.

(٢٧٥) La Loi Type de la CUNDCI sur le commerce électronique 1996. la Des Nations Unies pour le droit comercial commission international CNUDCI –.

٢٧٦ فهمي، خالد مصطفى. (٢٠٠٧). النظام *القانوني للتوقيع الإلكتروني في ضوء التشريعات العربية والاتفاقيات الدولية*. مصر: الجامعة الجديدة. ص ٨٨.

الفرع الأول: تطبيقات المصلحة محل الحماية في جرائم التوقيع الإلكتروني

إنّ استخدام الوسائل التكنولوجية الحديثة من الأشخاص الطبيعية والمعنوية من التبادل السريع للمعلومات في وقت قصير، مما جعل الأفراد يفضلونها في تصرفاتهم القانونية، ومن انعكاسات هذا التطور ظهور التجارة الإلكترونية عبر الإنترنت «Le commerce électronique» أو ما يسمى بالتعاقد عن بعد. ولا شك أنّ الاستعانة بهذه التقنية أظهر معه بعض المشكلات العملية والقانونية على مستوى المعاملات الإلكترونية. لذلك، يمكن القول إنّ المصالح محل الحماية في التوقيع الإلكتروني متعددة وإن كانت تصب في حماية حرية ممارسة وتداول السلع والخدمات عبر الإنترنت.

حماية حجية التوقيع الإلكتروني: الأصل أنّ التوقيع يرتبط ارتباطاً وثيقاً برضاء صاحبه وإقراره بمضمون التصرف القانوني الذي تضمنه المستند بتوقيعه في النهاية. وقد أثار الخلط بين الحماية المقررة للمستند وبين الحماية المقررة للإرادة بعض الصعوبة. ويرجع ذلك إلى صعوبة الجزم بصحة التوقيع الإلكتروني ومدى الوثوق برضاء صاحبه بالتصرف الذي وقع عليه، وأنّ ما اتصل علمه به واطلع عليه من شروط المحرر يتطابق مع ما تم التوقيع عليه(٢٧٧) فإذا شاب إرادة الموقّع عيب مثل التدليس، بأن قام بوضع التوقيع الإلكتروني على محرر، بينما انصب هذا التوقيع على محرر آخر يحوي مضمون مختلف فهل يشكل هذا الفعل اعتداء على المستند الإلكتروني ذاته، أم أنّ هناك صورة أخرى من الحماية تختلف عن الحماية المقررة للمحرر بصفة عامة؟(٢٧٨)

---

(٢٧٧) حجاي، عبد الفتاح. (٢٠٠٤): *التوقيع الإلكتروني في النظم القانونية المقارنة. مصر:* دار الفكر العربي. ص ١٠٩ ص ٣٥٧.

(٢٧٨) قشوش، هدى حامد. (٢٠٠٣) *الحماية الجنائية للتوقيع الإلكتروني*. الإمارات: دراسة مقدمة إلى المؤتمر الذي عقدته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في موضوع *"القانون والكومبيوتر والإنترنت"*، وذلك بفندق هيلتون العين في الفترة من ١ – ٣ مايو ص ٥٨١.

ويرى بعض الفقه أنّ الحماية الجنائية للمحرر – باعتبارها تهدف إلى حماية التوقيع وتضمن أدائه لدوره الاجتماعي – لا صلة لها بما شاب إرادة الموقع من عيوب مثل الغلط أو التدليس أو الإكراه، وفي هذه الحالة، فإنّ التوقيع المنسوب لصاحبه يكون صحيحاً منتجاً لآثاره القانونية، بل إنّه قد يرد عليه التصحيح والإجازة(٢٧٩)

وقد أيّد المشرّع المصري في قانون التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤ وجهة النظر الأولى ورتب على ذلك تجريم الاعتداء المادي على التوقيع أو الوسيط أو المحرر الإلكتروني سواء بالإتلاف أو التعييب أو التعطيل كما جرم تزوير التوقيع الإلكتروني أو تصنيع برنامج يكون من شأنه إعداد توقيع إلكتروني(٢٨٠) فقد نصّ المشرّع المصري في المادة ٢٣ من قانون التوقيع الإلكتروني ١٥ لسنة ٢٠٠٤ على أنّه «مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من، أتلف أو عيب توقيع أو وسيطاً أو محرراً إلكترونياً أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر أو استعمل توقيعاً أو وسيطاً أو محرراً إلكترونياً معيباً أو مزوراً مع علمه بذلك.

وإذا كانت المادة (٢٧) من مشروع القانون المصري للتجارة الإلكترونية، قد نصّت على أنّه "يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن عشرة آلاف جنيه أو بإحدى هاتين العقوبتين، كل من صنع أو حاز أو حصل على نظام معلومات أو برنامج لإعداد توقيع إلكتروني دون موافقة

---

(٢٧٩) غنام، محمد. (٢٠٠٢). *عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكومبيوتر*. دراسة مقدمة إلى المؤتمر الذي عقدته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في موضوع "القانون والكومبيوتر والإنترنت". وذلك بفندق هيلتون العين في الفترة من ١ – ٣ مايو

(٢٨٠) حجازي، عبد الفتاح. (٢٠٠٤). *التوقيع الإلكتروني في النظم القانونية المقارنة*. مصر: دار الفكر العربي. ص ١٠٩ ص ٣٥٧.

صاحبه"، فإنّ القانون المصري ١٥ لسنه ٢٠٠٤ قد صدر خلوا من أي نص مماثل مكتفياً في ذلك بالفقرة د/ من المادة ٢٣ التي جرّمت فقط (التوصل بأية وسيله إلى الحصول على توقيع أو وسيط أو محرر إلكتروني). كما حرص المشرّع الفرنسي في المادة ١٣١٦/ ١ من القانون رقم ٢٣٠ لسنة ٢٠٠٠ على المساواة التامة في الحجية كدليل في الإثبات بين الكتابة الإلكترونية والكتابة على الورق(٢٨١) وإن كان المشرّع قد أعقب ذلك بالنص في نفس المادة على أنّه يشترط أن تكون هذه الكتابة الإلكترونية تعبر عن الشخص الذي صدرت عنه قانوناً(٢٨٢) وهو بذلك يكون قد حسم خلافاً في الفقه استمر سنوات(٢٨٣)

الفرع الثاني: حماية سرية وخصوصيه تداول البيانات في جرائم التوقيع الإلكتروني

إنّ حماية الخصوصية في مجال التوقيع الإلكتروني، يجب أن ترتبط بمنظومة متكاملة تحدد عناصر الحماية ونطاقها، وهناك خمسة مبادئ أساسية تحكم ما يسمى بالممارسات العادلة والمقبولة أو النزيهة في نطاق خصوصية المعلومات أو حماية البيانات الشخصية وهذه المبادئ هي: الإبلاغ/ الإخطار Notice: ويراد بهذا المبدأ التزام مزود الخدمة أو الموقع بإخطار مستخدمي المواقع بما إذا كان الموقع أو مقتضيات الخدمة ينطويان على جمع بيانات شخصية وبيان إلى أي مدى تجمع هذه البيانات وتستخدم. الاختيار Choice: ويوجب هذا المبدأ التزام الشركات صاحبة المواقع أو مزودي الخدمة بتوفير خيار للمستخدم بخصوص استخدام بياناته في غير الغرض المخصصة من أجله. والوصول للبيانات Access: ويوجب هذا المبدأ منح القدرة للمستخدمين للوصول إلى بياناتهم والتثبت من صحتها

(٢٨١) leclercQ(jean) preuve et signature électronique de la loi du13 mars2001 au décret du 30mars2001.

(٢٨٢) Philipp. Nataf: Commentaires sur la loi portant adaptation du droit De la preuve aux technologies de l'information - J.C.P. N 21 - 22 - 25 Mai 2000 p. 836.

(٢٨٣) قشوش، هدى حامد قشقوش. مرجع سابق. ص ٧١.

وتحديثها. والأمن Security: ويتعلق هذا المبدأ بالتزامات المواقع ومزودي الخدمة بمعايير الأمن المتعين تطبيقها لضمان سرية البيانات وسلامة الاستخدام وحظر الوصول غير المصرح به لهذه البيانات، وتتضمّن أيضاً كلمات السر والتشفير وغيرها من وسائل أمن المعلومات(٢٨٤) كما أن تطبيق القانون Enforcement: ويتعلق هذا المبدأ بفرض الجزاءات على الجهات الملتزمة بالمبادئ المتقدمة(٢٨٥)

وقد تتداخل الحماية المقررة للتوقيع الإلكتروني والحماية الجنائية للأسرار: ذلك أنّ المستند قد يحوي سراً يرغب الفرد في الاحتفاظ به بعيداً عن تدخل الأخرين. غير أنّه مع ذلك، فإنّ التفرقة بين جرائم المساس بالمستند الإلكتروني وإفشاء الأسرار ممكنة، ففعل إفشاء السر يجب أن يتم من شخص مؤتمن على الحفاظ على هذا السر؛ وذلك بخلاف الاعتداء على المستند الإلكتروني، إذ يجوز أن يقع من أي شخص. ومن ناحية أخرى، فإنّه حتى ولو كانت الجريمة لا تتطلب إفشاء السر من أشخاص مؤتمنين عليه على نحو ما ينصّ عليه المشرّع المصري من تجريم الحصول بطريقة غير مشروعة على سر من أسرار الدفاع عن البلاد أو تسليمه أو إذاعته (المادة ٨٠ أ)؛ فإنّ الفارق يبقى أيضاً بين الفكرتين، فمدلول "السر" في جرائم إفشاء الأسرار أضيق نطاقاً من مدلول سرية المستند، فالقانون يحمي السر أياً كان الشكل الذي حفظ فيه هذا السر وقد يكون المستند الإلكتروني غير متضمّن لسر ما، ولكن رغم ذلك فلا يجوز الاطلاع عليه، فالكثير من البيانات الشخصية التي تتضمنها المستندات الإلكترونية لا تنطوي على أسرار بالمعنى الدقيق لمدلول السر ومن ثم لا تشملها الحماية الجنائية الواردة بالنصوص

(٢٨٤)- Thomas J. Smedinghoff "Security Breach Notification Law- Defining a New Corporate Obligation," World Data Protection Report (October 2005).

