Firmas Digitales

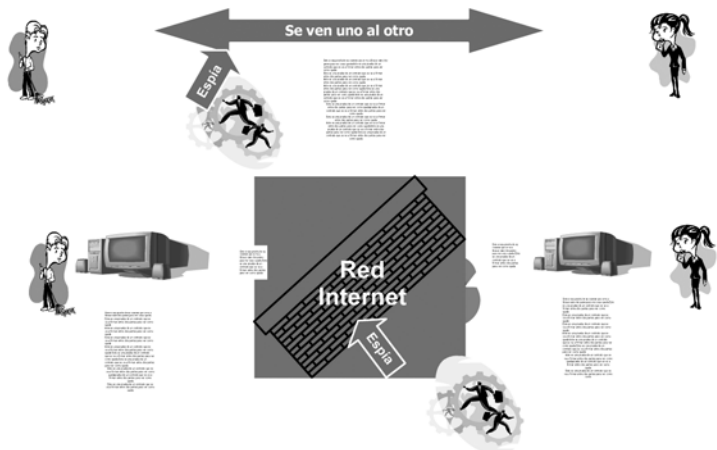
Ing. Esteban Di Tada *

Este artículo es la versión taquigráfica de la presentación que el Ing. Esteban Di Tada realizo el 7 de Mayo de 2002 en el salón de actos del Congreso de la Nación. Se efectuó dentro del acuerdo de cooperación tecnológica que la Facultad de Ingeniería de la Universidad de Palermo firmó con la Comisión de Modernización Parlamentaria de la HCDLN.

Es un gran honor poder participar de este seminario en el que se tratará un tema que, posiblemente, sea de actualidad durante mucho tiempo, como ha sucedido con la firma ológrafa, utilizada como medio de identificación.

Quiero mostrarles en esta imagen, la diferencia entre el mundo virtual de Internet y el mundo real en el que desarrollamos nuestras actividades.

Diferencia mundo real y virtual



En el mundo real estamos frente a frente con nuestro interlocutor y, por medio de un complejo sistema, podemos identificar a la otra persona por su imagen, sus gestos, su voz, en fin, por una serie de atributos que procesamos en nuestro cerebro. En el mundo virtual no vemos a nuestros interlocutores. Solamente nos comunicamos por medio de una consola que está frente a nuestros ojos. El objeto de este seminario es analizar de que manera es posible dotar a las transacciones virtuales de seguridades análogas a las que tienen las transacciones personales.

También veremos de forma resumida la historia de Internet. Quiero destacar que, si bien el tema de la firma digital no está obligatoriamente asociada con Internet, el desarrollo

* Decano de la Facultad de Ingeniería. Universidad de Palermo.

de las comunicaciones en la red ha forzado a mejorar constantemente los aspectos de su seguridad. Cada vez se realizan más transacciones críticas por Internet lo que obliga a sus actores a establecer métodos y normas que garanticen la seguridad de las mismas.

Vamos a hablar de seguridad, de lo que es la criptografía, de las claves simétricas y asimétricas, y finalmente de las firmas digitales.

Como ocurre en casi todos los textos, utilizaremos en los ejemplos los nombres "Roberto" y "Alicia". Si en el mundo real Roberto y Alicia quieren firmar un documento evitando que alguien los vea, simplemente se ubicarían en un recinto cerrado para que nadie tenga la posibilidad de observarlos. En todo caso, utilizarán alguna tecnología para descubrir si existen micrófonos o cámaras ocultos.

En el mundo virtual, en el de la red, Roberto envía el documento a través de Internet, y Alicia lo verá en otro lado. Ellos están completamente separados, uno podría estar en Buenos Aires y otro en Tokio. No se pueden ver porque están completamente distantes. Además, aquél que observe lo que hacen no va a estar en el mismo recinto que ninguno de ellos.

Puede estar en cualquier parte del universo observando esa red.

Entonces, los fenómenos normales que ocurren -de seguridad, de identificación, para garantizar que un documento no se cambie o que se niegue haberlo firmado cuando realmente se firmó- son completamente diferentes debido a que el contexto en que se realizan estas operaciones es totalmente distinto.

Cuando se habla de seguridad, dentro de la cual la firma digital juega un papel muy importante, en realidad está haciendo referencia a un término muy amplio que vamos a precisar con un mayor detenimiento.

Primero, hay un concepto de confidencialidad o privacidad. Segundo, hay un concepto de autenticación por medio del cual cada uno de los interlocutores verifica la identidad del otro. Las palabras "confidencialidad" o "privacidad" son bastante frecuentes en el lenguaje coloquial y consisten en que realmente nadie se entere de lo que estoy tramitando o gestionando al comunicarme con otra persona.

"Autenticación" es tener la certeza de que cuando me comunico con alguien ese alguien es el que dice ser y que la otra persona, cuando se comunica conmigo, esté segura de que yo sea yo. Cuando lo hacemos en el mundo real lo vemos a través de complejos mecanismos fisiológicos porque vemos y reconocemos la cara, la voz y una serie de cosas; a lo mejor, algunos reconocerán el áurea que puedan tener. Cuando lo hacemos por teléfono la cosa es más dificultosa. A veces reconocemos la voz pero en ocasiones ésta viene distorsionada por alguna razón y ni siquiera se la puede reconocer.

"Autorización" es saber que la gente que hace algo está autorizada para hacer eso que va a hacer. Cuando se compra una casa es necesario hacer una serie de trámites para que el comprador esté seguro de que estoy autorizado a vender esa casa, por ejemplo, que soy propietario, que la casa no está hipotecada y algunos otros hechos factibles.

"Integridad" es el hecho de que la información llegue tal cual se la mandó. Es decir, si mando una transacción de mi tarjeta de crédito por 30 pesos, que después no me aparezcan 3 mil pesos. O sea, que tenga la garantía de que la información no es alterada en el transcurso de la comunicación.

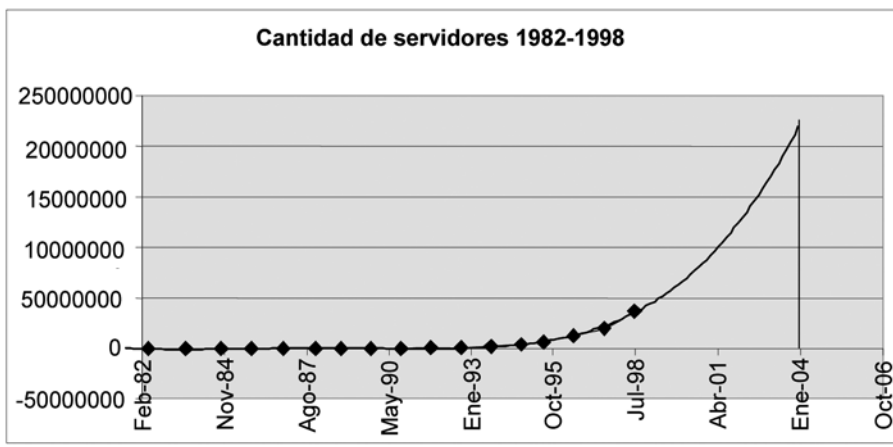
Finalmente el "no repudio" es el hecho de que no se pueda negar que se hizo una transacción. Por ejemplo, si se compra un libro en un librería virtual es necesario prevenir que se niegue haber realizado la operación. Es necesario poder garantizar la realización de una operación, así como el receptor de un cheque tiene la firma ológrafa del emisor, que garantiza el acuerdo del comprador.

