الفصل الخامس

البصمة الالكترونية

obeikandl.com

obeikandl.com

رغم أن التشفير يمنع المتلصّصين من الاطلاع على محتويات الرسالة، إلا أنه لا يمنع المخرّبين من العبث بها؛ أي أن التشفير لا يضمن سلامة الرسالة ومن هنا ظهرت الحاجة إلى البصمة الالكترونية للرسالة (**message digest**)، وهي بصمة رقمية يتم اشتقاقها وفقًا لخوارزميات معيّنة تُدعى دوالّ أو اقتران التمويه إذ تطبّق هذه الخوارزميات حسابات رياضية على الرسالة لتوليد بصمة (سلسلة صغيرة) تمثّل ملفًا كاملاً أو رسالة (سلسلة كبيرة). وتُدعى البيانات الناتجة البصمة الالكترونية للرسالة. وتتكوّن البصمة الالكترونية للرسالة من بيانات لها طول ثابت (يتراوح عادة بين ١٢٨ و١٦٠ بت) تؤخَذ من الرسالة المحوّلة ذات الطول المتغير. وتستطيع هذه البصمة تمييز الرسالة الأصلية والتعرُّف عليها بدقة، حتى إن أي تغيير في الرسالة ـ ولو كان في بت واحد ـ سيفضي إلى بصمة مختلفة تمامًا. ومن غير الممكن اشتقاق البصمة الالكترونية ذاتها من رسالتين مختلفتين. وتتميز البصمات الالكترونية عن بعضها بحسب المفاتيح الخاصة (**private key**) التي أنشأتها، ولا يمكن فك شفرتها إلا باستخدام المفتاح العام (**public key**) العائد إليها. ولهذا يُطلَق على اقتران التمويه المستخدَم في إنشاء البصمة الالكترونية اسم آخر هو اقتران التمويه الأحادي الاتجاه (**one-way hash function**). ومن الجدير بالذكر، أن استخدام خوارزمية البصمة الالكترونية أسرع من القيام بعملية التشفير اللامتماثل (**asymmetric encryption**) (تشفير نص باستخدام المفتاح العام)، ولهذا تُستخدَم خوارزمية البصمة الالكترونية كثيراً في إنشاء تواقيع رقمية.

١. خوارزميات البصمة الالكترونية للرسالة:

طوّر رونالد رايفست ـ خوارزميات **MD2** و**MD4** و**MD5** الخاصة بالبصمة الالكترونية للرسالة. وهذه الخوارزميات هي اقتران تمويه يُمكن تطبيقها على التواقيع الرقمية. وبدأ ظهور هذه الخوارزميات عام ١٩٨٩ بخوارزمية **MD2**، ثم تلتها خوارزمية **MD4** عام ١٩٩٠، ثم خوارزمية **MD5** عام ١٩٩١. ويُولّد كل من هذه الخوارزميات بصمة إلكترونية للرسالة بطول ١٢٨ بت. ورغم وجود تشابه كبير بين **MD4** و**MD5**، إلا أن خوارزمية **MD2** تختلف عنهما. ومن ناحية أخرى، فإن خوارزمية **MD2** هي أبطأ هذه الخوارزميات، على حين أن خوارزمية **MD4** هي أسرعها[1].

(1) موقع موسوعة جوريسبيديا القانوني موضوع خوارزميات البصمة الالكترونية.

خوارزمية MD4 مُضافًا إليها بعض خصائص الأمان الأكثر إحكامًا. ويمكن تطبيق خوارزمية MD2 بوساطة أجهزة كمبيوتر ذات ٨ بت (٨ـbit computers)، بينما يلزم أجهزة كمبيوتر ذات ٣٢ بت لتطبيق خوارزمي MD4 وMD5.

٢. كيف تعمل أجهزة البصمة الالكترونية؟

الأجهزة الالكترونية التي تتعرف على بصمة الأصابع كانت جزءًا أساسيًا في جميع قصص الجاسوسية في العقود الماضية، ولكن استخدامها كان قليلاً في الواقع، وفي السنوات الأخيرة انتشرت أجهزة البصمات الالكترونية في كل مكان، وخاصة في أقسام الشرطة والمنشآت المهمة.