(٢٨٥)- E. France, 'Using Design to Deliver Privacy', in One World, One Privacy, Towards an Electronic Citizenship, 22nd International Conference on Privacy and Personal Data Protection, Venice, 2830 September 2000, p. 216; see also J. Borking, 'Privacy Protecting Information Necessary', Environment IT in Measures Management, 10, 1998, pp. 6-11. http://www.truste.org.

التي تجرّم إفشاء الأسرار[٢٨٦] وتقتصر خطة التشريعات على تجريم وسيلة المساس بالحق في سرية المستند في غالبية الصور تاركة تحديد مضمون هذا الحق للمجني عليه.

الفرع الثالث: الاستعمال غير المشروع في جرائم التوقيع الإلكتروني

ويقصد بذلك أن يتم تداول البيانات بشكل مشروع، وأن يتم تداولها ممن له الحق في هذا التداول والاستخدام. فيشترط أن يتم تداول البيانات عن طريق مزود الخدمة الإلكترونية المصرّح له بذلك. وقد ورد النص على هذه الجريمة في المادة (٢٣/ ١) من قانون التوقيع الإلكتروني المصري الذي عاقب بالحبس والغرامة كل من أصير شهادة تصديق إلكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة المختصة.

حيث نصّت المادة ٢٣/هـ على هذه الجريمة فعاقبت بالحبس والغرامة أو أيهما كل من "... – توصّل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني أو اخترق هذا الوسيط أو اعترضه أو عطّله عن أداء وظيفته". ومؤدى ذلك أنّ التعامل غير المشروع يتخذ إحدى صورتين:

- **الأولى:** الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني بشكل غير مشروع.[٢٨٧]
- **والثانية:** اختراق الوسيط الإلكتروني أو اعتراضه أو تعطيله عن أداء وظيفته كما نصّت المادة (١٩) من القانون، على عدم جواز مزاولة نشاط إصدار شهادات التصديق الإلكتروني إلّا بترخيص من الهيئة[٢٨٨]

---

(٢٨٦) شمس الدين، أشرف. (٢٠٠٦). *الحماية الجنائية للمستند الإلكتروني* دراسة مقارنة. مصر: دار النهضة العربية الطبعة الأولى. ص ٤، وحاتم عبد الرحمن. *الإجرام المعلوماتي*. مصر: دار النهضة العربية. ص ١٣.

(٢٨٧) حجازي، عبد الفتاح بيومي. (٢٠٠٢). *النظام القانون لحماية التجارة الإلكترونية، الكتاب الأول، نظام التجارة الإلكترونية وحمايتها مدن*. مصر: دار النهضة العربية. ص ٥٥٥.

(٢٨٨) أنظر على سبيل المثال قانون الوقيع والسجلات الإلكترونية لولاية نيويورك.

وقد تشتبه الحماية المقررة للتوقيع الإلكتروني مع تلك المقررة لنظم تشغيل الحاسب الآلي، ووجه هذا الشبه أنّ محل الاعتداء في الحالتين ينصب على البيانات التي يتضمّنها المستند أو برنامج التشغيل. ولعل هذا التشابه هو الذي دفع برأي في الفقه إلى القول بأنّ البيانات المدخلة إلكترونياً لا تنفصل عن البرامج التي تنظمها وأنّهما لذلك، لا تختلفان في الطبيعة باعتبارهما كياناً معنوياً، وأنّ حماية هذه البرامج تعد في الوقت ذاته حماية للبيانات المعالجة إلكترونياً[٢٨٩].

وفي تقديرنا أنّ هذا الرأي محل النظر، ذلك أنّ تماثل البيانات الإلكترونية مع برامج تشغيل النظام الذي يتم التعامل مع هذه البيانات في ظله لا يعني تماثلهما في المصلحة التي يحميها المشرّع. فالمشرّع يحمى في الأولى ما انطوت عليه هذه البيانات من وقائع لها أهمية في الإثبات؛ بينما يحمي في الثانية نظم إدارة الحاسبات الآلية وهي مصلحة مختلفة عن الأولى. ولذلك، فإنّ من المتصور أن يتحقق المساس بإحدى المصلحتين دون الأخرى، فعلى سبيل المثال يمكن أن ينصب فعل الجاني على تزوير مستند إلكتروني أو كشف سريته، دون أن يمتد فعله إلى نظام التشغيل. وعلى العكس يمكن أن ينصب فعل الجاني على الإخلال بنظام التشغيل دون أن ينال من البيانات والمستندات المحفوظة في هذا النظام. وهذا التباين يعكس اختلاف في المصلحة التي رأى المشرّع جدارة حمايتها. وأنّه حتى إذا ترتّب على فعل الجاني الوارد على نظام التشغيل مساس بالمستندات الإلكترونية المحفوظة في هذا النظام، فإنّ الأمر لا يعدو أن يكون تعدداً معنوياً للجرائم، ذلك أنّ فعل الجاني يكون قد أفضى في هذه الصورة إلى نتيجتين مختلفتين، يقتصر أثره على توقيع عقوبة الجريمة الأشد، غير أنّ ذلك لا ينفي التعدد في هذه الحالة.

Report to the Governor and Legislature on New York Stat's op-cit., p.10.

(٢٨٩) القهوجي، على عبد القادر. (٢٠٠٠). *الحماية الجنائية للبيانات المعالجة إلكترونياً*. دراسة مقدمة إلى المؤتمر الذي عقدته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في موضوع "القانون والكومبيوتر والإنترنت" بمدينة العين: الإمارات. في الفترة من ١ – ٣ مايو ص ٤٤؛ وأنظر أيضاً في هذا الاتجاه: الدكتور محمد حماد مرهج الهيتي: *التكنولوجيا الحديثة والقانون الجنائي*. ص ٢٤٣.

المطلب الخامس: نطاق الحماية الجنائية للتوقيع الإلكتروني

تمهيد

بسبب العلاقة الوثيقة بين التوقيعات الإلكترونية والحكومة الإلكترونية، يمكن القول أن الحماية المقدمة لأحدهما تعني بالضرورة حماية الآخر. العلاقة بين التوقيعات الإلكترونية والتجارة الإلكترونية واضحة أيضًا. إذا كانت قوة هذه الصفقة عبارة عن تبادل للسلع والخدمات، فإن هذا التبادل هو في الواقع عقد يلخص جميع الشروط القانونية للعرض والقبول، ملزم بتوقيع منسوب إلى مالكه(٢٩٠)

من ناحية أخرى، قد تتداخل دائرة حماية الملكية الفكرية مع دائرة التوقيعات الإلكترونية لذلك، فإن حماية هذه البيانات تحمي أيضًا حقوق الملكية الفكرية في نفس الوقت. لذلك، يأخذ هذا المطلب في الاعتبار الحماية المقدمة للتوقيعات الإلكترونية في مجالات منفصلة: الحكومة الإلكترونية، والمعاملات المدنية، وأخيراً التجارة الإلكترونية(٢٩١).

الفرع الأول: حماية التوقيع الإلكتروني في مجال الإدارة الإلكترونية

أدى الأخذ بنظام الإدارة الإلكترونية إلى أن أصبح التعامل مع الأجهزة الإدارية والحكومية أكثر يسراً، بما يسر التعامل مع الحكومة بوزارتها وأجهزتها المختلفة،(٢٩٢). كما أنّه يمكن من خلال الحكومة الإلكترونية نقل المعلومات والاطلاع على البيانات والحصول على الوثائق والشهادات بسهولة ويسر وبلا توقف(٢٩٣)

---

(٢٩٠) Guide to Electronic Commerce Regulation, 2002, op-cit.

(٢٩١) شمس الدين، أشرف (٢٠٠٦). *الحماية الجنائية للمستند الإلكتروني* – دراسة مقارنة –، مصر: دار النهضة العربية الطبعة الأولى، ص ٨٠.

(٢٩٢)National office for formation Economy: Preliminary Findings from E-government Benefits Study, 2002. http://www.Egov_benefits.pdf; E-Government Act of 2002.

(٢٩٣)Glasgow City council: E-Government strategy creating a 21st Century city, Issue No 1 March 2002, p. www.glasgow.gov.uk.

ولا شك في أنّ الصلة الوثيقة بين التوقيع الإلكتروني والحكومة الإلكترونية تدفع إلى القول بأنّ الحماية المقررة لأحدها، تنطوي بطريق اللزوم على حماية الآخر(٢٩٤) ذلك أنّ الاعتداء على التوقيع أو المحرر الإلكتروني بالإتلاف أو التعييب أو التعطيل وكذا تزوير المحرر الإلكتروني الحكومي من شأنه أن ينال من ثقه الأفراد فيها ومن ثم، فإنّه فضلاً عن خضوع الجاني في تلك الأحوال لنصوص قانون التوقيع الإلكتروني الجنائية، فإنّه يخضع أيضاً بذات القدر للقواعد العامة في قانون العقوبات من حيث اعتبار المال المعتدى عليه من الأموال العامة، وكذا إسباغ صفه الرسمية على المحرر الحكومي الذي يكون محلاً للتزوير وبما يرتفع به إلى مصاف الجنايات(٢٩٥)

وممّا يؤكد الصلة بين التوقيع الإلكتروني والحكومة الإلكترونية ما نصّت عليه المادة (٢٧) من قانون التوقيع الإلكتروني الإماراتي التي نصّت على أنّه:

(١)على الرغم من وجود أي نص مخالف في أي قانون آخر، يجوز لأية دائرة أو جهة تابعة للحكومة، في أداء المهمات المناطة بهم بحكم القانون، أن تقوم بما يلي:

أ) قبول إيداع أو تقديم المستندات أو أنشائها أو الاحتفاظ بها في شكل سجلات إلكترونية.

ب) إصدار أي إذن أو ترخيص أو قرار أو موافقة في شكل سجلات إلكترونية.