Vamos a analizar brevemente cuál es la historia de Internet, que como dije ha sido lo que ha producido el desarrollo de los mecanismos de seguridad -entre los cuales la firma digital es muy importante- como consecuencia de su utilización cada vez más frecuente en transacciones de valor crítico.

Hace mucho tiempo la necesidad de la confidencialidad se basaba casi únicamente en operaciones del Estado, básicamente en la defensa Nacional, para que cuando se transmitiera una información a las fuerzas propias el enemigo no se enterara de su contenido. Al respecto hay películas notables, incluso una de las últimas, "Una mente brillante", se refiere a alguien que descubre un método para romper el cifrado de potenciales extranjeras.

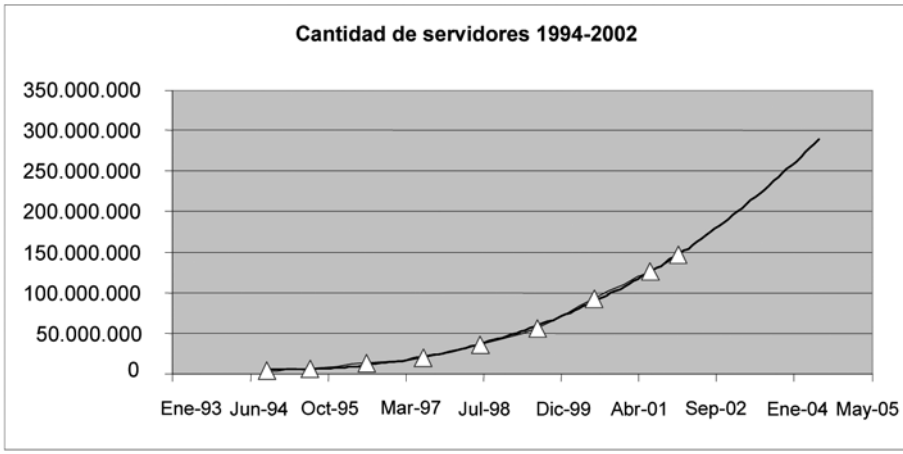
Ahora, el hecho de que en Internet haya gran cantidad de transacciones con valor económico ha hecho incrementar la necesidad de disponer de efectivos mecanismos de seguridad en la Red. Si vemos -y es interesante- cuántas son las computadoras que se encuentran conectadas a la red de Internet, cuántas son las que ofrecen servicios que están conectados -generalmente se las llama "servidores"- podemos apreciar que, evidentemente, la mayoría se encuentra en Europa, en los Estados Unidos, en Canadá y en el Asia de los "tigres" en desarrollo.

El 5 por ciento está en América latina, es decir que el potencial de crecimiento -y es el objetivo de presentar este gráfico- es enorme.

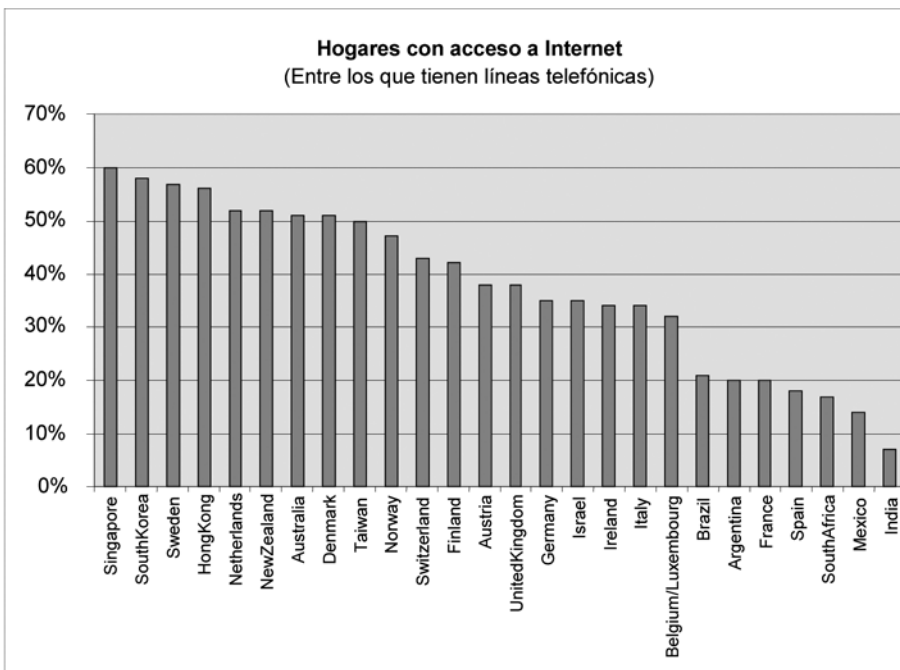


Si vemos este gráfico sobre los servidores o computadores que ha habido en el período 1982-1998 observamos que la línea es uniforme hasta 1994, y luego se produce un notable despegue. Se puede estimar que para enero de 2004 habrá unos 210 millones de equipos conectados a la red. Son cifras importantes.

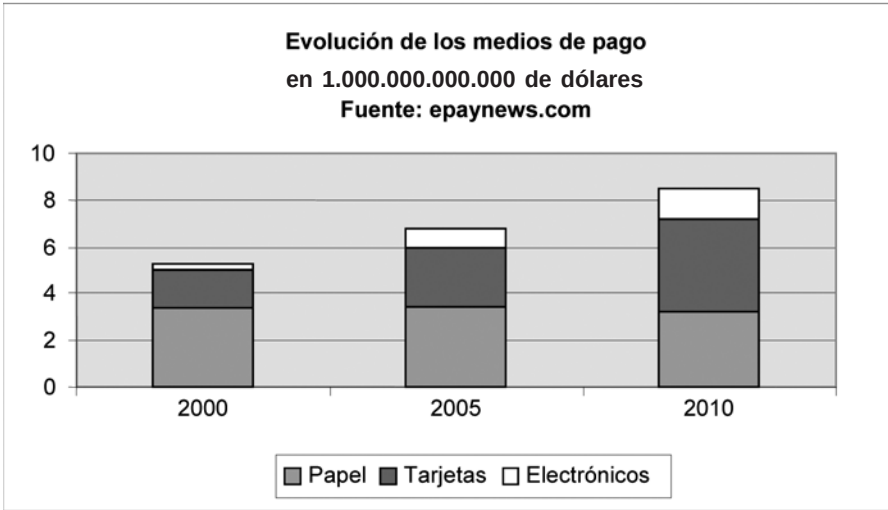
En el siguiente gráfico vemos el sentido de la curva en los años 2001 a 2005.



Si analizamos cuántos hogares con acceso a línea telefónica tienen conexión a Internet, vemos que la Argentina no está mal ubicada, porque se encuentra casi a la misma altura que Francia y otros países del Primer Mundo. Esto significa que en la Argentina un 20 por ciento de la gente que tiene línea telefónica cuenta con acceso a Internet.



Otro dato relevante, para el futuro cercano, es cómo evolucionan las transacciones de los medios de pago, expresados en billones de dólares. Este gráfico muestra que las transacciones en papel van a seguir creciendo muy poco hasta 2005 y luego van a disminuir, mientras que las transacciones en tarjetas de crédito seguirán aumentando, pero las electrónicas van a aumentar abruptamente. Esto nos hace pensar que estamos hablando de cuestiones de modernidad.



