

Provisión de Protocolos de Anonimato para la Protección de la Privacidad y el Desarrollo de la Democracia Electrónica en las CMC¹

Justo A. Carracedo Gallardo⁽¹⁾, Jose-David Carracedo Verde⁽²⁾

⁽¹⁾Departamento de Ingeniería y Arquitecturas Telemáticas (Diatel). Universidad Politécnica de Madrid (UPM)
Ctra. de Valencia Km 7, 28031 Madrid / carracedo@diatel.upm.es

⁽²⁾Departamento de Ciencia Política y de la Administración III. Universidad Complutense de Madrid (UCM)
Campus de Somosaguas, 28233 Madrid. / jdcarracedo@proyectos.diatel.upm.es

Resumen: *Hasta ahora, para la protección de la privacidad en las CMC se ha hecho mucho énfasis en la inclusión de protocolos que garanticen la confidencialidad de los datos (que sólo puedan leerlos los destinatarios autorizados), su integridad (que no puedan ser manipulados) y la autenticación de los individuos o entidades que participan en la comunicación (que no pueda ser suplantada la personalidad de los actores). En esta ponencia se discute acerca del significado que el concepto de privacidad tiene en el contexto de las CMC. Se analizan, también, determinadas situaciones en las que es necesario preservar la identidad del sujeto (anonimato) para conseguir una eficaz protección de la privacidad. Así, muchos de los ataques que pueden ejercerse para establecer amplios procesos de vigilancia pueden ser neutralizados mediante la adecuada implantación de protocolos avanzados de anonimato. Asimismo, se analiza cómo en muchas de las actividades necesarias para la implantación de la democracia electrónica es necesario conciliar la autenticación de los participantes con el hecho de que no se pueda establecer una relación entre las opciones o propuestas que realicen y quién las ha realizado. Esta situación se produce frecuentemente en los entornos de participación de los ciudadanos en la toma de decisiones y, de forma clara, en los escenarios de votación electrónica (que son un caso particular de éstos). Se describirá de forma resumida (e inteligible para los no especialistas en estas tecnologías) cómo el actual desarrollo de las técnicas de seguridad en redes telemáticas permite proveer los adecuados servicios de anonimato para que requisitos de este tipo sean satisfechos.*

1. ES NECESARIO DISPONER DE REDES SEGURAS

Las redes, debido a su dispersión geográfica y a los múltiples equipos y sistemas que de ellas forman parte, presentan un marco idóneo para posibles ataques y operaciones no autorizadas. Como veremos más adelante, el uso malicioso de la red puede afectar tanto a la seguridad de los sistemas como a la validez de la información que se almacena o transfiere. Modificar y falsificar un documento representado en formato electrónico es mucho más sencillo que hacerlo sobre un documento escrito en papel. Asimismo, debido al acceso remoto, sin ninguna de las cortapisas que introduce una comunicación presencial, es también relativamente

¹ Este trabajo ha sido realizado dentro de las tareas de proyecto *VOTESCRIPT: Votación Electrónica Segura basada en criptografía avanzada*, subvencionado dentro del Plan Nacional de I+D+I (código TIC 2000-1630-C02).

sencillo hacerse pasar en la red por quien realmente no se es, con los consiguientes riesgos de pérdida de fiabilidad de la información que se recibe.

La vulnerabilidad de las redes ante determinados ataques puede dar lugar a que ciertos derechos y libertades de que gozan los ciudadanos en otros ámbitos de comunicación convencionales no puedan ser ejercidos eficazmente en entornos de Comunicaciones Mediante Computadores, CMC. Ello hace que, admitiendo este tipo de limitaciones, sea inviable hablar de cualquier proyección digital de escenarios de comunicación que en la actualidad se llevan a cabo usando, por ejemplo, el papel como soporte.

Hace relativamente poco tiempo que se empezaron a diseñar e implantar redes telemáticas. No obstante, no es necesario insistir en el auge y expansión que las CMC ya han alcanzado y en el hecho de que su penetración prosigue extendiéndose cada vez a más esferas sociales. Algunos autores han visto en este proceso un cambio cualitativo en nuestras sociedades, un proceso constituyente de la llamada “Sociedad de la Información” o “Sociedad Red” [1].