ج) قبول الرسوم أو أية مدفوعات أخرى في شكل إلكتروني.

د) طرح العطاءات واستلام المناقصات المتعلقة بالمشتريات الحكومية بطريقة إلكترونية.

---

(٢٩٤) السعدي، واثبة داود. (٢٠٠٤). *الحماية الجنائية لبرامج الحاسوب*، دراسة مقدّمة إلى مؤتمر القانون والحاسوب كلية القانون بجامعة اليرموك بالأردن في الفترة من ١٢ – ١٤ تموز، ص ٩ – ١١.

(٢٩٥) قشوش، هدى حامد. (٢٠٠٣). *الحماية الجنائية التوقيع الإلكتروني*. دراسة مقدمة إلى المؤتمر الذي عقدته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة. في موضوع "القانون والكومبيوتر والإنترنت". وذلك بفندق هيلتون العين في الفترة من ١ – ٣ مايو ص ٥٨١.

(٢)إذا قررت أية دائرة أو جهة تابعة للحكومة تنفيذ أي من المهام المذكورة في الفقرة (أ) من هذه المادة فيجوز لها عندئذ أن تحدد:

أ. الطريقة أو الشكل الذي سيتم بواسطته إنشاء أو إيداع أو حفظ أو تقديم أو إصدار تلك السجلات الإلكترونية.

ب. الطريقة والأسلوب، والكيفية والإجراءات التي يتم بها طرح العطاءات واستلام المناقصات، وإنجاز المشتريات الحكومية.

ج. نوع التوقيع الإلكتروني المطلوب بما في ذلك اشتراط أن يستخدم المرسل توقيعاً رقمياً أو توقيعاً إلكترونياً محمياً آخر.

د. الطريقة والشكل الذي سيتم بها تثبيت ذلك التوقيع على السجل الإلكتروني والمعيار الذي يجب أن يستوفيه مزود خدمات التصديق الذي يقدم له المستند للحفظ أو الإيداع.

هـ. عمليات وإجراءات الرقابة المناسبة للتأكد من سلامة وأمن وسرية السجلات الإلكترونية أو المدفوعات أو الرسوم.

و. أية خصائص أو شروط أو أحكام أخرى محدّدة حالياً لإرسال المستندات الورقية، إذا كان ذلك مطلوباً فيما يتعلق بالسجلات الإلكترونية الخاصة بالمدفوعات والرسوم(٢٩٦)

الفرع الثاني: حماية التوقيع الإلكتروني في مجال المعاملات المدنية

قد يأخذ الإفصاح عن الإرادة شكل المستند الإلكتروني، ومثال ذلك أن يبرم عقد في صورة كتابة إلكترونية ويتم التوقيع عليه إلكترونياً(٢٩٧)

وممّا لا شك فيه أن تعييب التوقيع أو تزويره سواء في مرحلة إنشائه، أو بعد إتمامه، يؤدي إلى المساس بإرادة المستهلك والإخلال بحقوقه، ذلك أنّ العلم بالبيانات الجوهرية للمبيع يضمن كفالة حق

(٢٩٦) المادة ٢٧ من *قانون المعاملات والتجارة الإلكترونية* لإمارة دبي رقم ٢ لسنة ٢٠٠.

(٢٩٧) شرف الدين، أحمد شرف الدين. (٢٠٠٢). *عقود التجارة الإلكترونية وتكوين العقد وإثباته*. مصر: كلية الحقوق جامعة عين شمس ص١١٠.

المستهلك في التبصير، ويضمن سلامة إرادته من العيوب. ومن شأن الإخلال بالمستند الإلكتروني أن يخل بهذه الحقوق(٢٩٨)

أولاً/ التوقيع الإلكتروني وحقوق الملكية الفكرية والذهنية:

يتماثل التوقيع الإلكتروني مع المصنف في أنّ لصاحب كل منهما الحق في الاستئثار به، ويحق له كشف محتواه أو تقييد الاطلاع عليه ويتماثلان كذلك في أنّ المشرّع يبسط حمايته لمحتوى كل منهما فلا يمتد إليه يد العبث أو التدمير أو التشويه، كما أنّ لصاحب الحق فيهما سلطة محو مضمونها أو سحبه أياً كان الشكل الذي يفرغ فيه(٢٩٩) ومن ثم تصبح الحماية المقررة لهذه البيانات هي في الوقت ذاته حماية لحقوق الملكية الفكرية(٣٠٠) إلّا أنّ محل الحماية الجنائية للمصنف يرتكز على حماية حق المؤلف على أفكاره، والذي يأخذ الاعتداء عليه غالباً صورة المساس مادياً بمحتواه وهو ما يختلف عن مدلول الحماية الجنائية للتوقيع الإلكتروني(٣٠١)

---

(٢٩٨) New Law Makes E-Signatures Valid, Contracts created online are now as legal as those on paper, 2002. http://cobrands.Consumer.findlaw.com/internet/nolo/ency/029C847E2EFC-4913-B6DDC5849ABE81F9.html.

(٢٩٩) المادة الثانية من اتفاقية برن المعقودة في ٢٣ ديسمبر سنة ١٩٩٩.

(٣٠٠) القهوجي، على عبد القادر: *الحماية الجنائية للبيانات المعالجة إلكترونياً*، دراسة مقدمة إلى المؤتمر الذي عقدته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في موضوع "القانون والكمبيوتر والإنترنت"، وذلك بفندق هيلتون العين في الفترة من ١ – ٣ مايو سنة ص ٣٨١. وأنظر الدكتور مدحت رمضان حيث يتناول جرائم المساس بحقوق الملكية الفكرية وحق المؤلف باعتبارها من الجرائم التي تحمي التجارة الإلكترونية. أنظر الحماية الجنائية للتجارة الإلكترونية: ص ٥٧ وما بعدها. د أشرف توفيق شمس الدين – الحماية الجنائية للمستند الإلكتروني دراسة مقارنه دار النهضة العربية الطبعة الأولى ٢٠٠٦ ص ٤.

(٣٠١) فقد أعلنت الرابطة الوطنية للمستهلكين عن إحصاء الاتجاهات الاحتيال عبر الإنترنت، خلال شهر يناير – ديسمبر ٢٠٠٥ فتبيّن أنّ شكاوي المزادات عبر الإنترنت ٤٢ بالمائة من مجموع الشكاوى ومتوسط الخسارة لكل ضحية: ١٥٥، ١ دولار أمريكي كما تمثّل مبيعات السلع العامة (لا تتم من خلال المزادات) ٣٠ بالمائة من مجموع الشكاوى ومتوسط الخسارة لكل ضحية:٥٢٨، ٢ دولار أمريكي وتمثل عروض المال من نيجيريا ٨ بالمائة من مجموع الشكاوى متوسط الخسارة لكل ضحية: ٩٣٧، ٦ دولار أمريكي وترجع نسبة ٢ بالمائة من مجموع الشكاوى إلى حالات انتحال الشخصية القانونية Phishing تلك المواقع التي تصمم بطريقة تجعلها تبدو كشركات مشروعة ومؤسسات حكومية) ومتوسط الخسارة لكل ضحية: ٩١٢ دولار أمريكي

FTC, Consumer Fraud and Identity Theft Complaint Data, January December 2005, http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf

ثانياً/ التوقيع الإلكتروني والحق في الإعلام:

ويقصد بالحق في الإعلام حق كل إنسان في أن يستخلص ويتلقى وينقل المعلومات والأنباء والآراء على أية صورة دون تدخل من أحد. وهذا الحق – على هذا النحو- وثيق الصلة بالصور المختلفة لحرية الرأي والتعبير، ولا سيما حرية الصحافة والإعلام. ويعرف الإعلام الإلكتروني قبل التعاقد عبر شبكة الإنترنت بأنّه التزام قانوني سابق على إبرام العقد الإلكتروني يلتزم بموجبه أحد الطرفين الذي يملك معلومات جوهرية فيما يخص العقد المزمع إبرامه بتقديمها بوسائط إلكترونية في الوقت المناسب وبكل شفافية وأمانة للطرف الآخر الذي لا يمكنه العلم بها بوسائله الخاصة. كما أنّ الالتزام بالإعلام الإلكتروني قبل التعاقد عبر شبكة الإنترنت هو التزام عام يشمل جميع أنواع العقود التي تبرم عبر الإنترنت، كالالتزام بالمساعدة الفنية والإعداد المهني وكالالتزام بتقديم النصح والمشورة[٣٠٢] وللتوقيع الإلكتروني صلة وثيقة بالحق في الإعلام ذلك أنّه إذا كان هذا الحق الأخير يعني أنّ للفرد الحق في أن يتلقى ويطلع وينقل المعلومات، فإنّ هذه المعلومات قد يحتويها المستند الإلكتروني المتضمّن للتوقيع، غير أنّ مدلول المستند الإلكتروني لا يتطابق دائماً مع دائرة المعلومات، فقد تصاغ المعلومات في شكل مستند إلكتروني أو في غير ذلك من الصور، ويعني ذلك أنّ للمعلومات نطاقاً أوسع من نطاق المستند الإلكتروني.

الفرع الثالث: حماية التوقيع الإلكتروني في مجال التجارة الإلكترونية

تعني التجارة الإلكترونية إتمام التعاقدات بين المتعاملين عن بعد باستخدام وسائل الاتصال الإلكتروني مثل شبكة الإنترنت وغيرها[٣٠٣].

---

(٣٠٢) عمران، السيد محمد. (٢٠٠٨). *الالتزام بالإعلام الإلكتروني قبل التعاقد عبر شبكة الإنترنت*. مصر: دار النهضة العربية. ص٢٣

(٣٠٣) رمضان، مدحت عبد الحليم. مرجع سابق. *الحماية الجنائية التجارة الإلكترونية*، ص ١٥ – ١٧. وحجازي، عبد الفتاح (٢٠٠٢). *النظام القانون لحماية التجارية الإلكترونية وحمايتها مدنياً*. ط١. مصر: دار النهضة العربية. ص٢٢.