Respecto de la seguridad en Internet, vamos a recordar algo de historia. Los jeroglíficos egipcios eran una forma de codificar cierta información. Los chinos empleaban la naturaleza ideográfica de su idioma, que no era silábico ni compuesto por palabras sino que estaba formado por símbolos que indicaban una idea completa. Por ejemplo, la frase "el sol naciente es muy hermoso" se representaba con un solo símbolo, que generalmente iba derivando de cosas que tenían un cierto valor figurativo sobre el hecho de que el sol saliera. Era una forma de codificar la información, y se usaban diferentes ideogramas como para que gente de otros sectores no pudiera entenderlos.

En la India el gobierno empleaba códigos secretos para comunicarse con su red de espías. Esto lo vemos en todas las películas de espías, donde se recibe información secreta. En la Mesopotamia asiática la historia fue similar, al igual que en Babilonia y Asiria.

Es interesante saber que en *La Ilíada*, cuando Belerofonte fue expulsado del reino por haber sido acusado de intentar seducir a la esposa del rey, le enviaron una carta para que se fuera a otro reino, y en ella estaba oculta su propia condena de muerte. Es decir, ya Homero había pensado en esto en La Ilíada, mil quinientos años antes de Cristo.

Los griegos empleaban una tabla por medio de la cual reemplazaban una letra por un par de números, llamada tabla de Polibius.

Julio César fue uno de los primeros que escribió en clave desplazando las letras. Utilizando el alfabeto latino, en lugar de escribir una "a" escribía la "c", y en vez de una

"b", la "d"; es decir, desplazaba dos lugares el alfabeto, y el resultado era completamente ininteligible.

Durante el siglo pasado -a veces no me acostumbro a hablar de siglo pasado cuando me refiero al siglo XX- y lo poco que ha transcurrido del siglo XXI, los acontecimientos se precipitaron muchísimo. La Segunda Guerra Mundial desató la necesidad de manejarse con claves, lo cual a su vez trajo aparejada la necesidad de aprender a descifrar los mensajes.

A este hecho debemos sumar otro igualmente importante: la invención de la teoría de la información de Shannon, a mediados del siglo XX. Esto ha significado un paso trascendental, porque dicha teoría luego fue utilizada en muchos otros procedimientos completamente ajenos a la transmisión de información, como por ejemplo el secuenciamiento genético.

Tampoco podemos dejar de mencionar la creación en 1952 de la National Security Agency (NSA) del gobierno de los Estados Unidos de Norte América, que fijó estándares prácticamente mundiales en materia de claves. La NSA es el organismo que más matemáticos ha contratado para realizar este tipo de trabajo.

También me parece importante destacar que con la publicación de algunos libros -como *The Codebreakers*- comenzó a difundirse un concepto que hasta ese momento de ninguna manera había sido mantenido en secreto, con lo cual toda la gente pudo tomar conciencia de los problemas de seguridad que existen en la transmisión de la información.

En los años 1970 y 1975 se crean dos estándares de cifrado muy importantes, conocidos como Data Encryption Standard (DES) y criptografía pública -a los que me referiré más adelante-, y en 1980 se funda el American Council Education, abocado a la enseñanza de las distintas técnicas de cifrado.

Luego de esta breve historia me gustaría explicar en qué consiste la criptografía. En criptografía se usa una serie de términos, uno de los cuales es "texto en claro" o también "texto plano"; esto es, ni más ni menos, lo que una persona dice y es entendido claramente por los demás.

Si ese texto es sometido a un proceso de cifrado mediante la utilización de una clave, se transforma en un texto cifrado que ya no es posible entender. La información se transmite de esa manera y el receptor del mensaje debe hacer el proceso inverso: tiene que tomar ese texto cifrado que nadie entiende, utilizar la clave y reconstruir el mismo texto remitido por el emisor del mensaje.

Este es un tipo de cifrado, pero existen otros. Son famosas las películas sobre la invasión de Normandía en las que los maquíes, los integrantes del movimiento de resistencia francés, recibían instrucciones a través de las transmisiones de la BBC. Por ejemplo, la frase "Juanita, vení que papá te espera" encerraba cierto significado completamente diferente del significado coloquial de la oración.

Este tipo de cifrado, conocido como criptografía subliminal, consiste en incluir en un mensaje completamente inocente un texto que encierra cierto significado.

Estas técnicas permiten evitar que un observador externo pueda acceder a la información transmitida. De ellas la más sencilla es la trasposición, que consiste en tomar el alfabeto y desplazar determinada cantidad de letras. De esta manera la "N"

puede corresponder a la "A", la "O" a la "B", la "P" a la "C", y así sucesivamente. Si quisiera cifrar la expresión "Esto es una prueba", lo primero que tendría que hacer es ver para la primera letra en claro, la "E", qué letra se corresponde. De acuerdo con nuestra secuencia, es la letra "R"; lo mismo hago con la "S" -a la que le corresponde la letra "F"-, y así en forma sucesiva hasta cambiar todas las letras de la oración.

Mi texto claro original era "Esto es una prueba", y queda "RFGB RF HAN CEHRON".

Este sistema es fácil de descifrar. El algoritmo es muy elemental, por lo que no sirve prácticamente para nada, pero es el principio básico sobre el que se basan las técnicas del cifrado.

Nuestros corresponsales toman la frase "Esto es una prueba" y utilizan la clave de cifrado. En este caso se establece que se va a utilizar la "N" como principio, y ésta es la información que se transmite. El que va a descifrar la frase tiene la clave, sabe que es la "N", y obtiene como resultado la frase "Esto es una prueba".

Cualquier observador extraño que vea esto sin hacer un proceso para tratar de romper la clave no entendería qué es lo que se está transmitiendo.

Como síntesis, decimos que existe un algoritmo, que es la tabla de sustitución que se había mencionado anteriormente. Además, se define una clave, que en el caso que nos ocupa es la "N" (Es la letra que corresponde a la A). Se define una metodología para

que, en función de la clave y del algoritmo, se pueda transformar el texto claro en cifrado y viceversa.

Esto nos introduce en el concepto de "protocolo". El protocolo es una serie de reglas que regulan la comunicación entre dos o más interlocutores de un proceso de transmisión de información. Un protocolo se usa, por ejemplo, cuando se llama por teléfono y se dice:

- Hola, ¿hablo con el 4721-4322?-, dice el generador de la llamada
- Sí, ¿quién habla?, contesta el receptor (Nótese que si no hubiera entendido el nombre hubiera dicho: Por favor me repite el nombre)
- Habla Fulano de Tal.

Este es un protocolo por medio del cual establecemos un vínculo para empezar a hablar, porque si se marcó un número erróneo y, directamente se comienza a hablar, la otra persona no tendrá ni idea de lo que está escuchando. Entonces, se utiliza un protocolo para garantizar que esa comunicación es correcta.

¿Qué limitaciones tiene el mecanismo de cifrado que se ha visto? Que solamente pueden existir 26 claves, porque son 26 las formas diferentes en que se podría rotar el alfabeto. Y hay algo muy elemental: cualquiera puede armar en su casa la tabla. Sólo es necesario hacer 26 pruebas sencillas para descifrar el mensaje. Esto es muy sencillo, y por lo tanto esta forma de trabajo genera una inseguridad terrible.

Pero el principio básico es el mismo de los mecanismos de cifrado que se emplean en la realidad. Hay que evitar que, por la simplicidad, el sistema sea tan vulnerable que no cumpla con el objetivo final, que es que nadie se entere de lo que se está transmitiendo.