No obstante, por desgracia, no está suficientemente extendida entre los usuarios de redes telemáticas la **exigencia** de soluciones técnicas (que las hay) para neutralizar la vulnerabilidad de las redes a que antes hacíamos referencia. Esta debilidad se consigue cancelar mediante las técnicas de Seguridad en Redes. Desafortunadamente, en gran medida, ese tipo de demandas colisionan con la interpretación que hacen algunos poderes públicos acerca de lo que debe ser considerado como seguridad en las comunicaciones. Esta ponencia está en línea con otros trabajos de los autores [2] [3] que tratan de centrarse en el análisis de los problemas desde el punto de vista de los ciudadanos, procurando detectar cuales son sus necesidades y apuntando a los remedios que las satisfagan.

Mediante la incorporación de servicios de seguridad (que en el siguiente apartado se describen) en las redes telemáticas se ha de conseguir, al menos, garantizar que los derechos y salvaguardas actualmente reconocidos en las comunicaciones convencionales sean respetados también en la proyección y plasmación que estos tienen en las CMC. Pero hay más: siendo esto necesario, no es suficiente: mediante una adecuada utilización de los servicios de seguridad, los ciudadanos podrían disponer de herramientas que les permitiesen alcanzar niveles de independencia y privacidad como jamás antes en la Historia se les habían presentado. Al entorno configurado conforme a esta perspectiva es a lo que denotamos como *Seguridad Cívica*, acepción que ampliaremos más adelante.

2. ATAQUES, PROTOCOLOS DE SEGURIDAD Y SERVICIOS DE SEGURIDAD

2.1 Protocolos y servicios telemáticos

En las CMC, el intercambio de información que se lleva a cabo entre los sistemas informáticos que permiten el acceso a la red (y también entre aquellos que soportan su funcionamiento interno) está gobernado mediante *protocolos telemáticos*. De forma muy

general² y simplificada, podríamos decir que en un protocolo se especifica tanto la estructura interna de la información digital que intercambian entre sí los computadores que protagonizan la comunicación, como las reglas del juego bajo las cuales ésta se lleva a cabo. Por otro lado, el *servicio telemático* asociado a un determinado protocolo podemos considerarlo definido por el conjunto de operaciones de comunicación que se ofertan al usuario para que haga uso de ellas cuando lo considere necesario.. Así, por ejemplo, podemos elegir entre distintos protocolos de correo electrónico (X.400, MIME, etc.) cada uno de los cuales ofrece un servicio concreto y diferenciado pero muy similar al que ofrecen los restantes.

En realidad, podríamos decir que lo que le importa al usuario final son los servicios que se le ofrecen y la manera en que la *Interfaz de Usuario* (presentación en pantalla, uso del teclado y del ratón, etc.) le permite hacer uso de las facilidades que el servicio le brinda. Por contra, la estructura y funcionamiento del protocolo serían competencia de los técnicos que lo desarrollan o instalan.

2.2 Servicios de Seguridad

En general, denominamos *ataque* a cualquier uso malicioso de la red, realizado de forma intencionada. Además, accidentalmente, se podrán producir otras disfunciones en el comportamiento de las redes. Será, por tanto, necesario encontrar soluciones que contrarresten estos peligros.

Ello se consigue mediante los *servicios telemáticos de seguridad* que protegen las comunicaciones de los usuarios ante posibles ataques. Un servicio de seguridad, que no difiere, desde un punto de vista conceptual, de cualquier otro servicio telemático, es proporcionado por el correspondiente *protocolo telemático de seguridad*. Nuevamente hay que insistir en que lo que le interesa al usuario es conocer qué servicios de seguridad le ofrece el sistema en el que trabaja y de qué ataques le protegen.

Para hacer frente a los *ataques* que puedan presentarse, en la norma ISO 7498 -Part 2, *Security Architecture* [4], que en 1988 puso los cimientos de la nueva conceptualización de la Seguridad en Redes, se definen cinco servicios básicos de seguridad:

a) *Servicio de Autenticación (Authentication)*³. Este servicio sirve para garantizar que una entidad comunicante (una persona o una máquina) *es quien dice ser*. En la literatura puede encontrarse también bajo la denominación de “servicio de autenticación”, ya que ambos términos

² Carlos Monsiváis en “Días de Guardar” (Editorial Era, México, reimpresión de 2000, pag 17) dice: *Generalizar: mentir y decir la verdad al mismo tiempo, sin dejar de mentir y sin dejar de decir la verdad*. En esta ponencia, dirigida a personas no especialistas en temas relacionados con la Telemática, las descripciones técnicas tienen que ser, por breves, inevitablemente algo imprecisas. No obstante, estas generalizaciones no merecen ser calificadas de mentiras, aunque sean parciales, porque no pretenden engañar a nadie. Más bien podríamos decir que no son *totalmente verdaderas*, pero sí *suficientemente verdaderas* para los objetivos aquí perseguidos.