٣. أساسيات بصمات الأصابع:

من المعروف أن كل شخص خلقة الله عزّ وجلّ له طبيعة خاصة به، توجد في أطراف أصابعه، ولا تتشابه بصمات إنسان وآخر أبدًا، حتى وإن كانا توأمين متطابقين، وهذا من المعجزات الإلهية في خلق الإنسان، حتى وإن بدت لأول وهلة أن بصمات شخصين متطابقة فإن الفحص البصري الدقيق للخبراء يمكنه تمييز الفرق بسهولة وكذلك برامج الحاسب يمكنها التعرف على هذه الفروق بين البصمات، وهذا هو دور أجهزة التعرف على البصمات، فهي تصور بصمة الإصبع عن طريق الماسح الضوئي، ثم تخزنها في ملف على الجهاز وعند الطلب يتم أخذ بصمة لمستخدم ومطابقتها بالبصمة المخزنة فإن تطابقا يسمح له بالمرور.

٤. وظائف أجهزة تصوير البصمة:

أجهزة تصوير البصمات لها وظيفتان[٢]، **الأولى**: الحصول على صورة رقمية لبصمة الأصابع لشخص معين يسمح له بالمرور، والوظيفة **الثانية**: هي أخذ صورة بصمة الأصابع لشخص يطلب السماح له بالمرور، وبعد الحصول عليها فإنه يطابقها بالصورة الأصلية المخزنة عنده.

هناك طريقتان للحصول على الصورة الرقمية لبصمات الأصابع، الطريقة **الأولى**: هي المسح الضوئي، **والثانية**: هي المسح الكهربي، وكلاهما يؤدي إلى نفس النتيجة ولكن بطرق مختلفة.

(2) د. محمد رضوان هلال بحوث وأراء جديدة في التزييف والتزوير الناشر عالم الكتب ٢٠٠٥.

المسح الضوئي:

يحتوي الماسح الضوئي على جهاز حساس **charge coupled device (CCD)** مثل الموجود في الكاميرات الرقمية، وهو عبارة عن مصفوفة من خلايا حساسة للضوء تسمى **photosite** [٣] وتنتج إشارة كهربية عند تعرضها للضوء، وكل خلية تنتج مربعًا متناهيًا في الصغر وهذا المربع إما مضيء أو مظلم طبقًا لنتيجة تعرضه للضوء، فالخلايا التي لم تتعرض للضوء تكون مظلمة وتلك التي تعرضت للضوء تكون مضيئة، وتتكون الصورة من المظلم والمضيء ثم تتحول إلى دورة رقمية ليتم حفظها الكترونيًا، وتبدأ عملية المسح الضوئي حينما يضع الشخص يده على لوح زجاجي ثم يلتقط الجهاز الصورة، ثم تعالج هذه الصورة لتنقي من الشوائب، ثم تتم مقارنتها بالصورة الأصلية المخزنة.

المسح الكهربي:

بدلاً من الحصول على صورة بصمات الأصابع باستخدام الضوء فإن المسح الكهربي ينتج نفس الصورة ولكن عن طريق المكثفات الكهربية والتيار الكهربي. فهو عبارة عن دائرة كهربية حول مكبر للتيار، ومكبر التيار مكون من عدة ترانزيستورات ومقاومات ومكثفات، ومكبر التيار يغير قيمة الجهد الكهربي لمولد جهد كهربي متصل بدائرة مغلقة وبدورها متصلة بمكبر آخر يحتوي على لوحين من الموصلات يكوّنان مكثفًا كهربيًا يمكنه تخزين الشحنة الكهربية، وعند أخذ البصمة فإن الشخص يضع يده على لوح المكثف الثالث ونتيجة لخطوط البصمة على سطح الجلد فإن الشحنة الناتجة يتغير طبقًا لشكل البصمة، والجهاز الحساس يلتقط قراءات جهد الشحنة الكهربية ويحدد من قيمتها شكل بصمات الأصابع وفي النهاية تتكون الصورة مثل تلك التي تكونت في المسح الضوئي.

التساؤل الذي يطرح نفسه هنا، لماذا الطريقة الكهربية لأخذ البصمة بالرغم من تعقيداتها الشديدة، وهناك طريقة المسح الضوئي السهلة؟ الإجابة بسيطة: يمكن خداع الماسح الضوئي بوضع ورقة عليها صورة البصمة بينما الجهاز الكهربي لابد من وجود يد حقيقية تضغط على الجهاز، بالإضافة إلى صغر حجمه.