ولا يقتصر مدلول التجارة الإلكترونية على التعامل على السلع، بل أيضاً إلى تقديم الخدمات المختلفة[٣٠٤] ويتسع مدلول التجارة الإلكترونية ليشمل مرحلة ما قبل التعاقد والتي تتضمن الإعلان والترويج والعرض وصولاً لإتمام التعامل، كما أنّ مدلولها يتسع أيضاً ليشمل تنفيذ الالتزامات التي تتولد عن إبرام العقد مثل الشحن والتسليم وسداد الثمن والضمان وتقديم خدمات ما بعد البيع كالصيانة والمساعدة الفنية وغيرها[٣٠٥]

وللتجارة الإلكترونية آثار مهمة على التجارة الدولية والداخلية على حدٍ سواء. فالتجارة الإلكترونية، تعني إمكانية تبادل السلع والخدمات عبر حدود الدول ودون التقيد بإقليم معين أو جنسية معينة[٣٠٦] وللتجارة الإلكترونية بذلك مزايا وفوائد عديدة، فهي تؤدي إلى سهولة إبرام الصفقات والتصرفات القانونية الدولية، ودون الحاجة إلى وسيط. وهو ما يؤدي إلى الإقلال من النفقات وإلى تخطي العقبات والحواجز الجغرافية بين الدول[٣٠٧]

---

(٣٠٤) وسع التوجيه رقم ٤٨ لسنة ١٩٩٨ الصادر من المجلس الأوروبي من مفهوم التجارة الإلكترونية ليشمل تقديم كافة الخدمات عن بعد باستخدام وسائل إلكترونية ويقع هذا التعريف ليشمل تقديم الخدمات المهنية مثل المحاماة والاستشارات القانونية والوساطة والسمسرة والرعاية الصحية والتأمين، وخدمات التسلية مثل الفيديو عند الطلب والألعاب الإلكترونية وزيارة المتاحف إلكترونية، أو الخدمات المتعلقة بالمعلومات مثل المكتبات والصحف الإلكترونية، وخدمات التسوق والشراء عن بعد غير أنّ هذا التعريف لا يغطي تقديم خدمات البث الإذاعي والتلفزيوني، وخدمات البنك الإلكتروني والتسوق من خلال البريد أو الكتالوجات، ففي هذه الصورة ينتفي تعريف التجارة الإلكترونية لعدم تقديم الخدمة من بعد أو لأنّ الوسيلة المقدمة بها الخدمة ليست إلكترونية. كما أنّ التعريف لا يسري أيضاً في المجال المنظم بالتشريعات المالية مثل الاستثمار والخدمات البنكية الإلكترونية. Guide to Electronic Commerce Regulation, 2002, op-cit.

(٣٠٥) عبد العظيم حمدي (٢٠١١). *التجارة الإلكترونية، أبعادها الاقتصادية والتكنولوجية والمعلوماتية*. مصر: مركز البحوث بأكاديمية السادات للعلوم الإدارية. سلسلة الإصدارات. ع ٣. ص ٩ – ١٠.

(٣٠٦) Guide to Electronic Commerce Regulation, 2002 .**http://www.diffuse.org/commerce.html.**

(٣٠٧) كاثرين ل. مان/ سو إيكيرت كليلاند نايت. (٢٠٠٣). *التجارة الإلكترونية العالمية*. ترجمة الشحات منصور. مركز الأهرام للترجمة والنشر. القاهرة، الطبعة الأولى. ص ٢.

أولاً/ جريمة تزوير التوقيع الإلكتروني:[٣٠٨]

لقد نصّت على هذه الجريمة المادة (٢٣) فقرة (ب) من القانون الجديد رقم ١٥ لسنة ٢٠٠٤ والخاص بتنظيم (التوقيع الإلكتروني) – سالف الذكر– والتي ورد فيها أنّه:

"مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف أو بإحدى هاتين العقوبتين كل من: (أتلف توقيعاً، أو وسيطاً، أو محرراً إلكترونياً، أو زور شيئاً من ذلك بطريقة الاصطناع، أو التعديل، أو التحوير، أو بأي طريق آخر..). رغم أنّ النص السابق أشار إلى أكثر من صورة للاعتداء على التوقيع الإلكتروني وغيره (الوسيط، والمحرر الإلكتروني) من ذلك إتلاف، أو تعييب، أو تزوير التوقيع الإلكتروني. إلّا أنّ ما يهمنا هي الصورة الأخيرة والخاصة بتزوير التوقيع الإلكتروني فقط دون غيره من الوسائط الإلكترونية والمحررات الإلكترونية.

والجديرٌ بالذكر، أنّ المشرّع بين صور السلوك الإجرامي المكونة للركن المادي في جريمة تزوير التوقيع الإلكتروني بقوله: "أو زور شيئاً من ذلك بطريقة الاصطناع، أو التعديل، أو التحوير.." إلّا أنّ مشرّعنا المصري قد أحسن صنعاً في إطلاقه الصور التي يمكن أن يتحقق بها الركن المادي للجريمة وذلك

(٣٠٨) – يؤكد البعض أنّه بظهور الإنترنت فقدت الكتابة التقليدية قيمتها وظهر ما يعرف بالكتابة الإلكترونية، لذلك فإنّ التلاعب في التوقيع الإلكتروني بإدخال تداولات معلوماتية كاذبة يؤدي إلى التزوير في الكود، أو الرمز، أو الشفرة، أو الرقم تقوم به جريمة التزوير. السيد عتيق "*جرائم الإنترنت*" "المرجع السابق"، ص ١٢٦.

بقوله "أو بأي طريق آخر" مما ينم ذلك عن بعد نظر المشرّع فيما قد يستحدث من صور يمكن بها تغيير الحقيقة في التوقيع الإلكتروني أو تزوير التوقيع الإلكتروني.[٣٠٩]

تجدر الإشارة إلى أنّ أسلوب تزوير التوقيع الإلكتروني له طبيعة خاصة تختلف عن أسلوب جريمة التزوير التقليدية يتمثل ذلك في استخدام الكمبيوتر في إجراء التزوير، لأنّ المستندات التي يتم التوقيع عليها هي في الأصل مستندات معالجة آلياً (des documents informatisés) وليست محررات (des écritires) مكتوبة بالمفهوم التقليدي[٣١٠] غني عن الذكر أنّ جريمة تزوير التوقيع الإلكتروني (جريمة عمدية) يتخذ الركن المعنوي (القصد الجنائي العام) بعنصرية العلم والإرادة، فيجب توافر علم الجاني بوقائع الجريمة، واتجاه إرادته إلى تحقيق النتيجة الإجرامية المرجوة أو التي يسعى إليها.

حقيقة أنّ نصّ المادة السابقة إنّما جاء يضفي حماية جنائية ظل الكثيرون في انتظارها – لا سيما البنوك والمتعاملون بنظام التجارة الإلكترونية – فلقد أوضحنا من قبل أهمية التوقيع الإلكتروني بالنسبة لنظام التعامل بالبطاقات سواء في السحب من الموزعات الآلية أو في الوفاء لدى التجار لا سيما المؤسسات التجارية الكبرى التي تعرض منتجاتها عبر شبكات الإنترنت وتقبل الوفاء باستخدام أرقام البطاقات.

ونصّت المادة رقم من القانون الكويتي رقم ٣. السنة ٢٠١٤ في شأن المعاملات الإلكترونية على أن يكون كل من السجل الإلكتروني والمستند الإلكتروني والرسالة الإلكترونية والمعاملة الإلكترونية والتوقيع الإلكتروني في مجال المعاملات المدنية والتجارية والإدارية منتجة لذات الأثار القانونية المترتبة

(٣٠٩) يؤكد بعض الفقه أنّ الركن المادي في جريمة تزوير التوقيع الإلكتروني لا يختلف عن الركن المادي في جريمة التزوير التقليدية من حيث عناصره من تغيير الحقيقة بإحدى الطرق المنصوص عليها قانوناً للتزوير – على التفصيل السابق – بالإضافة إلى ضرورة توافر الضرر – على التفصيل السابق. هدى حامد قشقوش *"الحماية الجنائية للتوقيع الإلكتروني"* "المرجع السابق"، ص ٥٨٣.

(٣١٠) هدى حامد قشقوش. *"الحماية الجنائية للتوقيع الإلكتروني"*. المرجع السابق. ص ٥٨٤.

على الوثائق والمستندات والتوقيعات الكتابية من حيث إلزامه لأطرافه. أو قوته في الإثبات أو حجيته متى أجري وفقاً لأحكام هذا القانون". ونصّت المادة ١٠ من القانون الاتحادي الإماراتي رقم ١ لسنة ٢٠٠٦م بشأن المعاملات والتجارة الإلكترونية على أن: "

١. لا يحول دون قبول الرسالة الإلكترونية أو التوقيع الإلكتروني كدليل إثبات:

أ. أن تكون الرسالة أو التوقيع قد جاء في شكل إلكتروني.

ب. أن تكون الرسالة أو التوقيع ليس أصلياً أو في شكله الأصلي، متى كانت هذه الرسالة أو التوقيع الإلكتروني أفضل دليل يتوقع بدرجة معقولة أن يحصل عليه الشخص الذي يستشهد به.

٢. في تقدير حجية المعلومات الإلكترونية في الإثبات، تراعي العناصر الآتية:

أ. مدى إمكانية الاعتداد بالطريقة التي تم بها تنفيذ واحدة أو أكثر من عمليات إدخال المعلومات أو إنشائها أو تجهيزها أو تخزينها أو تقديمها أو إرسالها.

ب. مدى إمكانية الاعتداد بالطريقة التي استخدمت في المحافظة على سلامة المعلومات.

ج. مدى إمكانية الاعتداد بمصدر المعلومات إذا كان معروفاً.

د. مدى إمكانية الاعتداد بالطريقة التي تم بها التأكد من هوية المنشئ.

هـ. أي عنصر آخر يتصل بالموضوع.

٣. ما لم يتم إثبات عكس ذلك. يفترض أنّ التوقيع الإلكتروني المحمي:

أ. يمكن الاعتداد به.

ب. هو توقيع الشخص الذي تكون له صله به.