Estos sistemas se llaman "de clave simétrica" porque es necesario que ambos interlocutores conozcan la clave, y la clave es la misma; en este caso es la "N". Es decir, las partes tienen que ponerse de acuerdo antes de alejarse. Por supuesto que si alguien oye que será la "N", podrá saber qué se está transmitiendo.

Hasta este momento se utiliza el DES, el Data Encryption Standard, con sus variantes. En un principio el secreto se basaba en el conocimiento del algoritmo de cifrado. Esto tiene el inconveniente que si los oponentes obtienen el método, se pierde toda la seguridad, y no puede recuperarse más.

Otro de los serios problemas que tiene este estilo de cifrado es la dificultas de comunicarse con un interlocutor que no se conoce previamente. Si se empleara un método secreto sería necesario realizar previamente un comunicación segura para intercambiarse método y clave. ***Esto es inaceptable de ser aplicado a la totalidad de las operaciones de Comercio Electrónico.*** ¿Cómo se haría para comprar por primera vez en Amazon, por ejemplo? Sería imposible trabajar así.

Como se ha dicho previamente el método empleado en la actualidad es el de Data Encryption Standard con todas sus variantes. Este método es estandarizado por la National Security Agency, la NSA. Hay quienes dicen que fue estandarizado de tal manera que sólo ellos tienen las condiciones para poder descifrar y romper cualquier clave. Eso ni se sabe; se sospecha pero no se está seguro.

Anteriormente se dijo que si la seguridad se garantizaba por el secreto del método de cifrado empleado, ello tenía el problema que el conocimiento del método por parte de

terceros, anulaba toda la seguridad. ***Actualmente los métodos son estándar y la seguridad se garantiza por la clave.***

Por lo tanto, la cantidad de claves es muy importante. Cuando ustedes entran a una red de bancos son solamente cuatro dígitos; no es seguridad suficiente. En otros países son seis u ocho dígitos. Cuatro dígitos son muy pocos; son números, así que se pueden formar 9.999 números diferentes. Se pueden hacer las 9.999 pruebas (en promedio con 5000 alcanzaría); no es una cifra que esté fuera del alcance del ser humano.

La cantidad de claves diversas es muy importante. Reitero que en un principio la seguridad se basaba en algoritmos. Actualmente eso está abandonado, basándose el secreto en el conocimiento de la clave, al tiempo que los algoritmos son públicos.

Demos algunos ejemplos. Si la longitud de la clave fuera de diez caracteres, y si se invirtieran cien mil dólares utilizando el método de cifrado estándar, se requerirían setenta mil años poder hacer todas las combinaciones y ver cuál fue la empleada (Empleando el estado de la tecnología del año 1995). Fíjense que si se utilizaran dieciséis caracteres, en lugar de diez, para llegar a un diez con once ceros -se requerían cien mil millones de años, invirtiendo diez billones de dólares.

Esto se mide así porque es evidente que hay una relación entre la importancia del contenido del mensaje y el secreto requerido. Es muy posible que durante la época de la guerra fría los Estados Unidos pudieran invertir miles de millones de dólares para tratar de descubrir cuáles eran las claves de los rusos. Y de hecho lo hicieron; pero es muy difícil que alguien haga esa inversión para cambiar el monto de una compra hecha con una tarjeta de crédito por sólo 30 pesos, porque nadie va a tener interés en eso.

Por lo tanto, es importante diferenciar cuándo hay una necesidad de seguridad, lo que depende del hecho de que se trate de una persona física, de una empresa o de un gobierno. Del privado al gobierno la necesidad de seguridad aumenta porque generalmente el gobierno maneja información que es mucho más sensible y puede generar graves problemas si es detectada por un tercero, no solamente en situaciones bélicas, sino también, a veces, en cuestiones comerciales. Hace tiempo se contaba una historia -no sé si es real- de una negociación sobre venta de cereales en la cual la Argentina tenía rota la clave del país comprador y se enteraron de las instrucciones que el embajador había recibido sobre el precio máximo que tenía que pagar por la exportación.

Entonces, es muy importante llegar a una negociación cuando se sabe cuales son las instrucciones recibidas y se conoce el monto que el otro gobierno está dispuesto a pagar. Por eso recalcamos que la seguridad no solamente hace a problemas de contenido bélico, sino que también puede tratarse de cuestiones de índole comercial.

Para poder tener una real idea de lo que números tan grandes significan (10 billones de años por ejemplo) hicimos un cálculo. Y diez billones de años son treinta y tres mil millones de viajes de ida y vuelta en jet al sol. Las magnitudes son muy grandes, porque uno a veces ve el número fríamente y no lo imagina.

Otro enfoque.¿Qué pasa si se desea escribir todas las combinaciones de una clave en un papel? ¿Qué volumen se necesitaría para almacenar esos papeles?

Los resultados son sorprendentes. Si se quisiera almacenar en papel todas las claves diferentes que se pueden construir con 64 caracteres (512 bits) se necesita un depósito que tuviera un volumen que fuera
6200000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000
veces el volumen de la Tierra (No se asombre. Es 6,2 seguido por 125 ceros). Esto significa que para nosotros, los seres humanos, es un número infinito y está fuera del alcance de nuestra imaginación.

Estos ejemplos dan una idea de los números que se están usando. Todo esto es lo que se llama "fuerza bruta", término que en nuestra profesión se utiliza para decir que se hacen todas las combinaciones posibles. No siempre las técnicas de rupturas de clave consisten en hacer la totalidad de las combinaciones posibles.

¿Qué problema tiene la clave simétrica, es decir aquella en la que, tanto el emisor como el receptor de la información, usan la misma clave? En primer lugar, si un banco tuviera un millón de clientes, tendría que guardar en secreto un millón de claves. Esta es una cifra bastante razonable de clientes, porque hay muchos bancos que tienen más de un millón de cuentas; por ejemplo el Citibank tenía como estrategia llegar al año 2010 con mil millones de clientes, cifra que parece un poco exagerada, pero era su objetivo.

Guardar el secreto de un millón de personas es imposible, porque de alguna manera se filtra la información. Entonces surgió una idea, que es la clave asimétrica, también llamada "clave pública". Esto fue inventado cerca de mediados del siglo XX, y tiene un fuerte contenido matemático. Ya no se trata de un problema de reemplazar letras sino que subyace una fuerte teoría matemática. Las claves de remitente y destinatario son diferentes; una clave es secreta y la otra es pública, y la secreta no se puede calcular a partir de la pública. Si alguien conoce la clave pública no puede reconstituir a partir de ella la clave privada.

¿Cómo se hace cuando se envía un mensaje? La clave pública se encuentra a disposición de todo el mundo. Como un número telefónico en la guía. Cuando se envía el mensaje se lo cifra con la clave privada. El que lo recibe lo puede descifrar empleando la clave pública. Esto es importante para la firma digital. El estándar de facto que se utiliza de hecho se llama RSA.

¿Qué sucede con la firma ológrafa? Cuando Roberto y Alicia quieren firmar un documento, lo escriben, dejan un espacio abajo y ponen sus firmas. Si los dos tienen confianza de que Roberto es Roberto y Alicia es Alicia y que los dos están autorizados a firmar el documento, se quedan satisfechos. Esto es lo que sucede cuando uno firma un acuerdo.

En la firma digital nadie ve al otro, porque es un contacto virtual y lo que ven es la pantalla de una computadora. Roberto y Alicia quieren enviar un documento; entonces el que lo envía calcula un resumen o digesto que tiene una característica muy importante.

En primer lugar nunca se puede, a partir de él, reconstruir el documento original. En segundo término, cualquier cosa que se cambie en el documento también se cambiará en el digesto. La razón por la que se hace esto se verá más adelante.