(3) د. شريف محمد غانم " محفظة النقود الالكترونية " المرجع السابق.

٥. استخدام البصمة الالكترونية يؤدي للإصابة بالسرطان:

حذّر أحد الأطباء الاستشاريين والمتخصصين في الأمراض الجلدية من خطورة استخدام بعض الوزارات والإدارات الحكومية والمنشآت الخاصة لأجهزة البصمة الالكترونية لأخذ بصمة اليد بالكامل لإثبات حضور وانصراف الموظفين في دوامهم الرسمي وأكد أحد الاستشاريين تسبب أجهزة البصمة في الإصابة بالسرطان بالإضافة إلى الأمراض الجلدية مشيراً أن هذا الإجراء يؤدي إلى نقل الجراثيم مثل الدمامل والفطريات من الموظفين المصابين بهذه الأمراض إلى الموظفين الأصحاء.

وثبت طبيًا أن مثل هذه الأجهزة الالكترونية تنقل حساسية تلامسيه إضافة إلى فطريات اليد والدمامل بل قد يتعدى ذلك إلى نقل أمراض خطيرة مثل الجراثيم البكتيرية إذا كانت في الأصبع مثلاً، ودعا إلى أهمية أخذ الحذر والحيطة عند استخدام مثل هذه الأجهزة لخطورتها على الصحة العامة[٤].

يشار إلى أن عدد من الوزارات والأجهزة الحكومية والمنشآت الخاصة قد بدأت منذ سنوات قليلة باستخدام نظام البصمة الالكترونية في دوام موظفيها حضوراً وانصرافًا وهذه البصمة هي عبارة عن شريحة زجاجية توضع راحة الكف عليها بالكامل أو بالإبهام أو السبابة ثم تمرر المعلومات للجهاز الكترونيًا لإثبات الشخصية في الحضور والانصراف، ويقول أحد الأشخاص أنه اتصل هاتفيًا بمدير عام الهيئة السعودية للمواصفات والمقاييس نبيل ملا وسأله عن أضرار هذه الأجهزة وقال له بالحرف الواحد هذه الأجهزة غير مصرح بها من قبل الهيئة ولم تعط الهيئة أي تصريح لها كما أشار عدد من الأطباء والمختصين أن هذه الأجهزة تصور أشعة تسبب الأمراض السرطانية للجلد والدم وتحدث طفرات للحمض النووي (DNA) الذي ينتج عنه عيوب بالموالي مثل مرض داون ومرض تيرنر كما أن هذه الأجهزة تطلق أشعة (X-RAY) وبالتالي تتعرض له اليد دون واق ما يركز عملية الإصابة. وألمح الأطباء إلى أن ضرر هذه الأجهزة وسوف يحدث في المدى البعيد أو القريب لأن تتعرض له عشر مرات في الأسبوع أي نحو ٤٠ مرة في الشهر.

هذا وكانت بعض الأجهزة الحكومية قد قامت بإلغاء نظام البصمة الالكترونية بعد مدة قليلة من تطبيقها في دوام حضور وانصراف موظفيها بعد أن ثبت لديها خطورة هذه الأجهزة

(4) أحمد الأحمدي مكة المكرمة مقاله "استخدام البصمة الالكترونية يؤدي إلي الإصابة بالسرطان" ٢٠٠٨.

على الصحة العامة ولاختزال بعض الأجهزة تواصل أعمالها في تطبيق هذا النظام ويعتزم عدد من الموظفين رفع قضية على هذه الإدارات لدى ديوان المظالم للمطالبة بإلغاء هذا النظام من أجل الحفاظ على سلامة الجميع من الأخطار الجسيمة الناجمة عن استخدام هذه الأجهزة والتي من أبرزها مرض السرطان.

