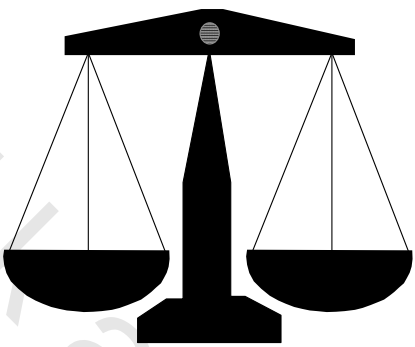

الفصل الثالث

التوقيع الإلكتروني

obeikandl.com

obeikandl.com

التوقيع الإلكتروني

س٤١: ما هو تعريف التوقيع الإلكتروني؟

ج : ورد تعريف التوقيع الإلكتروني في الفقرة (ج) من المادة (١) من قانون التوقيع الإلكتروني في مصر رقم ١٥ لسنة ٢٠٠٤م والصادر في غرة ربيع الأول ١٤٢٥هـ الموافق ١١ أبريل سنة ٢٠٠٤م بأنه "ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره" .

س٤٢: ما هي حجية التوقيع الإلكتروني؟

ج : حسب الفقرة (جـ) من المادة الأولى من قانون التوقيع الإلكتروني فإنه يجعل للمحرر الحامل له قيمة قانونية في الإثبات .

س٤٣: هل يشترط أن يكون التوقيع الإلكتروني الرقمي بالمعنى المتعارف عليه؟

ج : كما حددت الفقرة (ج) من المادة (١) من قانون التوقيع الإلكتروني فإنه لا يشترط أن يكون التوقيع بالطريقة المتعارف عليها ، ولكن يتم بأي وسيلة تُعيِّن صاحبها تعييناً يوجب الالتزام بما تعاقد عليه .

س٤٤: هل للتوقيعات الإلكترونية الرقمية أشكال؟

ج : نعم للتوقيعات الإلكترونية أو الرقمية أشكال متعددة؛ فمنها البسيط ومنها المعقد ومنها الإجرائي ومنها الحيوي .

س٤٥: ما هي الأشكال المختلفة للتوقيع الإلكتروني تفصيلاً؟

ج : التوقيعات الإلكترونية أو الرقمية تتخذ أشكالاً منها :

١ـ التوقيع الإجرائي :

يسمى هذا التوقيع بالتوقيع المكوّد أو المشفّر، وهو عدة خطوات منطقية متتالية يمكن من خلالها التعريف بالشخص، ويحكمها مفتاحان أحدهما يعرف بالمفتاح الشخصي أو السري **Personal Identification Number (PIN)** أو الـ **Secrete Key** ويمكن الوصول إليه من خلال مفتاح عام **Public Key Infrastructure (PKI)** ومن أمثلتها التوقيعات المستخدمة في بطاقات الائتمان **Credit Cards** والتي تستخدم في الصرف الآلي من البنوك أو الدفع خلال منافذ البيع من خلال قارئات **Readers**

٢ـ التوقيعات البيومترية Biometric Signatures :

وهى تعرف بالتوقيعات القياسية وهى خاصية من خواص الإنسان مثل :

١ـ قرنية العين	IRIS
٢ـ بصمة الإصبع	Finger Print
٣ـ بصمة الصوت	Voice Print
٤ـ بصمة الوجه	Face Print
٥ـ بصمة الدم	Blood Print

٣ـ التوقيعات البيولوجية Biological Signature

وهى خاصة بالشخص والتي توقع بخط اليد ويتم نقلها بإحدى وسائل النقل إلى جهاز الكمبيوتر لتسجل رقمياً باستخدام الوسائل الغالية :

١ـ الفاكس (الناسوخ)	Facsimile
٢ـ الماسح الضوئي	Scanner
٣ـ الإدخال بالكاميرا الرقمية بقلم رقمي	Digilal Pen
٤ـ الإدخال على سطح حساس	Sensitive Surface

وهنا نتطرق لشرح نوعين من التوقيعات وهما : التوقيع ببصمة الدم، والتوقيع بالقلم الرقمي .

ـ التوقيع ببصمة الدم حيث يتم تعريض اليد للجهاز القارئ لكلمة للسر Password فيفتح الجهاز لهذا الشخص ولا يفتح لغيره؛ لأن للدم بصمة خاصة بكل شخص.

ـ القلم الرقمي هو قلم يكتب به على ورق عادى في وجود كاميرا، فما يُكتب يسجل على الشاشة في الحال بكل تفاصيله، فإن كان توقيعاً سجل توقيعاً كأنه بخط اليد وذات لون مداد القلم، والقلم هنا مزود برأس يمكن من إدخال صوت وصورة للشخص القائم بالكتابة.