Siguiendo con el ejemplo, Roberto, con la clave pública de Alicia, cifra el resumen. Así como antes agregaba la firma, ahora agrega el resumen cifrado al documento y envía todo junto. Alicia lo recibe y descifra el digesto con su clave privada; luego, con el mismo mecanismo utilizado por Roberto, hace un resumen y lo compara con el que él le envió. Si son iguales, la firma es correcta; si son diferentes, la firma no es correcta. Es decir que no fue Roberto quien lo firmó.

En suma, así como la firma ológrafa se agrega a un documento escrito, la firma digital es un texto que se agrega al documento original.

Ahora bien; ¿por qué no se cifra con RSA el documento entero y sólo se emplea el digesto o resumen? Primero, porque el proceso de cifrado con clave pública es muchísimo más lento que el que se realiza con clave privada. Es por este motivo que la clave pública no es empleada para cifrar todo el documento. Si se trata de una pequeña carta sencilla y corta, no hay problema; pero si lo que se envía es un documento que ocupa mucho espacio el proceso de cifrado con clave pública insume demasiado tiempo. Para que se tenga una idea, este mecanismo puede ser entre cien y mil veces más lento -dependiendo ello de los algoritmos y la tecnología utilizados- que el de clave simétrica.

Segundo, si se quiere garantizar confidencialidad en la comunicación, además de la firma debe procederse al cifrado con clave simétrica a través -por ejemplo- del algoritmo DES mencionado previamente.

Esto nos introduce en un tema muy importante, que es el de los protocolos. Siguiendo con nuestros personajes, veamos cómo Roberto puede estar seguro de que se está comunicado con Alicia. En primer lugar, debe generar con su equipo un número cualquiera, al azar. Luego lo cifra con la clave pública de Alicia; ella lo descifra con su clave privada y lo reenvía con la clave pública de Roberto, quien lo descifra con su clave privada. Si son iguales Roberto puede estar seguro que está comunicado con Alicia, porque si no fuera Alicia, luego del descifrado habría obtenido cualquier otro resultado.

Este es un principio de autenticación, y tiene mucho que ver con la definición de protocolos de seguridad -tema sobre el que no hablaré ahora en profundidad- que son tan importantes como las técnicas de cifrado. Se puede usar un buen cifrado, pero si las normas que regulan la comunicación no son buenas se pierde toda la seguridad que podría existir en esa comunicación.

Tomando nuevamente a los personajes de nuestra historia, Roberto y Alicia pueden usar la clave para establecer comunicaciones; pero ahora esa clave es simétrica, que de acuerdo con lo que manifesté antes puede llegar a ser entre cien y mil veces más rápida que la clave pública.

Como mencionamos previamente, el RSA es uno de los estándares de facto que actualmente se utilizan para su uso de firmas digitales.

Sin embargo no es el método que está definido en los estándares formales.

Si se busca en Internet **(http://www.itl.nist.gov\fipspubsfip186.htm)** se encontrará que no es el algoritmo RSA el estándar. ¿Por qué no se usa? Porque como los inventores Rivest, Shamir y Adleman (La sigla RSA proviene de las iniciales de los creadores) patentaron el mecanismo, el gobierno americano no podía usar esa tecnología de cifrado;

es decir, la patente la tenía un privado. Eso hubiera sido imposible. Por eso las normas de cifrado son diferentes de lo que es un estándar.

La dificultad en el RSA se basa en el obstáculo de encontrar los factores primos de números muy grandes; parte de la idea de factorizar un número de muchos dígitos: por ejemplo, descomponer un número de doscientos dígitos en sus factores primos.

Un número primo es aquél que sólo es divisible por la unidad y por sí mismo. Acuérdense cuando en el colegio primario la maestra les daba un número y les decía: "15, ¿cómo es su descomposición en factores primos?" Resulta que 15 es divisible por 3, por 5; entonces, 15 es igual a 3 por 5. Es decir, se trataba de encontrar los factores primos de ese número. Y así, 21 era 3 por 7; y 18, 2 por 9. Se podía hacer. ¿Con qué números? Con 220, 350.

Ahora, ¿qué pasa si se quisiera emplear el mismo mecanismo pero con un número que tiene doscientos o cuatrocientos dígitos? Es prácticamente imposible. La seguridad se basa en esa dificultad. Cada tanto salen artículos que buscan métodos más rápidos para lograr la descomposición. Últimamente han aparecido algunos sobre nuevos métodos. Cada vez que la tecnología avanza, obliga a aumentar la cantidad de caracteres de las claves, porque va resultando más fácil poder romperlas.

En un artículo del 15 de abril de 2002, Bruce Schneier hace una estimación de la longitud de clave requerida. La información está en los *bits.* El *bit* es la mínima unidad de información, es algo que vale 0 o 1, nada más. Normalmente, 8 *bits* constituyen un caracter. Si se quisiera transformar de bits a caracteres es necesario dividir por 8 la cantidad de bits.

Bruce Schneier dijo que había que ir aumentando la longitud de las claves a medida que pasaba el tiempo. Hizo esta estimación, y en ese artículo manifestó que pensaba que la tecnología de computación avanzaría más rápido de lo que progresó. Es decir, la realidad demostró que no avanzó tan rápido como él -en el año 95- creía que iba a avanzar.

Sin embargo, él propuso ciertas longitudes que variaban según los usos. Para los individuos, eran más cortas, para las empresas, más largas, y para el gobierno, más extensas todavía. ¿Por qué? Porque se estima que el individuo corre menos riesgo que una empresa, y que una empresa corre menos riesgo que un gobierno.

Como ya manifestamos previamente, la velocidad del RSA es del orden de mil veces menor que la del DES; varía entre cien y diez mil, pero esto depende de la elección del valor de la clave. Es importante decir que existen circuitos electrónicos, llamados *chips,* que realizan este proceso en forma automática, con lo cual se acelera sensiblemente tanto el cifrado como el descifrado.

Como ya se dijo antes la seguridad del RSA se basa en la dificultad de descomponer un número en sus factores primos. ¿Cómo se haría para un número de doscientos dígitos? Es importante mencionar que este sistema de claves podría extenderse para trabajar con más de dos interlocutores. Se podría utilizar una clave compuesta y formar una especie de *meeting;* cada uno podría tener su clave privada y existiría una clave pública para todos.

De esta manera sería posible que uno de los interlocutores enviara un documento, que otros agregaran sus firmas y que, en definitiva todos pudieran tener la certeza que había sido firmados por cada uno de los integrantes del grupo.

Es decir que este concepto se puede extender a circunstancias mucho más generales que el mero hecho de querer comprar un libro en un sitio de Comercio Electrónico. Se pueden firmar contratos por más de dos partes, etc. El concepto importante de recalcar es que este mismo principio es válido para reuniones en las que haya más de dos interlocutores. Por qué no pensar en cuerpos colegiados virtuales.

Pero la realidad no es tan simple como se la ha planteado cuando dos personas desean firmar conjuntamente un documento como nuestros amigos Roberto y Alicia. Todos sabemos que cuando firmamos una escritura se lo hace frente a un escribano público, porque entre comprador y vendedor no existe plena confianza. Se puede conocer a la otra persona y saber que la casa le pertenece, pero se quiere que alguien lo ***certifique.*** Y cuando se presenta un cheque, el comprador dice "Yo a vos te conozco, pero quiero que ese cheque esté ***certificado*** por el banco".