٦. الحماية الجنائية للمستند الالكتروني:

تتيح التكنولوجيا الحديثة القيام بالكثير من الأعمال التي كان يستحيل من قبل إنجازها: فلقد وفرت هذه التكنولوجيا في مجال الاتصالات الالكترونية إمكانية تحقق التواصل الإنساني وإنجاز المعاملات في سهولة ويسر، وأتاح استخدامها حُسن تقديم خدمات الرعاية الصحية وتنمية الملكية الفكرية، وغيرها من مجالات. وتعد شبكات المعلومات ونظم التبادل الالكتروني للبيانات تطبيقًا للاستخدام التكنولوجي الحديث في مجال الاتصالات ونقل المعلومات وهي تختلف بذلك كثيراً عن غيرها من الوسائل التقليدية للاتصال والإعلام، وهذا الاختلاف يؤدي إلى أمرين: **الأول** هو تعدد أوجه استعمالات هذه الوسائل وأتساعها، **والثاني** هو الحاجة إلى تنظيم قانوني يضع الإطار لهذه الاستعمالات، غير أن هذه التكنولوجيا قد يساء استعمالها وأن يهدد استخدامها السلامة العامة والمصلحة الوطنية، فإذا كانت وسائل الاتصال الالكتروني الحديثة تتيح إنجاز المعاملات المالية بشكل سريع وموثوق به أيا كان مكان المتعاملين؛ فإن استعمال هذه الوسائل لا يخلو من مخاطر، فقد يستغل بعض المجرمين هذه الوسائل في ارتكاب جرائمهم بطريق الاحتيال أو المساس بخصوصية هؤلاء المتعاملين وسرية معاملاتهم. وإذا كان التقدم التقني قد حاول مكافحة الجرائم في مجال الاتصالات ولجأ إلى تشفيرها بما يحفظ سريتها، فإن هذه الإجراءات ـ مع ذلك ـ قد أفضت إلى استغلال الجناة لهذه الإجراءات في ارتكاب جرائمهم باستخدام وسائل اتصال يصعب اختراقها أو الوقوف على محتواها، وهو ما يعني أن التقدم التقني قد أمد المجرمين بوسائل بالغة القوة والفاعلية في ارتكاب جرائمهم.

٧. أهمية المستند الالكتروني:

ترجع أهمية المستند الالكتروني إلى أنه يتماثل مع المستند الورقي من حيث أوجه الاستعمال وأنه قد يماثله ـ في نظر الكثير من التشريعات ـ من حيث القوة القانونية المقررة له، غير أن المستند الالكتروني له الكثير من المزايا التي تكفل له انتشاراً واسعًا وتزايداً مستمراً في الاستخدام.

فمن ناحية فإن المستند الالكتروني يتصل بطائفة مهمة من النظم الإدارية والتجارية والمالية التي تمتد لتشمل الدولة والأفراد على حد سواء، فالمستند الالكتروني هو أحد الأدوات المهمة في تنفيذ فكرة "الحكومة الالكترونية"، التي تقدم خدماتها إلى الأفراد والهيئات العامة والخاصة، وللمستند الالكتروني صلة بنشاط الهيئات التي تعمل في مجال البنوك والتأمين والخدمات الطبية وغيرها، فهذه الهيئات تؤدي عملها بالاعتماد على هذا المستند من خلاله.

والمستند الالكتروني هو الوسيلة لتحقق التجارة الدولية أهدافها، فمن خلال هذا المستند وحده يمكن إنجاز المعاملات وإبرام التصرفات والصفقات التي تقضيها فكرة التجارة الالكترونية. ومن شأن كفالة حماية المستند الالكتروني أن يفضي إلى سهولة المعاملات التجارية وسرعة إنجازها وإلى توفير النفقات. وللمستند الالكتروني صلة وثيقة بالحق في السرية والخصوصية، وللمستند الالكتروني صلة بحماية حقوق المستهلك، فهذا المستند يتبلور فيه حقوق طرفي التعاقد، فهو المرجع للوقوف على ما أتفق عليه الطرفان وتحديد التزاماتهما القانونية، والحماية المقررة للمستند الالكتروني تضمن في الوقت ذاته حماية للمستهلك.

وقد أثرت الصلة بين المستند الالكتروني وبين المصالح سالفة الذكر، في أن النصوص التي تحمي هذه المصالح قد تتضمن بعض صور حماية المستند الالكتروني أو على الأقل تكمله الحماية المقررة له، ومن ذلك على سبيل المثال التشريعات التي تحمي، الحق في الخصوصية[٥]؛ حرية المعلومات والاتصالات الالكترونية؛ التجارة الالكترونية؛ تشريعات الكمبيوتر؛ تشريعات حماية البيانات؛ التشريعات المتعلقة بالحكومة الالكترونية.