س٤٦: هل تعد كلمات السر توقيعات؟

ج: نعم تُعد كلمات السر توقيعات رقمية إذ هي دالة على الشخص الذي يحتفظ بها فقط دون حالة القرصنة أو حالة الاختراق من الغرباء أو الإفشاء من الأشخاص المؤتمنين عليها العاملين في الشركات والمؤسسات وغيرها.

س٤٧: من هو المُوقِّع الرقمي؟

ج: الموقع الرقمي Signer هو الشخص الطبيعي أو الاعتباري الذي يتعامل بنفسه أو عن طريق غيره باستخدام التوقيع الإلكتروني من خلال مصدر توثيق.

س٤٨: هل تُعد بصمة الدم توقيعًا إلكترونيًّا؟

ج: نعم تصلح بصمة الدم التي سبق الحديث عنها كتوقيع إلكتروني لأنها خاصة بشخص واحد لا غيره وتميزه.

س٤٩: هل هناك تقسيم آخر للتوقيعات الرقمية؟

ج: يمكن تقسيم التوقيعات الرقمية إلى:

١ـ التوقيع الممسوح:

هو توقيع الشخص بيده والذي يمسح بطريقة أو بأخرى ليدخل إلى الحاسب الآلي.

٢ـ التوقيع الحيوي :

هو أحد خواص الإنسان الطبيعية كما سبق الحديث عنها .

٣ـ التوقيع المكود :

هو عدة إجراءات وهو رموز أو حروف أو أرقام .

كما يمكن تقسيم التوقيعات الرقمية إلى:

١ـ التوقيعات الرقمية الارتباطية :

هي التي لها ارتباط بشخص الإنسان .

٢ـ التوقيعات الرقمية الحرة :

هي التي ليس لها ارتباط بشخص الإنسان .

س٥٠: هل تعد الخواص الطبيعية للإنسان وسيلة آمنة تستخدم كتوقيعات رقمية؟

ج : في الغالب فإن استخدام إحدى خواص الإنسان يكون آمنًا عندما تكون هناك برامج على درجة عالية من الثقة والأمن، لكن يمكن استغلالها أو تجريبها من قبل القراصنة وتكون مفتاحاً للسر الذي يمكن به التجسس على خصوصية الشخص أو صرف أمواله أو التشهير به أو ابتزازه .

س٥١: ما الفرق بين التوقيع الإلكتروني والتوقيع الرقمي؟

ج : لا يوجد في الغالب تمييز بين النوعين؛ فكلاهما ليس على الورق لكن يطلق على التوقيع القابل للرؤية أو الظهور **Visual Signature** التوقيع الإلكتروني، بينما التوقيع الرقمي يكون مخفياً كشفرة فهو عبارة عن أرقام أو حروف أو رموز .

س٥٢: ما هي محاذير التوقيع الإلكتروني؟

ج : يحيط بالتوقيع الإلكتروني أو الرقمي محاذير في التعامل إذ إنه عصب التجارة الإلكترونية

obeikandl.com

ولذلك لابد أن يحاط بالموثوقية حتى لا تهتز الثقة فيه وحتى لا يستغل في عمليات النصب ومن هذه المحاذير :

١ـ احتراز المُوَقّع أن لا يُستغل توقيعه أو يُستخدم بطرق غير مشروعة **Abuse Methods** .

٢ـ إخطار الشخص الذي علم باستغلال توقيعه الجهة أو الشركة التي يتعامل معها .

٣ـ عند طلب شهادة من المُوَقّع **Signer** تؤيد توقيعه فعليه أن يقدم ما يدل على تأكيد البيانات التي تدرج في الشهادة .

٤ـ تحديث التوقيع الإلكتروني عبر منظومة حتى لا يتم التوصل إلى المفتاح الخاص به بتقادم التكنولوجيا مع الزمن .

س٥٣: ما هو القانون النموذجي الخاص بالتوقيع الإلكتروني؟

ج : هو القانون الذي يعرف بقانون اليونسترال أو الأونسترال **UNCITRAL** وهو اختصار للعبارة **United Nations Commission on International Trade Law** وهو الذي وضع بمعرفة لجنة مختصة بالأمم المتحدة .

س٥٤: اذكر بعض الشركات الخاصة بالتصديق لاستخراج الشهادات الموثقة في الولايات المتحدة؟

ج : من الشركات المستقلة التي تستخدم في توثيق التوقيعات الإلكترونية أو الرقمية :

١ـ **Digital Signature Trust** .