Es decir que las nociones de certificación y de registro surgen de las actividades que cotidianamente realizamos en el mundo real. En efecto, cuando por ejemplo Alicia quiere firmar un contrato con Roberto, cada uno lleva su respectivo documento de identidad que le fue otorgado por una entidad de registro, tal como el Registro Nacional de las Personas. Pero este hecho no es suficiente desde el punto de vista legal. Se necesita la presencia de un escribano que sea testigo de la operación, que registre las firmas y que protocolice o legalice los documentos. Este procedimiento da la garantía legal de que la operación es perfecta.

Este fenómeno del mundo real, de lo cotidiano, se repite también en el caso del mundo virtual, donde también existe la necesidad de certificar las transacciones que se realicen. Por ejemplo, a Roberto, que tiene una determinada identidad, se le asigna una clave privada y otra pública. Hay un documento que se llama "certificado", que tiene un estándar regulado por la RCC 2.527, otorgado por una autoridad certificante que asocia su identidad a su clave pública. Y también podría existir una autoridad de registración similar a los organismos de registro de documentos. La necesidad de la existencia de ambos depende de la dimensión del universo del que se esté hablando.

El que registra es el que realmente toma los datos de ese individuo y en lugar de decir "La firma que está al pie es de esta persona", dice: "Esta cantidad de doscientos dígitos que le entrego es la firma pública de esa persona". La firma privada no está porque ese documento es público, por lo que todo el mundo se enteraría.

Entonces, cuando alguien se comunica, junto con su firma pública va el certificado. Y el que lo recibe dice: "Aquí Fulano certifica que la identidad de aquella persona a la cual le asignó esta clave pública es Esteban Di Tada, que vive en tal lugar, que hace tal cosa...", etcétera. El nivel de detalle, tanto en el registro como en los datos que se piden, depende mucho del tipo de transacción que se haga, y del costo que se va a pagar por ese certificado.

En el MIT se elaboró una metodología llamada PGP para cifrar y firmar mails, que es gratuita y se entrega a todo el mundo. Pero si mañana se quiere hacer en forma electrónica una operación de comercio entre una terminal automotriz y una productora de autopartes, entre las que puede haber transacciones de varios millones de dólares, quizás tenga

que pedirse un certificado que costará, con toda seguridad, sumas importantes, porque, asociado a esa operación, hay que contratar, por ejemplo, los seguros. Normalmente hasta una operación de mil dólares el seguro es muy barato, casi gratis, pero a medida que el monto que se garantiza es más grande, los costos son mayores, no por la tecnología y los algoritmos que se emplean sino por las mayores responsabilidades que se van tomando. Ese es el concepto de certificado.

Respecto de la estructura del certificado, se trata de un documento como cualquier otro: tiene la firma, quién es la autoridad que lo emite, cuál es su validez. Un certificado que garantiza que esa firma digital pública es mía puede tener un año de validez o un número de n años. Quienes ingresan frecuentemente en Internet habrán visto la leyenda que dice que el certificado ha caducado, que si quiere continuar va a entrar en un sitio seguro, etcétera. Todo este proceso de cifrado y descifrado es transparente al usuario, nadie se tiene que preocupar por hacerlo, lo hace el software automáticamente.

Además el certificado tiene otra serie de datos: la clave pública del dueño, la identidad del emisor, la identidad del dueño, y puede haber cien extensiones.

En conclusión, así como en el mundo real es necesario certificar ciertas acciones, también lo es en el mundo virtual. Así como en el mundo real lo certifico con una fotografía y mi firma, en el virtual podría poner mi fotografía pero no serviría para identificar, lo que sí hace la firma pública.

Existen distintos tipos de certificados: el X509, el SPKI o infraestructura simple de clave pública, los certificados de buena privacidad o PGP, y las transacciones electrónicas seguras o SET, originariamente desarrolladas por Visa y que se utilizan para transacciones con tarjetas de crédito para certificar que ambas partes son quienes dicen ser para efectuar la operación.

Un tema que puede ser muy importante es el empleo de características físicas de la personas para poder identificarla a fin de firmar un documento, como puede ser la impresión de la huella dactilar, o las rayas del iris, tema este último que han desarrollado los japoneses y han comenzado a experimentar y dicen que es superior al de la huella dactilar. Se podría dejar volar la imaginación para encontrar otros métodos, como el ADN, para asociar la identidad del individuo. Pero siempre va a existir el concepto de registro, porque se requiere otra persona que determine la capacidad para actuar en procedimientos comerciales.

Por más que se examine mi ADN y se concluya en que no puede tratarse de otra persona, quién sabe si soy yo el dueño de la casa de la que digo ser el dueño y quién sabe si no estoy bajo juicio e inhibido de llevar a cabo ciertas acciones. Esto lo debe certificar una estructura.

Luego de esta exposición, quedo a disposición del auditorio para responder a todas las preguntas que me quieran formular.

PARTICIPANTE.- Me gustaría saber cuál es el estado legal en que se encuentra el tema de la firma digital tanto en la Argentina como en el resto del mundo.

Sr. DI TADA.- Como los aspectos legales no son mi especialidad tal vez no soy yo quien debe dar una respuesta. De todas maneras, creo que tendríamos que hacer una

división entre países sajones y países latinos; es decir, entre países con derecho consuetudinario y países con una legislación basada en el derecho romano.

La firma digital es un tema sobre el que se está trabajando mucho. En lo que se refiere a la Argentina, se ha sancionado una ley que todavía no ha sido reglamentada por el Poder Ejecutivo y que será una especie de ley fundamental que dará origen a toda una estructura legal.

Son muchas las cuestiones que me parece interesante analizar. Por ejemplo, los problemas de peritaje; es preciso determinar cómo se va a actuar en caso de que hubiere que hacer peritajes.

A esto debemos sumar situaciones más complejas. Supongamos que se envía un documento desde la Argentina hasta la China y que, de alguna manera, se produce un problema legal. Cómo se manejan estos casos de doble jurisdicción, no sé; tal vez el doctor Carlos Peña pueda dar una respuesta.

Sr. PEÑA.- Voy a responder en nombre de la Dirección de Informática y Sistemas.

En el mes de noviembre del año pasado se sancionó la ley 25.506. Esta norma, actualmente en vigencia, es tan fuerte que en su artículo 3° dispone: "Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia." Esto es lo que dice el artículo 3°, aunque en el artículo 4° se enumeran algunas excepciones a su aplicación.

Más adelante se establece que el Poder Ejecutivo deberá reglamentar la ley en un plazo de ciento ochenta días. Uno de los problemas que se presenta es saber quién dará las firmas digitales. El Poder Ejecutivo es la autoridad de aplicación, y es quien dentro de un sistema de libre competencia entregará a las empresas que así lo soliciten la autorización para dar firmas digitales. El concurso aún no fue realizado y tampoco se han establecido los estándares tecnológicos.

La ley fue promulgada y publicada en el mes de diciembre del año pasado, con lo cual los ciento ochenta días se cumplirán en el mes de junio del corriente año. A partir de allí todos en la Argentina podrán contar con firmas digitales, firmas que tendrán la misma validez legal que las manuscritas.

PARTICIPANTE.- Quisiera saber cuáles serán los lineamientos a seguir en la Cámara de Diputados respecto de este tema.

Sr. DI TADA.- Nuevamente cederé el uso de la palabra al doctor Peña, porque como no pertenezco a la Cámara no puedo responder; pero, ¿a qué se refiere cuando habla de "lineamientos"?