³ Además de la denominación en español, en algunos casos se añade también el nombre con el que se conocen estos conceptos en inglés, debido a que la mayoría de la literatura sobre este asunto con la que el lector puede encontrarse está escrita en ese idioma.

son perfectamente válidos en español, aunque “autenticación” es de origen más antiguo y más auténtico (y más breve). Este servicio protege contra un ataque muy fácilmente perpetrable en las redes: la *suplantación de personalidad (masquerade)* mediante el cual una entidad remota se hace pasar por quien no es.

b) *Servicio de Confidencialidad de los datos (Data Confidentiality)*. Proporciona protección para evitar que los datos sean revelados, accidental o deliberadamente, a un usuario no autorizado. Es decir, garantiza que los datos tan sólo van a ser *entendibles* por el destinatario o destinatarios del mensaje. Para ello, el mensaje se alterará de tal manera que aquellas personas que no sean los destinatarios autorizados, aunque lo capturen, no podrán ser capaces de entender su significado. Cuando es proporcionado, protege a los usuarios de las redes contra el típico “pinchazo” (*wiretapping*) de una comunicación. Para llevar a cabo estos pinchazos, en la actualidad no es necesario recurrir a escaleras y alicates, ya que se puede acceder indebidamente a un nodo de la red y obtener parte de la información que por allí circula. Este tipo de ataques se denomina *de divulgación o repetición del contenido (replay)*.

c) *Servicio de Integridad de los datos (Data Integrity)*. Este servicio garantiza al receptor del mensaje que los datos recibidos coinciden exactamente con los enviados por el emisor de los mismos, de tal forma que puede tener garantías de que a la información original no le ha sido añadida, ni modificada, ni sustraída alguna de sus partes. Es decir, el receptor de la información (o el proveedor del servicio) detectará si se ha producido o no un ataque de *modificación del mensaje*, lo que le permitirá rechazar o dar por buenos los datos recibidos.

d) *Servicio de No Repudio (Non-repudiation)*. Está relacionado con el intercambio de mensajes a través de redes telemáticas para dar garantías respecto a su emisión y recepción. Como su nombre indica, sirve para evitar que alguno de los participantes en la comunicación niegue (repudie) haber formado parte de ella. Podríamos distinguir tres situaciones:

d1) *No Repudio con prueba de origen*. En este caso, el receptor del mensaje adquiere una prueba, demostrable ante terceros, del origen de los datos recibidos.

d2) *No Repudio con prueba de envío*. El receptor o el emisor del mensaje adquieren una prueba, demostrable ante terceros, de la fecha y hora en que el mensaje fue enviado.

d3) *No Repudio con prueba de entrega*. El emisor del mensaje adquiere una prueba, demostrable ante terceros, de que los datos han sido entregados al receptor adecuado.

e) *Servicio de Control de Acceso (Access Control)*. Sirve para evitar el uso no autorizado de los recursos de la red. Puede servir para permitir que sólo quien esté autorizado para ello pueda conectarse a una determinada máquina, y para que, una vez conectado, cada usuario sólo pueda tener acceso a aquellas facilidades para las que ha adquirido permisos.

Hay quienes añaden un sexto servicio: *disponibilidad (availability)*. Hace referencia a la protección que es necesario introducir para que las distintas partes del sistema que componen la red estén disponibles para ser utilizadas por quienes dispongan de autorización para ello. Podríamos considerar que esto no constituye realmente un nuevo servicio, sino más bien un

conjunto de facilidades de seguridad, ya que las protecciones que teóricamente provee pueden ser satisfechas con el uso combinado de los anteriores cinco servicios básicos.

Además de estos servicios “clásicos” que se definieron a finales de la década de los 80, debido a los requisitos que exigen algunos de los nuevos servicios telemáticos que están actualmente siendo vislumbrados (aunque aún escasamente implantados) cabe hablar de un nuevo servicio de seguridad en las redes telemáticas:

f) *Servicio de Anonimato (Anonymity)*. Se trata de conseguir que la identidad de la persona que realiza una determinada operación telemática permanezca oculta ante algunos de los actores presentes en esa operación. Se trata de emular en la Red situaciones de la vida real (si se puede seguir llamando así por mucho tiempo) en las cuales es conveniente mantener cierto anonimato. Si dentro del correo postal es posible enviar cartas de forma anónima, también el correo electrónico debe permitir esa posibilidad.