٢ـ **Very Sign** .

س٥٥: ماذا يسمى الموثّق في نظام التوثيق الرقمي؟

ج : يسمى الشخص الموثق أو الذي يقوم بالتوثيق **Notary** .

س٥٦: هل يتم الاعتماد فقط على التوقيع الإلكتروني الرقمي دون الأصول أو المراجع الورقية؟

ج : من الخطورة بمكان أن يتم الاعتماد كلية على الصور الرقمية والتي تُعد وهمية **images** والتي لابد وأن تكون لها أصول ورقية، حتى إن عملية التعامل بالتجارة الإلكترونية تتم على أساس إرسال فاكس ثم الرد بفاكس أو عبر البريد الإلكتروني للتأكيد على التعامل الرقمي.

س٥٧: ما أهمية مقدمي خدمة التوثيق للمستندات الرقمية؟

ج : هم يضفون الثقة والشرعية في التعامل بالمستندات الرقمية والتوقيعات الرقمية والتجارة الإلكترونية والوثائق الحكومية الرقمية، ويقومون بحماية المعلومات الشخصية للمشتركين في الخدمة.

س٥٨: ما هي شروط الثقة في الشهادة الموثقة؟

ج : ١ـ يجب أن تشمل الشهادة على البيانات محدد بها شخصية مقدمها والدولة التي أنشأتها.

٢ـ اسم المُوَقّع الفعلي أو حتى المستعار لكي يمكن التحقق منه.

٣ـ أن تكون للمُوَقّع **Signer** ميزة خاصة بالشهادة المعطاة له.

٤ـ المفتاح العام الذي يكون موصّلاً للتوقيع الخاص والذي يكون تحت رقابة الموقع.

٥ـ تحديد قيمة الصفقات التي تستخدم الشهادة من أجلها.

٦ـ لابد من تحديد مدة صلاحية الشهادة من حيث بدايتها ونهايتها.

٧ـ تحديد المجال الذي تستخدم فيه الشهادة.

٨ـ الرقم الخاص بالشهادة.

س٥٩: ما هي صلاحية الأسطوانات والأقراص حتى يتم الاعتماد عليها في الإثبات؟

ج : فيما يبدو أن هناك مشكلة حادثة وستستمر في الكيفية والمدة التي تحفظ بها الأسطوانات

والأقراص كي تصلح في الإثبات، والمفترض أن هناك بيانات أساسية ويتم استحداث أخرى، فماذا سيكون الوضع لو حدث تلف أو إتلاف في هذه المعدات دون وجود أصول ورقية محفوظة؟

س٦٠: هل الشهادات الموثقة قابلة للتزوير؟

ج: نعم حتى الشهادات الموثقة قابلة للتزوير وخاصة بعد وجودها على الورق، فتبدأ أذهان المزورين تتجه إلى محاكاتها، وساعتها نتمنى لو عدنا إلى الطرق البدائية في التوثيق واستعمال قوالب الأختام والتوقيع بخط اليد.

س٦١: هل من الضروري تلازم الدليل الورقي والدليل الرقمي؟

ج: تقوم بعض الجهات بإعداد الدليل الورقي بعد تحويله إلى دليل رقمي عن طريق الميكروفيلم، ويقال إنه ليس بلازم أن يكون هناك تلازم للدليل الورقي والدليل الرقمي، وفى حالة المنازعات يتم اللجوء للميكروفيلم للإثبات.

س٦٢: ما هي حجية الصورة الرقمية؟

ج: آلات الطبع المتصلة بالأجهزة الرقمية مثل الفاكس أو الناسوخ والطابعات الكمبيوترية لا تصدر أصولاً بل ينتج عنها صور مستنسخة وتكرار لأصل، ويرى البعض أنها مبدأ ثبوت بالكتابة، ويرى البعض الآخر مبدأ عدم ثبوت بالكتابة.

س٦٣: ما هي المستندات الرقمية وحجيتها؟

ج: المستندات الرقمية **Digital Documents** هي مستندات جديدة تُعرف بالـ **New Documents** تحملها دعامات خيالية وليست ورقية، وهى قابلة للنسخ للاحتفاظ بها للإثبات، وقابلة للتغيير والتبديل دون ترك آثار دالة في الغالب، وقد تُجرى عليها عمليات التزوير. ويصعب الإثبات في جرائم هذه المستندات إلا بمساعدة أدلة وقرائن أخرى.