PARTICIPANTE.- Este tema seguramente tiene implícito el concepto de certificación, y al respecto en algunos ámbitos de la Cámara deberán ser mucho más estrictos que en otros. ¿Cuál es la implementación que piensa dársele dentro del ámbito de la Cámara?

Sr. PEÑA.- Uno no siempre necesita una firma digital. Para decir a alguien que nos encontraremos con él al día siguiente, a las tres de la tarde, no precisamos firmar digitalmente, ya que ello es algo que no tendrá graves consecuencias.

La Dirección de Informática y Sistemas está en este momento elaborando los programas necesarios. Lo que sucede es que tiene que adaptarse a los estándares

tecnológicos, porque por supuesto no podría hacer algo distinto. Esto no llevará mucho tiempo. Luego tendrán que realizarse las implementaciones necesarias y ver si será obligatorio o facultativo y en qué casos el uso de la firma digital.

Por supuesto que nadie puede imponer una obligación a quien no pueda cumplirla. La firma digital requiere toda una práctica, saber utilizarla, conocer en qué casos se necesita y en cuáles no.

Sr. DI TADA.- De todas maneras es importante aclarar que para el usuario este sistema no implica absolutamente ningún cambio en su trabajo. Nosotros en la universidad tenemos firmas digitales para los mails. El único problema es que a veces sale un mensaje avisando el vencimiento del certificado. El mensaje advierte que si no se lo renueva, se va a trabajar en un sitio no seguro, es decir no protegido. Luego, lo único que uno tiene que hacer es hacer clic en un botón. No es que esto entrañe un trabajo adicional sobre la gente, si la pregunta iba orientada a averiguar esto.

PARTICIPANTE.- ¿Qué opinión tiene el Colegio de Escribanos con respecto a la firma digital?

Sr. PEÑA.- Por supuesto que no podemos contestar por el Colegio de Escribanos, pero entendemos el sentido de su pregunta. Hay un artículo de la ley que dice que las entidades que controlan la matrícula en relación con la prestación de servicios profesionales podrán emitir certificados digitales en lo referido a esa función, con igual validez y alcance jurídico que las firmas efectuadas en forma manuscrita, aunque de todas maneras quedan sujetas a las fiscalizaciones de la autoridad de aplicación.

Es decir, uno podría decir que el Colegio de Escribanos y el Colegio de Abogados van a poder ser autoridades certificantes, que expidan firmas. Ahora, alguien podría pensar que ciertas firmas certificadas no serían necesarias. Hay algo que aclarar. Es muy fácil mandar y recibir con firma digital. Como decía el ingeniero Di Tada, es hacer clic sobre tres botones una vez que uno tiene preparadas las cosas, pero la disminución de costos es muy importante.

Con la informática determinados procedimientos son reemplazados por otros más eficientes. Indudablemente, si tuviésemos que mandar tantas cartas como mails mandamos ahora, sería imposible hacerlo, hasta desde el punto de vista físico; pero el tema va más allá de eso. Podríamos pensar cuáles son todos los procedimientos administrativos de todo tipo que se han generado porque la tecnología que había estaba basada en el papel. En los procesos judiciales es algo evidente, como las notificaciones por cédula. Hay muchos procesos que se configuraron porque la tecnología disponible era el papel. Si nosotros hacemos lo mismo y dejamos las normas pero haciéndolo informáticamente avanzamos pero cualitativamente nos quedamos en lo mismo. Habría que ver si puede desarrollarse una metodología que nos permita investigar cuáles son las estructuras y los procesos administrativos creados sobre la base de la tecnología del papel y la relevancia de su reemplazo.

PARTICIPANTE.- Mi pregunta es la siguiente: si nosotros implementamos un sistema de firmas digitales y certificados, ¿no estamos aumentando el desempleo? Porque estaríamos reemplazando un factor humano que hacía todas estas tareas por un sistema automático.

Sr. DI TADA.- Este es un tema muy interesante. Creo que la experiencia mundial y la de algunos países que en el pasado han tenido alguna situación de crisis económica similar a la nuestra indican que el fenómeno ha sido completamente diferente y ha aumentado la cantidad de empleo que había, porque en realidad el hecho de utilizar o no una firma digital no elimina la necesidad de contar con empleados. En el caso particular de las actuales personas que registran, es decir, los escribanos, si se los autoriza a ser autoridades certificantes creo que esto quedaría salvado o podría haber una transferencia de ingresos de un sector a otro.

Hay un caso interesante, que es el de Irlanda. Ese país, hace aproximadamente veinte años, tenía una deuda externa equivalente al 130 por ciento de su producto bruto. Tenía un alto nivel de pobreza, con un índice de desocupación que llegó a superar el 20 por ciento; y decidió iniciar un proyecto tecnológico. Es interesante destacar que la mayor producción de Irlanda en aquella época correspondía a *commodities*, básicamente de la agricultura, y más del 20 por ciento de los puestos de trabajo -creo que el 28 por ciento de ellos- estaba dirigido hacia las actividades agrícolas.

Actualmente el nivel de desocupación de Irlanda está por debajo del 4 por ciento. La proporción de gente dedicada a la actividad agrícola es solamente del 9 por ciento. Tan así es que eso le genera un pequeño problema en el sentido de que tiene que ser importadora de alimentos. El producto bruto per cápita supera los 22 mil dólares anuales. Y creo que su deuda externa es inferior al 50 por ciento de su producto bruto.

Considero que la experiencia de ese país es muy prometedora. Ellos se focalizaron en algunas áreas de la tecnología, entre ellas la informática, la electrónica, la industria farmacéutica y los servicios de medicina -respecto de estos últimos no está muy clara la forma en que los brindaban, porque me parecía un poco raro poder exportar esa clase de servicios-, y el resultado fue extraordinario.

Otros países también son ejemplo en esto. La India, en el ejercicio 2000-2001, exportó 5 mil millones de dólares en tecnología, ya sea en software o productos afines; y de acuerdo con un estudio de la firma Mc. Kenzie en el año 2008 piensa exportar por 50 mil millones de dólares.

La India tiene una estructura diferente, es una dimensión de país distinta. Son mil millones de habitantes, por lo que tiene una problemática diferente que la de la Argentina; pero hay otros países -entre ellos Rusia- que lo están haciendo, cada uno de los cuales está ocupando un nicho diferente dentro de la tecnología.

El hecho del desarrollo de una industria de software ha generado también la radicación de empresas de industrias electrónicas, con lo cual el nivel de ocupación es más alto. Por supuesto que para que esto fuera factible todo empezó con una política coherente y permanente en materia de educación a fin de generar recursos humanos capaces de sustentar este tipo de actividades.

No creo que esto genere desocupación, sino que si se conforma una política coherente referente a la evolución de las principales fuentes de recursos económicos del país, va a ser un factor de ocupación.

PARTICIPANTE.- Por un lado, ¿cuál es el ente que regula el otorgamiento de la firma digital?

Por otra parte, si yo tomara un DNI ajeno y le cambiara la foto podría intentar vender la casa del verdadero titular de ese documento; del mismo modo quisiera saber cuáles son los riesgos que se corren con la firma digital que se otorga a una persona física o jurídica, si alguien se puede adueñar de esa firma o crear una firma falsa.

Sr. DI TADA.- En general los certificados vienen cifrados con la firma de la autoridad certificante, así como el DNI viene firmado por la autoridad del Registro Nacional de las Personas que lo emite. Es imposible que no exista una posibilidad de fraude, pero desconozco la experiencia al respecto.