ومن ناحية أخرى فإن حماية المستند الالكترونية تؤدي إلى تحقيق الاستقرار والأمان القانوني، فحماية المستند الالكتروني سواء من حيث الصلب والتوقيع، وصيانته من المساس بسريته وكشف محتواه يكفل للإفراد الطمأنينة واستقرار المعاملات، كما يؤدي إلى أن يصبح هذا المستند دليلاً في الإثبات يقف على قدم المساواة مع المستند الورقي، وهو ما يؤدي في النهاية إلى استقرار النظام القانوني وقله المنازعات.

٨. أثر الأخذ بفكرة المستند الالكتروني على القوانين السارية:

يؤدي الأخذ بفكرة المستند الالكتروني إلى إحداث تعديلات مهمة على القوانين السارية، ومن ذلك على سبيل المثال القانون المدني والتجاري اللذين يعتمدان في إتمام التصرفات على

(5) د. أسامة قايد "الحماية الجنائية للحياة الخاصة وبنوك المعلومات" ـ دار النهضة العربية ـ القاهرة ٢٠٠٧.

التوقيع الكتابي والمستندات الورقية. ويؤدي إقرار فكرة المستند الالكتروني تشريعيًا إلى وجوب تعديل هذه التشريعات. كما يؤدي الأمر بالتبعية إلى تعديل القوانين المتعلقة بالإثبات المدني والتجاري والجنائي، وإلى أن يقرر الشارع القوة القانونية التي يسبغها على المستند الالكتروني.

كما سوف يؤدي الأخذ بفكرة المستند الالكتروني إلى تعديل القوانين المالية والضريبية السارية والتي كانت لا تعتد بالأدلة المستمدة من مستندات الكترونية في الإثبات والتعامل، كما قد تدعو الحاجة كذلك إلى تعديل قوانين حماية المستهلك. وسوف يترتب على إقرار المستند الالكتروني التأثير على القوانين التي تنظم حفظ الأوراق الحكومية وإعدامها.

على أن الأثر المهم في تقديرنا للأحد بفكرة المستند الالكتروني هو وجوب إصدار تشريع مستقل ينظم أهم تطبيقات المستند الالكتروني في التعامل وهي السجلات والتوقيع الالكتروني ويضع الضمانات القانونية والفنية لهما ويحدد القوة القانونية التي يخلعها الشارع عليهما في الإثبات. وإختلاف خطة التشريعات في موضع النص على حماية المستند الالكتروني فتختلف خطة التشريعات المقارنة في موضع النص على الحماية الجنائية للمستند الالكتروني وتتوزع إلى ثلاثة اتجاهات:

الاتجاه الأول: يرى إصدار قانون يعاقب فيه على جرائم الكمبيوتر بصورها المختلفة ومن ضمنها الجرائم الماسة بالمستند الالكتروني في صورها المختلفة، وتقترن هذه الخطة في تجريم هذه الأفعال بإصدار تشريعات تنص على صورة معينة من المستند الالكتروني مثل "السجلات والتوقيع الالكتروني" ومن أمثلة التشريعات التي تبنت هذه الخطة تشريعات الولايات المتحدة الأمريكية.

والاتجاه الثاني: من التشريعات يذهب إلى إدخال تعديلات على النصوص التشريعية القائمة على نحو يؤدي إلى استيعابها الصور المستحدثة من الجرائم الالكترونية ومن بينها صور الاعتداء على المستند الالكتروني، ثم تفرد هذه الخطة التشريعية قوانين خاصة ببعض الموضوعات مثل الاتصالات والتوقيع الالكتروني والتي تتضمن نصوصًا تتصل بتجريم الاعتداء على المستند الالكتروني. ومن أمثلة التشريعات التي تبنت هذه الخطة الأخيرة القانون الألماني والفرنسي.

والاتجاه الثالث: هو الذي لم يفرد بعد تجريمًا خاصًا للجرائم الالكترونية، ومازال يكتفي بالنصوص التقليدية التي ينصص عليها في التشريعات المختلفة ومن أهمها قانون العقوبات، غير أنه يفرد الحماية الجنائية على بعض صور المستند الالكتروني ومن أمثلة هذا الاتجاه غالبية تشريعات الدول العربية.