ج. قد وضعه ذلك الشخص بنية توقيع أو اعتماد الرسالة الإلكترونية المنسوب إليه إصدارها

٤. ما لم يتم إثبات عكس ذلك يفترض أنّ السجل الإلكتروني المحمي:

أ. لم يتغير منذ أن أنشئ.

ب. معتد به.

ونصّت المادة ١١ من القانون ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات على أن يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو من النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون". ونصّت المادة (٧) من المرسوم سلطاني العماني رقم (٢٠٠٨/٦٩) بإصدار قانون المعاملات الإلكترونية على أن تنتج الرسالة الإلكترونية أثرها القانوني وتعتبر صحيحة وقابلة للتنفيذ شأنها في ذلك شأن الوثيقة المكتوبة إذا روعي في إنشائها واعتمادها الشروط المنصوص عليها في هذا القانون واللوائح والقرارات الصادرة تنفيذاً لأحكامه".

تتعدّد أشكال التوقيع الإلكتروني وهناك طرق مضى عليها وقت كبير وطرق حديثة وقد يتم اكتشاف طرق جديدة في المستقبل، وسأقوم بذكر صور التوقيع الإلكتروني على النحو التالي[٣١١]:

(١)التوقيع الرقمي (التشفير):

حيث يعتبر التوقيع الرقمي أو التشفير أحد أهم أنواع التوقيع الإلكتروني نظراً لشيوعه ويعتبر بمثابة الحدث التكنلوجي الثالث الأهم في القرن العشرين بعد تنظيم النسل والقنبلة النووية، ويتم التوقيع الرقمي عن طريق التشفير وذلك باستخدام مفاتيح سرية وطرق حسابية معقدة (لوغاريتمات) تؤدي

(٣١١) خالد ممدوح إبراهيم. المرجع السابق، ص ١٩٩.

لتحويل التوقيع أو الكتابة من رسالة مفهومة ومقروءة إلى رسالة رقمية غير مقروءة وغير مفهومة، وقد قام المشرّع بحماية التشفير من الاعتداء، كما نصّت المادة (٤٨) من القانون التونسي رقم ٨٣ لسنة ٢٠٠٠ م، في شأن المبادلات والتجارة الإلكترونية، الذي يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية معلقة بإمضاء غيره بالسجن لمدة لا تتراوح ٦ أشهر وعامين وغرامة تتراوح ما بين ١٠٠٠ إلى ١٠٠٠٠ دينار أو بإحدى هاتين العقوبتين. أمّا القانون الإماراتي فقد نصّ في المواد من (٢٦) إلى (٣٣) تتعامل مع العقوبات المفروضة على مخالفة أحكام هذا القانون. وسيتّم معاقبة أي شخص ينشر أو يوفّر أو يقدم شهادة مصادقة إلكترونية تحتوي على معلومات غير صحيحة بالسجن لمدّة لا تقل عن عام وأو دفع غرامة لا تقل عن ٥٠,٠٠٠ درهم ولا تزيد على ٢٥٠,٠٠٠ درهم. كما تناقش هذه المواد العقوبات المفروضة على تقديم بيانات غير صحيحة عن عمد إلى مزوّد خدمات التصديق بغرض طلب الحصول على أو إلغاء أو إيقاف شهادة المصادقة الإلكترونية.

(٢)التوقيع البيومتري:

يصنف التوقيع البيومتري باعتباره صورة للتوقيع من خلال الخصائص البيولوجية لصاحب التوقيع كبصمة الإبهام أو بصمة شبكية العين أو بصمة الصوت أو بصمة الشفاه، فيتم دراسة الشخصية من المظهر الخارجي للأداء كما في تحديد خط الإنسان بدراسة درجة ضغط اليد على القلم وكمية الاهتزازات التي تصدرها اليد عند الكتابة.

(٣)التوقيع باستخدام الرقم السري:

يتم هذا النوع من التعامل في التوقيع عن طريق التعامل مع البنوك والأفراد وعملائه، بإعطاء الأفراد بطاقات ممغنطة تسمح لهم بسحب النقود من خزائن البنك والبنوك الأخرى والقيام بعمليات

الشراء من المحلات التجارية والدفع عن طريق هذه البطاقة، وذلك عن طريق كتابة حامل البطاقة أرقاماً سرية تعطى له.

(٤)حجية التوقيع الإلكتروني وشروطه في القانون الإماراتي

لقد نصت المادة (٢٠) على أنّه: "يعامل التوقيع على أنّه توقيع إلكتروني محمي إذا كان من الممكن التحقق من خلال تطبيق إجراءات توثيق محكمة، منصوص عليها في هذا القانون أو معقولة تجارياً ومتفق عليها بين الطرفين. ومن نص المادة السابقة نجد بأنّ المشرّع الإماراتي يمنح الحجية للتوقيع الإلكتروني في حالة كان هذا التوقيع محمي من خلال إجراءات معينة وواضحة، وأن تكون تلك الإجراءات منصوص عليها في القانون، أو معقولة جرى التعامل عليها تجارياً، وتم الاتفاق عليها بين الطرفين (الموقّع إلكترونياً والجهة المستقبلة للتوقيع).

وتنقسم العقود الإلكترونية من حيث كيفية تنفيذها إلى نوعين، منها ما يبرم عبر الإنترنيت وينفذ خارجها، حيث يشمل هذا النوع العقود التي يكون محلها الأشياء المادية التي يقتضي تسليمها في بيئة مادية، والنوع الآخر من هذه العقود ما يبرم وينفذ عبر شبكات الاتصال ذاتها، حيث يشمل العقود التي يكون محلها الأشياء غير المادية وتقديم الخدمات، ومنها عقود الاشتراك في الإنترنيت وعقود الاشتراك في بنوك المعلومات وعقود الإعلانات وغيرها.

إنّ العقد المبرم بالطريقة التقليدية يعتمد على الكتابة والتوقيع التقليديين كعامل إسناد في الإثبات، في حين أنّ العقد الذي يبرم عن طريق شبكة المعلوماتية يقوم على تبادل البيانات إلكترونياً على دعامات غير ورقية داخل أجهزة الاتصال أو خارجها والتوقيع عليها ممن يرسل الرسالة الإلكترونية

بواسطة التوقيع الإلكتروني، لذا فإننا سنتناول في هذا المطلب مفهوم كل من المحررات الإلكترونية والتوقيع الإلكتروني ودورهما في إثبات العقد الإلكتروني.

ثانياً/ دور المحررات الإلكترونية الموقعة إلكترونياً في إثبات الجرائم الواقعة على التوقيع:

لا يوجد في الأصل اللغوي لكلمة محرر ما يقتصر معناها على نوع معين من الدعامات سواء كانت ورقاً أو غير ذلك إذ أنّ معنى المحرر وفقاً للمفهوم اللغوي هو: "كل ما يستند إليه ويعتمد عليه"(٣١٢) وبعد أن كان محل الإثبات ينحصر فقط بالمستند الورقي أصبحت البيانات والمستندات عبارة عن تسجيلات إلكترونية وهذا لم تعد فكرة المحرر تقتصر على مفهومها القانوني التقليدي السائد فأصبحت بعد ذلك منصبة على المحرر الإلكتروني على حد سواء وهذا ما يوجب على رجل القانون تغيير نظرته للمحرر بمفهومه التقليدي ويلاحظ على هذا التغير لن يكون قانونياً فحسب بل نفسياً في المقام الأول. وإذا كانت الكتابة هي الوسيلة الأساسية لإثبات التصرفات القانونية فإنه لا يوجد ما يمنع من أن تكون الكتابة محررة على دعامات وسائل الاتصال الحديث وخاصة شبكة المعلومات حتى ولو لم تكن في صورتها التقليدية، فالكتابة عندما تتخذ الطابع الإلكتروني توصف بأنّها كتابة إلكترونية أو محررات إلكترونية، وعليه سنتناول في هذا المطلب تعريف هذه المحررات وشروط اعتمادها ومدى حجيتها في الإثبات.(٣١٣)

تعريف المحرر الإلكتروني: عرّف المحرر الإلكتروني بأنّه: "ما هو مكتوب على نوع معين من الدعامات سواء أكان ورقاً أم غير ذلك من الوسائل الإلكترونية"(٣١٤)ة وعرّف من خلال رسالة البيانات الإلكترونية بأنّه: "معلومات إلكترونية ترسل أو تسلم بوسائل إلكترونية أياً كانت وسيلة استخراجها في

(٣١٢) شرف الدين، أحمد. (٢٠١٤): *قواعد الإثبات في المسائل المدنية والتجارية*. مصر: مطبعة نادي القضاة. ص ١١٤.

(٣١٣) توفيق فرج. (١٩٨١). قواعد *الإثبات في المواد المدنية والتجارية*. طبعة نادي القضاة. ص ١٦٦.

(٣١٤) العجلوني، أحمد خالد. (٢٠٠٥). *التعاقد عن طريق الإنترنت*، دراسة مقارنة. مصر: دار الثقافة. ص ٤٥.

المكان المستلمة فيه، أو أنّه البيانات والمعلومات التي يتم تداولها بين المتعاقدين إلكترونياً يتم تبادلها من خلال وسائل إلكترونية سواء كانت من خلال شبكة الإنترنيت أم من خلال الأقراص الصلبة أو شاشات الحاسب الآلي أو أيّة وسائل إلكترونية[٣١٥]". حيث يرتب العقد الإلكتروني كغيره من العقود الأخرى التزامات على عاتق كل متعاقد في مواجهة المتعاقد الآخر.