Pienso que la firma digital tiene más agilidad para su anulación, y además su validez puede ser por períodos más breves, dado que no exige un trabajo físico para volver a emitir un documento; se puede generar por seis meses, con lo cual el daño estaría más acotado.

Sr. PEÑA.- La autoridad de aplicación de la ley es la Jefatura de Gabinete de Ministros, y es la que debe elaborar todas las normas que controlan el sistema. Quienes entregan firma digital, dentro del Estado, son los distintos organismos, y en la administración pública nacional lo hace la Subsecretaría de Gestión Pública. En el ámbito privado lo van a hacer personas jurídicas privadas, es decir, empresas.

Cuando uno envía una firma digital, ésta tiene que ser reconocida por la ley argentina, y solamente lo son aquellas que dan las empresas reconocidas por la autoridad de aplicación y las extranjeras con las cuales se realicen convenios de reciprocidad.

El primer acto para obtener una firma digital es un acto no digital: alguien se tiene que presentar y demostrar su identidad para que le den una firma digital a su nombre, porque de otro modo cualquiera podría presentarse, dar un nombre ajeno y hacer contratos a nombre de otro. Este es uno de los temas que dependen de la reglamentación que dictará el Poder Ejecutivo; todavía estamos en período de elaboración. En la Cámara no nos preocupamos por eso porque todos los funcionarios de planta están identificados y sabemos quién es el receptor de la firma digital.

Por otro lado, es posible que se pierda la clave, como puede ocurrir con la clave de una tarjeta de crédito. Podría suceder que un empleado infiel de la empresa que entrega la firma digital filtre una clave. Frente a esto existen dos resguardos: en primer lugar, las auditorías y control de las empresas; en segundo término, los sistemas de seguro. Si alguien firma por mí tras haberme sacado la firma digital -que puede haber muchas formas-, en el anteproyecto de decreto reglamentario se prevé la contratación de un seguro.

Veamos cuál es el sistema. La firma digital es válida; mejor dicho, da presunción de validez. Podría ocurrir que una firma se pierda por culpa de la misma persona que tiene la clave; por ejemplo, es muy común que la gente escriba sus claves debajo del teclado de la computadora o en algún papelito. Quien tiene la clave es el responsable de la pérdida, más allá de la responsabilidad que le puede caber a terceros por el uso que hagan de la firma.

Este es, básicamente, el régimen general. Pero hay otros aspectos jurídicos, porque la ley establece pautas no sólo para la firma digital sino también para la denominada firma electrónica.

Sr. DI TADA.- Lo que acaba de señalar el doctor Carlos Peña es interesante. ¿Cómo hace una persona para recordar de memoria una clave de doscientos dígitos? En mi

caso particular no sólo olvido las que tienen cuatro dígitos sino que además hay veces que no recuerdo dónde las anoté.

Aquí es donde debemos hablar de algunos recursos tecnológicos muy interesantes. Uno de ellos consiste en utilizar una tarjeta *chip* de computadora para llevar la firma digital. Estas tarjetas *chip* pueden tener esquemas de seguridad muy sofisticados; por ejemplo, si alguien intenta violarlas se autodestruyen al estilo de *Misión Imposible.*

Para acceder a ellas se necesita otra clave, que puede ser manejada con mayor rapidez porque está formada por ocho o dieciséis dígitos.

Es importante saber que una persona puede llevar su firma privada en una tarjeta *chip*; si no, sería muy complicado tener que ingresar todos los dígitos cada vez que se la necesita.

PARTICIPANTE.- Pero la autoridad certificadora tiene la clave pública; no la privada.

Sr. DI TADA.- Generalmente la clave se genera en el propio equipo. Es por ello que la autoridad certificadora no tiene la clave privada. La clave pública aparece en el certificado que otorga la autoridad certificadora, pero es el propio equipo el que genera la clave privada.

Cualquier persona que tenga acceso al equipo de otra puede llegar a obtener su clave privada. El hecho de que la clave privada sea generada por el propio equipo torna dificultosa la operación desde otra computadora, como por ejemplo la de un cibercafé. Como en ese equipo no está la clave privada, es preciso incorporarla. Para eso la tarjeta *chip* resulta muy práctica; incluso ya hay lectores de tarjetas *chip* que reemplazan a las disqueteras.

Ahora bien: ¿qué ocurre si una persona pierde su tarjeta *chip*? Lo mismo que sucede cuando se pierde la tarjeta de crédito.

PARTICIPANTE.- O cuando a una persona le roban la computadora.

Sr. DI TADA.- Esa es otra situación. Lo importante es saber que cuando se pierde la tarjeta *chip* existe la posibilidad de informarlo para que caduque la validez del certificado.

PARTICIPANTE.- Me gustaría saber cuál es el retraso de la Argentina respecto de los países del Primer Mundo en materia de reglamentación y funcionamiento de la firma digital.

Sr. DI TADA.- Creo que es una pregunta muy difícil de responder, porque como la tecnología es pública cualquiera puede tener acceso a ella; entonces, el retraso estaría en el uso que se le da. Por ejemplo, quienes compramos libros en Amazon utilizamos la firma digital con un sistema conocido como SSL. Gracias a él se establece una comunicación segura porque tácitamente se produce un mecanismo de cifrado y firma digital.

Pienso que la Argentina no tiene atraso tecnológico sino demora en la implementación de los medios existentes, y estimo que con la sanción de la ley sobre firma digital se tiende a fomentar su uso.

Sr. PEÑA.- Una pequeña ventaja deriva de ese supuesto atraso. Digo "supuesto" porque tampoco yo creo que exista atraso alguno.

En este momento están saliendo. Lo está haciendo Perú y Venezuela. La primera fue en el Estado de Utah, en Estados Unidos. Recién están todos en el proceso de aplicación, no tanto en el problema legal. La ley argentina tuvo una enorme ventaja: como se hizo más tarde, se pudieron ver los errores que cometieron los otros y arreglarlos.

En realidad, la ley argentina no establece que la firma digital sea un sistema de doble clave, de clave pública y privada, lo cual nos ataría a ese tipo de tecnología, que es la que tenemos pero a lo mejor no es la que tendremos dentro de diez años. Fíjense que se define la firma digital como el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante. No se habla de claves pública y privada. Esa es una pequeña ventaja. Un país europeo, que no puedo recordar en este momento, ha modificado esto.

Las aplicaciones son innumerables. Una es en el *e-learning*, por ejemplo, la educación virtual. El problema cuando uno enseña a distancia es que no sabe quién es el que está del otro lado, quién es el que manda los mensajes, el que hace los exámenes.

PARTICIPANTE.- ¿En cuánto modificaron con respecto a la ley argentina?

Sr. PEÑA.- No, hay un país que la tuvo que modificar en su propia definición porque estaba mal definida. Nosotros podríamos imaginar formas mucho más sofisticadas de establecer la identidad, pero siempre hay un problema de costos. Por ejemplo, relacionar la clave con algunas características biométricas, como la lectura del iris, y otras.

PARTICIPANTE.- Habría que aclarar que el tema de la firma digital está inscripto en todo un problema de seguridad y confiabilidad informática. Este es uno de los tantos elementos; hay un software y un hardware que se requieren para Internet y para las técnicas nuevas de trasmisión de datos digitalizados. Esta es una de las tantas formas posibles.

Sr. DI TADA.- Les agradezco mucho haberme escuchado.

Habiéndose cumplido el objeto del seminario, lo damos por concluido, agradeciendo la participación de todos ustedes, y particularmente a la Dirección de Informática y Sistemas de la Cámara de Diputados de la Nación.