هذا وقد أعطت القوانين الدولية الحديثة نفس الحجية للمستندات الرقمية كما لو كانت مستندات ورقية فالنتائج المترتبة عليها واحدة.

حيث ورد بالمادة (١٦) من قانون التوقيع الإلكتروني المصري أن النسخ الإلكترونية للمحرر حجة على الكافة بالقدر الذي تكون فيه مطابقة لأصل المحرر.

وهذه المستندات الجديدة تعرف بالرسائل **Messages** وتكون في ملفات أو مجلدات، وقد تكون على هيئة رسالة بيانات **Data Message** ويتم تذييلها بتوقيع رقمي أو إلكتروني.

س٦٤: لماذا في الغالب يصعب الإثبات في جرائم تزوير المستندات الرقمية؟

ج: لأنه لا يوجد طمس أو محو جزئي أو تراكب لكتابة فوق أخرى أو تآكل لألياف الورقة أو مواضع ثنى وتطبيق، كما لا يتضح الكشط أو التعديل أو التحشير كما في المستندات التقليدية الورقية.

س٦٥: ما هي شروط تمتع الوثائق الرقمية بالحماية القانونية؟

ج: حددت المادة (١٨) من قانون التوقيع الإلكتروني المصري الشروط التي تجعل التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية تتمتع بالحجية، وحددتها في ثلاثة شروط هي:

١ـ ارتباط التوقيع الإلكتروني بالمُوَقِّع (**Signer**) وحده دون غيره.

٢ـ سيطرة المُوَقِّع (**Signer**) وحده دون غيره على الوسيط الإلكتروني.

٣ـ إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

هذا وفى رأينا لا يشترط وجود توقيع على المحرر، ومن الصعوبة بمكان سيطرة المُوَقّع على الوسيط الإلكتروني، كما أنه ليس من السهل كشف التزوير في بيانات المحرر.

س٦٦: كيف يمكن إخفاء الملفات المشتملة على المستندات بالحاسب الآلي؟

ج: حتى يمكن المحافظة على الخصوصية على أجهزة الحاسبات الآلية أو خلال الاتصال بالإنترنت فإن عدة طرق تستخدم لإخفاء الملفات الحاوية للمستندات وذلك لإبعادها عن المتلصصين والقراصنة؛ لأن أحدهما لو قام باستعراض محتويات القرص الصلب **Hard Disk** فستظهر له كافة الملفات.

ولإخفاء الملفات يتم اتباع الآتي:

١ـ الذهاب إلى الملف الحاوي للمستندات التي يراد إخفاؤها.

٢ـ النقر على جانب الفأرة الأيمن فوق الملف.

٣ـ اختيار **Properties** من الشاشة التي ظهرت.

٤ـ النقر داخل مربع تنشيط الخيار **Hidden** وهو الخاص بإخفاء الملف.

٥ـ النقر فوق **O.K.**

٦ـ يلاحظ اختفاء الملف.

س٦٧: كيف يتم إظهار الملفات المخبأة؟

ج: من المهم في المحكمة الرقمية هو التعرف على كيفية إظهار الملفات المخبأة إذ إنها قد تكون هي التي بها أسرار الجريمة.

يمكن إظهار الملفات المخبأة كالآتي:

١ـ فتح نافذة عرض الملفات كنافذة **My Computer**.

٢ـ من القائمة **Tools** يتم اختيار الـ **Folder Options**.

٣ـ من النافذة التي ظهرت نختار **View** فتظهر مجموعة خيارات.

Obeikandi.com

٤ـ النقر داخل مربع تنشيط الخيار **Show Hidden Files and Folders** .

٥ـ بذلك يتم إظهار الملفات المخبأة.

س٦٨: ما خطورة برامج الاختراق على المستندات؟

ج : من المخترقين قراصنة خطرين يقومون بإتلاف أو تدمير المستندات تماماً.

س٦٩: ما هي الكيفية التي يتم بها حماية المستندات ضد الاختراق والعبث والتجسس؟

ج : تنقسم هذه الوسائل إلى أمن شخصي فلابد للشخص أن يحمى خصوصياته ويكون لديه المعرفة الكافية لاستعمال المواقع وغلقها وتجنب التجريب لمواقع لا يعرفها ووسائل تختص بها شركات الأمن والشركات المنتجة وأخرى تقوم بها الحكومات.

س٧٠: كيف يتم إتلاف البريد الإلكتروني؟

ج : عن طريق الدفع بكمّ هائل من الرسائل إلى البريد الإلكتروني وهو المخصص له مساحة متواضعة فتشل حركته ويتوقف عن العمل.

obeikandl.com