ثالثاً/ دور التوقيع الإلكتروني التقليدي في الإثبات:

لكي يكون العقد الإلكتروني ذو قيمة قانونية وينتج آثاره فلا بد من التوقيع عليه، وإذا كان العقد الذي يبرم بصورة تقليدية يتم التوقيع عليه عن طريق الإمضاء أو البصمة أو الختم فإن العقد الإلكتروني يتم التوقيع عليه عن طريق استخدام التوقيع الإلكتروني وهذا ما سنتناوله في هذا المطلب وعلى النحو الآتي:

١ – تعريف التوقيع الإلكتروني: عرّف التوقيع الإلكتروني بتعاريف عدة تبعاً لاختلاف النظرة إليه فقد عرّف بناءً على الرسائل التي يتم بها أو بحسب الوظيفة التي يؤديها أو بناءً على التطبيقات العملية التي يتم بها، فقد عرّف بأنّه: "الرمز المصدري أو السري الذي يتم إدخاله في جهاز الحاسب عن طريق الرسائل الإدخال ليتم من خلاله إنجاز بعض المعاملات باتباع إجراءات محددة متفق عليها بين أطراف الالتزام وضمن الحدود التي تم الاتفاق عليها بين أو أنّه المعطيات التي تأخذ الشكل الإلكتروني والتي ترتبط بمعطيات إلكترونية أخرى تستخدم لإثبات صحتها أو أنّه مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته"[٣١٦] وقد عرّفته لجنة أعمال التجارة الدولية التابعة للأمم المتحدة عام ١٩٩٦ بأنّه: "عبارة

---

(٣١٥) رامي علوان (٢٠٠٢) : *التعبير عن الإرادة عن طريق الإنترنت وإثبات التعاقد الإلكتروني،العراق:* مجلة الحقوق جامعة الكويت، السنة السادسة والعشرون، العدد الرابع ديسمبر م، ص ٢٦٢.

(٣١٦) د. محمد فواز المطالقة، الوجيز في عقود التجارة الإلكترونية، عمان، ٢٠٠٦، ص ١٧٣.

عن مجموعة أرقام تمثل توقيعاً على رسالة معينة بحيث يتحقق هذا التوقيع من خلال الإجراءات الحسابية المرتبطة بمفتاح رقمي خاص بالشخص المرسل ومن خلال الضغط على هذه الأرقام الخاصة لمستخدم الشبكة المعلوماتية يتكون التوقيع الإلكتروني"[٣١٧] وقد عرّفه المشرّع الأردني بأنّه: "البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أية وسيلة أخرى مماثلة في رسائل معلومات أو مضافة عليها أو مرتبطة بها ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره من أجل توقيعه وبغرض الموافقة على مضمونه.

في حين عرّفه المشرّع الإماراتي بأنّه: "التوقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذي شكل إلكتروني وملحق أو مرتبط منطقياً برسالة إلكترونية وممهور بنية توثيق أو اعتماد الرسالة"[٣١٨] وعرّفه المشرّع البحريني بأنّه: "معلومات في شكل إلكتروني تكون موجودة في سجل إلكتروني أو مثبتة أو مقترنة به منطقياً ويمكن للموقع استعمالها لإثبات هويته.[٣١٩]

٢- حجية التوقيع الإلكتروني في الإثبات:

إذا كان التوقيع اليدوي في فترة من الفترات أفضل طريقة للتوقيع فهو لم يعد ملائماً للصور الحديثة للتعاملات التي أخذت الشكل الإلكتروني والتي يتعذر معها توافر التوقيع لذلك ظهر بديلاً عنه وهو التوقيع الإلكتروني[٣٢٠] وقد بذل الفقه جهوداً كبيرة لمحاولة جعل مفهوم التوقيع يتسع ليشمل التوقيع الإلكتروني باعتبار أنّ التوقيع الذي لم تعرفه القوانين هو وسيلة للتعبير عن إرادة صاحبه وبالتالي لا

(٣١٧) محمد إبراهيم أبو الهيجاء، عقود التجارة الإلكترونية، عمان، ٢٠٠٥ م، ص ٨٣.

(٣١٨) خالد ممدوح إبراهيم: المرجع السابق، ص ١٩٢.

(٣١٩) خالد ممدوح إبراهيم: المرجع السابق، ص ١٩٣.

(٣٢٠) نجوى أبو هيبة: *التوقيع الإلكتروني*، دار النهضة العربية، القاهرة، ٢٠٠٤ م، ص ٣٧.

يشترط أن يكتب بخط اليد[٣٢١] وإذا ارتبط التوقيع باعتباره دليلاً للإثبات بالكتابة لذلك لإسباغ الحجية القانونية على التوقيع الإلكتروني أن تتوافر في الرسالة أو المحرر المراد تصديقه بالتوقيع شروط الدليل المكتوب باعتباره وسيلة للتوثيق وذلك بالإضافة إلى الشروط اللازم توافرها في التوقيع ذاته والتي تمكنه من أداء وظيفته من تحديد الشخصية الموقع أو إقرار بمضمون المحرر ونسبته إلى الموقع والشروط التي يلزم توافرها لتحقيق الدليل الكتابي هي أن يكون الدليل مقروءً ومستمراً وغير قابل للتعديل.

ومع التقدم التقني أمكن للمستندات الإلكترونية كما لاحظنا أن تستوفي الشروط الواجب توافرها لتحقيق الدليل الكتابي الذي يتمتع بالحجية في الإثبات أمّا الشروط الواجب توافرها في التوقيع ذاته ليتمتع بالحجية القانونية في الثبات فيمكن ردّها إلى الدور أو الوظيفة التي يؤديها التوقيع وهي تحديد هوية الموقع الذي يستند إليه الدليل أو المستند والتعبير عن إرادة الموقّع في الالتزام بما وقّع عليه ولقد أضافت التشريعات الصادرة بهذا الخصوص الحجية القانونية على التوقيع الإلكتروني ومنها التوجيه الأوربي الخاص بالتجارة الإلكترونية وقانون الأونسترال النموذجي وقانون المعاملات الإلكترونية الألماني وقانون التجارة الإلكترونية في بريطانيا وقانون المعاملات الإلكترونية التونسي وقانون المعاملات الإلكترونية الأردني وقانون المعاملات والتجارة الإلكترونية لإمارة دبي وقانون التجارة الإلكترونية البحريني[٣٢٢] وتتفق جميع هذه التشريعات على ضرورة توافر شروط معينة تعزز من هذا التوقيع وتوفر فيه الثقة حتى يتمتع بالحجية وتدور هذه الشروط حول كون التوقيع مقصوراً على صاحبه وخاضعاً لسيطرته الفعلية وقابليته للتحقق من صحته مع ارتباطه بالبينات التي يثبته.

---

(٣٢١) زهرة، محمد المرسي (١٩٩٤): *مدى حجية التوقيع الإلكتروني في الإثبات في المسائل المدنية والتجارية*، بحث مقدم إلى مؤتمر والقانون المنعقد في ٢٩ يناير، م، ص ٧٣.

(٣٢٢) المادة (٥) من قانون المعاملات الإلكترونية البحريني.

رابعاً/ الطبيعة القانونية للعقد الإلكتروني:

- **الاتجاه الأول**[٣٢٣]: يذهب بعض الفقه، الإنكليزي والفرنسي والعربي إلى أنّ العقد الإلكتروني هو عقد إذعان على اعتبار أنّ المتعاقد لا يملك إلّا أن يضغط في عدد من الخانات المقترحة أمامه في موقع المتعاقد الآخر على مواصفات معينة ومنها مواصفات السلعة وثمنها المحدد مقدماً ولا يملك أن يناقش أو يعارض المتعاقد الآخر حول شروط التعاقد التي يوردها على الموقّع، فهو لا يكون أمامه إلّا التوقيع في حالة القبول أو عدم التوقيع في حالة الرفض، ويعتمد أنصار هذا الاتجاه إلى تغليب المعيار الاقتصادي إذ ينشأ الإذعان عندما يكون هنالك تفاوت بين الطرفين وتنعدم المساواة القانونية والفعلية بين إرادتيهما فأحدهما يتمتع بنفوذ قوي والآخر ضعيف بسبب حاجته الملحة للتعاقد.
- **الاتجاه الثاني**[٣٢٤] يذهب أنصار هذا الاتجاه إلى أنّ العقد الإلكتروني ما هو إلّا عقد رضائي وإن لم يكن من العقود المسماة إذ ينظر إلى كل عقد على حدي، وذلك لأنّ المتعاقد يستطيع اللجوء إلى مورد أو منتج آخر للسلعة أو الخدمة إذ لم تعجبه شروط أحد، كما أنّه لا يمكن الاعتماد على المعيار الاقتصادي فقط وإنّما يجب النظر إلى الاعتبارين القانوني والاقتصادي معاً وذلك لأنّ عقود الإذعان هي من عقود الاحتكار والمنافسة الضعيفة مثل عقد توريد الكهرباء أو الغاز ويكون احتكار هذه السلع احتكاراً قانونياً أو فعلياً.
- **الاتجاه الثالث**[٣٢٥]: يذهب رأي فقهي ونحن نتفق معه إلى أنّه يجب التمييز بين نوعين من العقود الإلكترونية عند تحديد الطبيعة القانونية إذ أنّ العقود الإلكترونية من حيث آلية إبرامها هي إمّا عقود

---

(٣٢٣) المومني، عمر حسن. (٢٠٠٣). *التوقيع الإلكتروني وقانون التجارة الإلكترونية*. الأردن: دون دار نشر. عمان ص ٣٤.

(٣٢٤) أبو الليل، ابراهيم الدسوقي. (٢٠١٦). *إبرام العقد الإلكترونية في ضوء أحكام القانون الإماراتي والقانون المقارن*، الإمارات: دون دار وسنة نشر. ص ٢٤.

(٣٢٥) د. إبراهيم الدسوقي أبو الليل. المرجع السابق، ص ٢٨.

يتم إبرامها عن طريق البريد الإلكتروني للمتعاقدين أو عن طريق المواقع الإلكترونية، فالعقود التي يبرم عن طريق المواقع الإلكترونية قد تحتوي على سمات عقود الإذعان أما بالنسبة إلى العقود التي تبرم عن طريق البريد الإلكتروني فغالباً ما تكون عقود رضائية إذ يتم التفاوض على إبرام العقد عن طريق إرسال الرسائل الإلكترونية بين المتعاقدين عن طريق المواقع الشخصية الإلكترونية إلى أن يقترن إيجاب أحد المتعاقدين بقبول الآخر فينعقد العقد.