Veamos también otros casos en los que este tipo de requisitos se presentan. En primer lugar, supongamos, por ejemplo, un buzón de sugerencias o de quejas dispuesto para que éstas sean depositadas en él de forma anónima. Otro caso parecido sería la realización de encuestas anónimas a un grupo de alumnos. Si estas tareas queremos llevarlas a cabo por vía telemática (ello sería cómodo, ágil y eficaz) sería necesario que el agente telemático que recibiese los mensajes no fuese capaz de relacionar las opiniones vertidas con los autores de las mismas. En el primero de los dos ejemplos podría permitirse que fuese cualquier persona quién depositase sus quejas en el buzón, y que formulase más de una. Pero en el segundo de ellos, sería necesario autenticar primero al alumno (sólo un grupo de ellos puede opinar) y garantizar después que no se conocerá cuál ha sido su opinión.

Esta misma complejidad (tener que combinar la autenticación de los actores y el mantenimiento del anonimato en relación con los datos que han sido depositados) se produce también en el *voto electrónico*. En la proyección electrónica del esquema de votación convencional, habrá que garantizar que solamente depositan su voto en la “urna” las personas autorizadas para ello y que sólo votan una vez y por una sola opción. Por supuesto, debe permanecer oculto quienes fueron lo que votaron cada una de las opciones. Además, el votante debe de disponer de mecanismos que le permitan comprobar que su voto ha sido contabilizado adecuadamente en la opción que eligió.

Otro caso interesante es el del dinero digital. Es latoso tener que llevar dinero en los bolsillos, pero tiene una enorme ventaja: podemos comprar de forma anónima. Por ello, el dinero digital mediante el que se compre a través de la red deberá ser también anónimo, cosa que no ocurre en la actualidad en las operaciones de *Comercio Electrónico*. El uso de tarjetas de crédito convencionales es cómodo y eficaz, pero permite que se creen registros en los que se relacione qué compramos, cuándo y dónde. Consideramos que sería necesario que el uso de las tarjetas de crédito estuviera dotado no sólo de confidencialidad, sino además protegido con servicios de anonimato, de forma que el banco sepa cuanto dinero se ha gastado, pero no dónde ni en qué, y el vendedor tenga certeza de que cobra el importe, pero no tenga capacidad para saber de quién. Este tipo de comportamiento sería el que se correspondería con un tipo especial

de tarjetas inteligentes que operasen bajo una infraestructura telemática: las *Tarjetas de Crédito Anónimas*.

2.3 Los servicios de seguridad son un valor añadido

Es importante percatarse de que los *servicios de seguridad* son un caso particular de los *servicios telemáticos* y que casi nunca aparecen de forma aislada, sino mejorando la funcionalidad de otro servicio telemático más convencional. Así, por ejemplo puede decirse que el PGP es un protocolo que proporciona un servicio de correo electrónico que, además, ofrece los servicios de autenticación del origen de los datos, integridad y confidencialidad. Es decir es un correo electrónico que ofrece funcionalidades similares a las otras aplicaciones corrientes de correo, pero que añade las protecciones que ofrecen los tres servicios de seguridad citados.

En algunos casos, como el del voto electrónico cuando se implemente, el anonimato será un valor añadido de obligada presencia, ya que en caso de no estar contemplado, el servicio de voto sería totalmente inservible. Algo similar debería ocurrir con el correo electrónico: un sistema que no ofrezca, como mínimo, los tres servicios de seguridad presentes en PGP debería ser rechazado por los usuarios. Además, para obtener una funcionalidad equivalente al correo postal certificado o a los envíos con acuse de recibo, sería imprescindible añadirle el servicio de no repudio de entrega.

Lo que queremos hacer notar es que son los ciudadanos los que deben exigir, de forma organizada, que las comunicaciones sean seguras, presionando a los proveedores de los servicios para que implanten las correspondientes protecciones de seguridad. Por ejemplo, el que las transacciones comerciales en la Red permitan el anonimato de la operación en los casos que el comprador lo crea conveniente, es una necesidad que han de sentir los ciudadanos usuarios para proteger su privacidad. Nunca será algo que interese a las empresas que ofrecen en la actualidad esos servicios, para las cuales, además de un engorro por el aumento de complejidad tecnológica que conlleva, representa la pérdida de una información que se cotiza muy bien en el mercado.