فإنّ استخدام التوقيعات الإلكترونية عادة يتضمن عمليتين، واحدة يتم إنجازها من قبل الموقع والأخرى من قبل مستلم التوقيع الإلكتروني:

١) إنشاء التوقيع الإلكتروني يستخدم نتيجة هاش يتم اشتقاقها من وتكون مقتصرة على كل من الرسالة الموقعة ومفتاح خاص معين. بغرض أن تكون نتيجة الـ هاش آمنة ومحكمة يجب ألا يكون هناك إمكانية أو احتمال ضئيل فقط بأنّ نفس التوقيع الإلكتروني يمكن إنشائه من خلال تركيبة أي رسالة أخرى أو مفتاح خاص آخر.

٢) التثبت من صحة التوقيع الإلكتروني: وهي عملية التأكد من التوقيع الإلكتروني من خلال الرجوع إلى الرسالة الأصلية وإلى مفتاح عام معين وبهذا يتم تحديد ما إذا كان التوقيع الإلكتروني قد تم إنشائه لتلك الرسالة باستخدام المفتاح الخاص المقابل للمفتاح العام المشار إليه.

مّا تقدّم تظهر العلاقة بين التوقيع الإلكتروني والتشفير، فالتوقيع الإلكتروني هو ختم رقمي مشفر، يملك مفتاحه صاحب الختم. ويعني تطابق المفتاح مع التوقيع الرقمي على الرسالة الإلكترونية على أنّ مرسل الرسالة هو من أرسلها فعلاً، وليست مرسلة من قبل شخص آخر. ويضمن التوقيع الرقمي عدم تعرض الرسالة لأي نوع من أنواع التعديل، بأي طريقة. لذلك يعتبر التشفير إجراء تقني يسمح بزيادة الأمان والثقة في التجارة الإلكترونية ويضمن السرية الكاملة في ذلك والحيلولة دون تعديلها أو اختراقها.

وقد اكتشف التشفير سنة ١٩٨٠ من قبل ثلاثة علماء، وعرّفوا علم التشفير بأنّه العلم الذي يعتمد على وسائل وطرق تجعل من المعلومة غير مفهومة وغير مقروءة إلّا لأطرافها، حيث يتأكد كل من المرسل والمرسل إليه عدم تسليم الرسالة لطرف ثالث غيرهما، يتم الاطلاع على البيانات إلكترونياً في المعاملات التجارية والإدارية باستخدام مفتاحين الأول عام معروف لعامة الناس أمّا الثاني فهو مفتاح خاص لا يعلمه سوى صاحبه، استعمال المفتاحين دلالة قاطعة على التأكد من هوية الأطراف اللذين قد يثبت من ذلك الإجراء رغبتيهما في التعاقد. وتتلخص أغراض التشفير في الاتي: –

أ. توثيق الموقّع:

في حال كان هناك زوج من المفاتيح واحد عام والآخر خاص وكانا مرتبطين بموقع معين ومحدد فإنّ التشفير ينسب ويعزو الرسالة إلى الموقّع. ولا يمكن تزوير التوقيع الإلكتروني ما لم يفقد الموقّع السيطرة على المفتاح الخاص (تعرض المفتاح الخاص للخطر) كأن يقوم بإفشائه أو يفقد الوسط أو الوسيلة المحتفظ به فيها مثل البطاقة الذكية.

ب. توثيق الرسالة:

كذلك فإنّ التشفير يعمل على تحديد هوية الرسالة الموقعة بثقة ودقة ويقين أكثر من التوقيعات على الورق. إنّ عملية التثبت من الصحة تكشف أي تلاعب حيث أنّ أي مقارنة بين الواحدة يتم إعدادها عند التوقيع والأخرى عند التثبت من الصحة تبيّن ما إذا كانت الرسالة هي نفسها عندما تم توقيعها.

ج. الفعالية:

إنّ عمليات إنشاء التوقيع الإلكتروني والتثبت من صحته بالتشفير تتطلب مستوى عال من الضمان بأنّ التوقيع الإلكتروني هو للموقّع بدون تكلف أو رياء. مقارنة مع الأساليب الورقية مثل

بطاقات نموذج اعتماد التوقيع والتي هي أساليب مملة وتستغرق الكثير من الجهد بحيث أنّه نادراً ما يتم استخدامها بالواقع – فإنّ التوقيعات الإلكترونية تعطي وتولد درجة ضمان أعلى بدون أن تضيف كثيراً على الموارد المطلوبة للمعالجة.

خامساً/ الجانب القانوني للتشفير:

إنّ كلمة تشفير يونانية الأصل وتعني باللغة الإنكليزية (متخفي أو سري) ويعرّف التشفير اصطلاحاً بأنّه عملية تمويه الرسائل أو المعلومات أو البيانات بشكل لا تقرأ من أحد سوى من الموجهة إليه. وعرّفه آخرين بأنّه (استبدال شكل البيانات من خلال تحويلها إلى رموز أو إشارات لمنع الغير من معرفتها أو تعديلها أو تغييرها، فالتشفير وسيلة فنية لحماية البيانات من الآخرين. في حين عرّفه ثالث بأنّه (عملية الحفاظ على سرية المعلومات الثابت منها والمتحرك باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير لهم بذلك لا يستطيعون فهم أي شيء لأن ما يظهر لهم هو خليط من الرموز والأرقام والحروف غير المفهومة)، وقد تطرّقت القوانين العربية المنظمة للتوقيع الإلكتروني إلى تعريف التشفير وتبيان مدلوله فالقانون التونسي مثلاً عرّفه في الفصل الأول بالآتي (التشفير: إمّا استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها).

أمّا المشرّع البحريني فلم يأت بتعريف للتشفير على نحو صريح كما هو في القانون التونسي إنّما ذكره تحت باب التعريفات في المادة الأولى معرفاً لمصطلح بيانات إنشاء التوقيعات بأنها بيانات فريدة كالرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء توقيع إلكتروني. ثم أضاف في تحديده لمصطلح بيانات التحقق من التوقيعات بأنّها كالرموز أو مفاتيح التشفير العامة التي تستعمل لغرض

التحقق من صحة توقيع إلكتروني. وكأنّ المشرّع البحريني يفرق بين نوعين من التشفير على أساس من يقوم بعملية التشفير هل هو المستخدم للشبكة أم الجهة المسؤولة عن إصدار شهادات تثبت موثوقية التوقيع.

وللتثبت من صحة توقيع إلكتروني معين لا بد من وجود استراتيجية مقنعة لكي يتم ربط شخص أو هيئة معينة بزوج المفاتيح. إنّ الحل لهذا هو استخدام طرف ثالث واحد أو أكثر يكون موثوق به لكي يربط موقع معين مع مفتاح عام محدّد. تلك الجهة الثالثة الموثوق بها يشار إليها بعبارة "جهة التصديق الإلكتروني" يقوم بإصدار شهادة في اعتماد توقيع معين لجهة معينة.

وقد عرّف القانون النموذجي الموحد للتوقيع الإلكتروني شهادة التصديق في المادة ٢ الفقرة ب منه بأنّها تعني (رسالة بيانات أو سجلاً آخر يؤكدان الارتباط بين الموقّع وبيانات إنشاء التوقيع)، كما عرّف مقدّم خدمات التصديق في الفقرة ٥ من نفس المادة بالقول (يعني شخصاً يصدر الشهادات ويجوز أن يقدّم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية).

وقد وردت القوانين العربية أيضاً تعريفات مشابهة لما ورد في القانون النموذجي منها القانون المصري للتوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤ والذي عرّف في المادة ١ / الفقرة هاء الموقّع بأنّه (الشخص الحائز على بيانات إنشاء التوقيع ويوقّع عن نفسه أو عمن ينيبه أو يمثله قانوناً) ثم انتقل في الفقرة (و) من نفس المادة ليعرف شهادة التصديق الإلكترونية بأنّها (الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع). كما عرّف القانون الأردني للمعاملات الإلكترونية رقم ٨٥ لسنة ٢٠٠١ شهادة التوثيق في المادة ٢ منه على أنها: الشهادة التي تصدر عن جهة مختصة مرخصة أو معتمدة لإثبات نسبة توقيع إلكتروني إلى شخص معين استناداً إلى إجراءات توثيق معتمدة.

ولكي يتم ربط زوج من المفاتيح بموقع محتمل تقوم "جهة التصديق الإلكتروني" بإصدار شهادة، سجل إلكتروني يذكر فيه المفتاح الشفري العام على أنّه "موضوع" الشهادة ويؤكد بأنّ الموقّع المحتمل المعرّف عنه في الشهادة يحمل المفتاح الخاص المقابل. يشار إلى الموقّع المحتمل بعبارة "المشترك". إنّ وظيفة الشهادة الرئيسية هي ربط زوج من المفاتيح مع مشترك معين. أي "مستلم" للشهادة يرغب في الاعتماد على والوثوق بتوقيع إلكتروني ينشئه المشترك المذكور في الشهادة (عندئذ يصبح المستلم هو الطرف المعتمد) بإمكانه استخدام المفتاح الشفري العام المذكور في الشهادة للتثبت من صحة التوقيع الإلكتروني أي بأنّه تم إنشائه بواسطة المفتاح الخاص المقابل. في حال نجحت عملية التثبت من الصحة فإنّ هذه السلسلة من الوقائع والمقدمات توفر الثقة والضمان بأنّ المفتاح الخاص المقابل محتفظ به من قبل المشترك المذكور اسمه في الشهادة وبأن التوقيع الإلكتروني قد تم إنشائه من قبل ذلك المشترك.

ولتأكيد صحة كل من الرسالة والهوية في الشهادة تقوم جهة التصديق الإلكتروني بتوقيعها إلكترونياً. إنّ التوقيع الإلكتروني لجهة التصديق الإلكتروني على الشهادة يمكن التثبت من صحته باستخدام المفتاح الشفري العام الخاص بجهة التصديق الإلكتروني والمذكور في شهادة أخرى من قبل جهة تصديق إلكتروني أخرى (والتي يمكن أن تكون على مستوى أعلى فيما يتعلق بالرتبة ولكن ذلك ليس بالضرورة) وتلك الشهادة الأخرى يمكن توثيقها بدورها بواسطة المفتاح الشفري العام المذكور كذلك في شهادة أخرى وهكذا.. حتى يتثبت الشخص المعتمد على التوقيع الإلكتروني من صحته. في كل حالة فإنّ جهة التصديق الإلكتروني المصدرة للشهادة يجب أن توقّع إلكترونياً على شهادتها الخاصة بها خلال الفترة التشغيلية للشهادة الأخرى المستخدمة للتثبت من صحة التوقيع الإلكتروني لجهة التصديق الإلكتروني.

إنّ أي توقيع إلكتروني سواء تم إنشائه من قبل مشترك معين لتوثيق رسالة ما أو تم إنشائه من

قبل جهة تصديق إلكتروني لتوثيق شهادتها (بالفعل رسالة متخصصة) يجب أن تكون مختومة زمنياً بشكل موثوق به وذلك كي يستطيع المتثبت من الصحة تحديد ما إذا كان التوقيع الإلكتروني قد تم إنشائه خلال مدة الصلاحية المذكورة في الرسالة.

ولكي يكون مفتاح عام وتعريفه مع مشترك معين متوفرين بسرعة وسهولة للاستخدام في التثبت من الصحة، يمكن نشر شهادة في حافظة أو يتم توفيرهم من خلال أي طريقة أخرى. إنّ الحافظات هي عبارة عن قاعدة بيانات إلكترونية من الشهادات والمعلومات الأخرى المتوفرة للاسترجاع والاستخدام في التثبت من صحة التوقيعات الإلكترونية. يمكن القيام بالاسترجاع أوتوماتيكياً من خلال أمر برنامج التثبت من الصحة بأن يستفسر مباشرة من الحافظة للحصول على الشهادات المطلوبة. أمّا عن كيفية عمل هذه التكنلوجيا فيمكن توضيحه بالنقاط الآتية:

- أولاً: يتم التقدم إلى الهيئة المتخصصة بإصدار الشهادات
- ثانياً: يتم إصدار الشهادة ومعها المفتاح العام والخاص للمستخدم الجديد
- ثالثاً: عندما ترسل الرسالة الإلكترونية تقوم أنت بتشفير الرسالة باستخدام المفتاح العام التابع للمستقبل أو المفتاح الخاص بك وفي كلتا الحالتين يتم إرفاق توقيعك الإلكتروني داخل الرسالة
- رابعاً: يقوم البرنامج الخاص بالمستقبل بإرسال نسخة من التوقيع الإلكتروني إلى الهيئة التي أصدرت الشهادة للتأكد من صحة التوقيع.
- خامساً: تقوم أجهزة الكمبيوتر المتخصصة في الهيئة بمراجعة قاعدة البيانات الخاص بها ويتم التعرف على صحة التوقيع وتعاد النتيجة والمعلومات الخاصة بالشهادة إلى الأجهزة الخاصة بالهيئة مرة أخرى.
- سادساً: يتم إرسال المعلومات والنتيجة إلى المستقبل مرة أخرى ليتأكد من صحة وسلامة الرسالة.
- سابعاً: يقوم المستقبل بقراءة الرسالة وذلك باستخدام مفتاحه الخاص إذا كان التشفير قد تم على

أساس قمة العام أو بواسطة الرقم العام للمرسل إذا تم التشفير بواسطة الرقم الخاص للمرسل، ومن ثم يجيب على المرسل باستخدام نفس الطريقة وهكذا تتكرر العملية.

المهم من الناحية القانونية هو الالتزامات التي يمكن أن تقع على كل طرف من الأطراف الثلاثة التي تتمخض عن اعتماد تقنية التوقيع الإلكتروني، ومن ثم لا بد من بيان المسؤولية التي تنشأ على كل طرف عند إخلاله بالالتزامات المفروضة عليه، عليه سنقوم بالتطرق إلى هذه الأطراف الثلاثة وماهي طبيعة المسؤولية التي يمكن أن تطالهم وعلى وجه الإجمال وكما يلي: –

الطرف الأول: مقدم خدمة التصديق (الموثق):

وهذه الجهة بحسب المادة ٧ /١ من القانون النموذجي للتوقيع الإلكتروني قد تكون شخصاً طبيعياً أو معنوياً عاماً أو خاصاً تعيّنه الدولة ليحدّد التوقيعات الإلكترونية التي تتوفر فيها الشروط المنصوص عليها في المادة السادسة من ذات القانون

وقد أوجبت الفقرة ٢ من المادة السابعة التزام جهة التصديق بالمعايير العالمية المعتمدة في المؤسسات التي تنهض هكذا أعمال، كما استبعدت أن يؤدي تطبيق الفقرة ٣ من المادة السابقة إلى حصول أي تعارض بين الأحكام المنصوص عليها في قانون التوقيع الإلكتروني وبين ما تفرضه قواعد القانون الدولي الخاص من قواعد للإحالة والإسناد عند التنازع بين القوانين لحكم مسألة مشوبة بعنصر أجنبي وذلك بتقديم قواعد القانون الدولي الخاص. أمّا المادة التاسعة من نفس القانون فقد رتبت مجموعة التزامات على مقدم خدمات التصديق من خلال تحديدها لسلوك مقدم خدمات التصديق في الآتي:

١) أن يتصرف وفقاً للتأكيدات التي يقدمها بخصوص سياساته وممارساته.

٢) أن يمارس عناية معقولة لضمان دقة واكتمال كل ما يقدمه من تأكيدات جوهرية ذات صلة بالشهادة طيلة دورة سريانها أو مدرجة في الشهادة

٣) أن يوفر وسائل يكون الوصول إليها متيسراً بقدر معقول وتمكن الطرف المعول أو المرسل إليه من التأكد من الشهادة، منها بيان هوية مقدّم الخدمات، سيطرة مقدّم الخدمات على البيانات التي تتعلق بإنشاء التوقيع، إنّ البيانات كانت صحيحة في الوقت الذي صدرت فيه.

٤) أن يوفر وسائل يكون الوصول إليها متيسراً بقدر معقول تمكن من التأكد من الشهادة عند الاقتضاء منها الطريقة المستخدمة في تعيين هوية الموقّع، إنّ البيانات المتعلقة بإنشاء التوقيع صحيحة ولم تتعرض لما يثير الشبهة، وجود أي تقييد على نطاق مسؤولية مقدّم خدمات التصديق، ما إذا كانت هنالك وسيلة إلغاء للتوقيع آنية.

٥) أن يستخدم في أداء خدماته نظماً وإجراءات وموارد بشرية جديرة بالثقة.

ومن ثم فإن أي إخلال بأي من تلك الالتزامات التي فرضتها المادة السابقة التاسعة بفقراتها المختلفة، تترتب عليه المسؤولية القانونية لمقدم خدمات التصديق. هذه المسؤولية بالطبع هي تعويض الأضرار الناشئة عن إخلاله بواجباته القانونية، إن كان بالخطأ العقدي أو بالخطأ التقصيري، وعليه أن يثبت في الشهادة حدود هذه المسؤولية وفقاً لقانونه الوطني، على أن يؤخذ في الاعتبار النفقات اللازمة لإصدار الشهادات وطبيعة المعلومات التي تضمّنها ومدى مساهمة خطأ المضرور في إحداث الضرر

الطرف الثاني: الموقع (مستخدم التوقيع الإلكتروني):

حدّدت المادة الثامنة من القانون النموذجي للتوقيع الإلكتروني، الالتزامات التي تقع على عاتق الموقع أو مستخدم التوقيع الإلكتروني وهي:

١) أن يمارس العناية المعقولة لاجتناب استخدام بيانات إنشاء توقيعه استخداماً غير مأذون به

٢) أن يبادر دون تأخر إلى إشعار أي شخص يمكن للموقّع أن يتوقع منه أن يعول على التوقيع

الإلكتروني أو أن يقدّم خدمات تأييداً للتوقيع الإلكتروني وذلك في حالة: معرفة الموقّع بأنّ بيانات إنشاء التوقيع تعرّضت لما يثير الشبهة. كون الظروف المعروفة لدى الموقّع تؤدي إلى احتمال كبير بأنّ بيانات إنشاء التوقيع ربما تكون قد تعرّضت لما يثير الشبهة.

٣) على الموقّع أن يقدّم البيانات الدقيقة والكاملة اللازمة لإصدار شهادة التصديق وأن يبذل العناية المعقولة لضمان سلامة هذه البيانات طوال مدة صلاحية الشهادة.

وبذلك فإنّ أي إخلال يقوم به مستخدم التوقيع الإلكتروني وفق الالتزامات المنصوص عليها في المادة الثامنة، يرتب مسؤولية مدنية عليه تتمثل في الالتزام بالتعويض عن الأضرار التي يمكن أن تطال المتعاملين معه.

الطرف الثالث: المرسل إليه:

على المرسل إليه الذي يتلقى رسالة بيانات موقّعة على شبكة الإنترنت أن يتخذ الاحتياطات المعقولة قبل أن يمنح الثقة في مرسلها ويتعامل معه، ولذلك فقد نصّت المادة ١١ من قانون النموذجي للتوقيع الإلكتروني على تحميل المرسل إليه التبعات القانونية في حالة تخلفه عن: اتخاذ خطوات معقولة للتحقق من موثوقية التوقيع الإلكتروني. اتخاذ خطوات معقولة إذا كان التوقيع الإلكتروني مؤيداً بشهادة لأجل: ١. التحقق من صلاحية الشهادة أو وقفها أو إلغائها، ٢. مراعاة وجود أي تقييد بخصوص الشهادة. ويؤخذ في الاعتبار عند تقدير درجة العناية المعقولة المطلوبة من المرسل إليه، طبيعة الصفقة وقيمتها والعلاقات السابقة بين الأطراف إن وجدت وما يقضي به العرف والعادات التجارية. فإذا لم يبذل المرسل إليه هذا القدر من العناية المعقولة، فعليه أن يتحمّل تبعة عدم تحرزه.