3. CÓMO PROVEER LOS SERVICIOS DE SEGURIDAD: CRIPTOGRAFÍA

Para implementar protocolos de seguridad que proporcionen a los usuarios los correspondientes servicios de seguridad, es necesario hacer uso de los llamados *mecanismos de seguridad* que son, podríamos decir, los ladrillos con los que se construyen los protocolos. La mayoría de los mecanismos de seguridad se basan en técnicas criptográficas, o, dicho de otro modo, la mayoría de los mecanismos de seguridad son *mecanismos criptográficos*.

La criptografía es la ciencia y el arte de ocultar mensajes. Aunque ha sido una práctica que ha venido llevándose a cabo desde hace miles de años, ha sido con el concurso de los computadores cuando ha adquirido la pujanza y el rigor con los que hoy se presenta.

3.1 Criptosistemas de clave secreta y de clave pública

Como ya es bien sabido, existen dos tipos de criptosistemas:

- a) Criptosistemas **simétricos** o de **clave secreta**, en los que se usa una misma clave secreta para cifrar y para descifrar los mensajes. (En este caso podríamos decir también “encriptar” y “desencriptar”, términos algo controvertidos en español). La criptografía clásica operaba bajo este mismo esquema. Los dos algoritmos más extendidos son el DES, nacido como estándar USA, y el europeo IDEA, aunque en la actualidad está en fase de aprobación otro algoritmo mucho más robusto: el Rijndael.

Este tipo de criptografía, con la que se pueden conseguir todos los servicios básicos de seguridad, representa un serio problema a la hora de distribuir y renovar las claves en entornos constituidos por grupos amplios de personas pertenecientes, además, a diferentes organizaciones. A modo de ejemplo, podemos pensar en grupo de tan sólo cuatro personas que pretendan establecer comunicaciones seguras dos a dos: se necesitarían seis claves secretas diferentes, de entre las cuales cada usuario estaría obligado a custodiar tres de ellas. Por ello, para grupos numerosos, como son los que se presentan en la Red, el uso exclusivo de este tipo de seguridad es, de por sí, impracticable

- b) Criptosistemas **asimétricos** o de **clave pública**, en los que cada usuario posee un par de claves, una de las cuales, la *clave privada* debe mantener secreta y la otra, la *clave pública*, deberá ser, como su nombre indica, de general conocimiento dentro del grupo en el que se esté trabajando. Este tipo de criptografía fue descubierto a finales de los 70 y representa un avance revolucionario en relación con lo que se había venido plateando hasta entonces. Aunque existen múltiples algoritmos que satisfacen estas condiciones, el RSA es el más extendido y usado de ellos. Se puede proceder de dos formas distintas:

b1) Si A quiere enviar un mensaje *confidencial* a B, cifrará el mensaje con la clave pública de B. Se puede demostrar que solamente B puede descifrar ese mensaje usando su propia clave privada (que sólo él conoce).

b2) Si A cifra un mensaje usando su clave privada, tanto B como cualquier otro usuario puede descifrarlo usando la clave pública de A, que es por todos conocida, adquiriendo seguridad de que el mensaje fue cifrado por A (*autenticación*) y que es el mismo que A procesó (*integridad*).

Debido a que ambos tipos de criptosistemas poseen ventajas y desventajas, la mayoría de los protocolos de seguridad se diseñan usando tanto algoritmos simétricos como asimétricos.

3.2 La firma digital y otros mecanismos para la provisión de servicios de seguridad

La **firma digital** es un mecanismo de seguridad de gran importancia porque cumple, en el mundo de las CMC, la misma función que la firma caligráfica en las comunicaciones

convencionales que utilizan el papel como soporte (aunque de forma muchísimo más robusta y segura). Se basa en el procedimiento de cifrado que antes hemos catalogado como b2), sólo que en este caso lo que A cifra no es el mensaje completo sino una muestra reducida, un resumen o *hash* de tamaño fijo (120 o 160 bits, según el algoritmo) e independiente de la longitud del mensaje original.

La firma digital sirve para proporcionar los servicios de *autenticación* y de *integridad*. El *control de acceso* suele conseguirse combinado con el de autenticación, de forma que una vez determinada la identidad de la entidad, se conoce, mediante unos registros previamente establecidos, cuales son las funcionalidades que le están permitidas.

Para proveer el *no repudio*, es imprescindible la presencia de *terceras partes de confianza*, **TTPs**, que son agentes telemáticos (es decir, sistemas automáticos) que, a requerimiento de partes, emiten piezas de información que pueden servir como *pruebas* o *evidencias* demostrables ante terceros. No sólo el servicio de no repudio sino muchos otros requieren de TTPs para ofrecer adecuadamente las protecciones que les son propias.

En los escenarios de comunicaciones seguras que será necesario implantar para la provisión de los servicios que requieren los ciudadanos deben existir múltiples TTPs de funcionalidades diversas constituyendo las llamadas *Infraestructuras de Clave Pública*, **PKIs** (de su nombre en inglés), entramado de agentes telemáticos que resulta imprescindible para la provisión de servicios avanzados de seguridad. Además de la adecuada definición técnica de las funciones que cumplen, será fundamental e imprescindible disponer de una reglamentación jurídica que sirva para proteger la privacidad de los ciudadanos, de forma que determine las responsabilidades con que deben pechar tanto sus gestores como quienes utilicen sus servicios.

El **certificado digital** es un documento, una pieza de información, de capital importancia en el que se asocia el nombre de una entidad con su clave pública (pareja de la clave privada correspondiente) durante un periodo de validez. El certificado es emitido por una TTP especial denominada **Autoridad de Certificación, CA**. Puede afirmarse que no puede existir un escenario de seguridad robusto donde no existan una o varias CAs. En la normativa legal vigente acerca de la validez de la firma digital, tanto en España [5] como en otros países, se dedica especial y pormenorizada atención a fijar las exigencias y los requisitos que deben cumplir tanto los certificados como las CAs que los emiten.

3.3 Esto y más para la provisión de servicios de anonimato

Para la provisión del servicio de anonimato, son de utilidad todos los mecanismos criptográficos antes referidos, además de otros específicos entre los que cabe destacar, por más llamativos, la *firma opaca* o *firma ciega* (*blind signature*) y *el secreto dividido*.

Un equivalente de la **firma opaca** “en el mundo del papel” podría consistir en que A prepara un documento para que sea firmado por B sin que B vea lo que está firmando. Para ello lo introduce en un sobre junto con un trozo de papel carbón, cerrando después el sobre. B firma

en el sobre y la firma se estampa en el documento. A recupera el sobre, lo abre, tira el papel carbón y obtiene el documento firmado por B. De forma similar, el mecanismo criptográfico de firma ciega se basa en la multiplicación del mensaje por un factor numérico de opacidad que sólo A conoce y que puede ser retirado por A una vez que haya obtenido la firma de B. Naturalmente, en el escenario de seguridad se han de proporcionar las necesarias salvaguardias para que B se decida a firmar a ciegas.

Por su parte, el **secreto dividido** es un equivalente digital del proceso seguido en algunos bancos mediante el cual dos o más ejecutivos poseen una llave de la caja fuerte, de tal forma que sólo juntándose todos ellos es posible abrirla. En nuestro caso, en entornos de seguridad en redes, consiste en dividir una determinada información secreta y repartirla entre varios actores de un proceso: sólo juntando las partes puede recuperarse el secreto completo (sin que ninguno de los actores tenga que revelar a los restantes cuál es su parte del secreto).

En los casos de voto electrónico y de dinero anónimo que antes hemos expuesto a modo de ejemplos significativos, tanto la firma opaca como el secreto dividido son, junto a otros mecanismos que aquí no citamos por razones de oportunidad, de gran utilidad para proporcionar anonimato junto con la imprescindible constatación de que quien opera es una persona autorizada para ello.

3.4 Análisis de riesgos y políticas de seguridad (o “la Telemática es demasiado importante como para dejarla sólo en manos de telemáticos”)

A modo de cierre, cabe decir, que para establecer comunicaciones seguras dentro de un determinado entorno o *dominio de seguridad*, será necesario realizar, de forma metódica, un **análisis de los riesgos** allí existentes y detectar los *ataques* contra los que es menester defenderse, de lo cual se deducirán los *servicios de seguridad* que son necesarios en cada escenario de comunicación. Para proveer los servicios será necesario que alguien implante los correspondientes *protocolos de seguridad*, lo que conlleva el uso de determinados *mecanismos de seguridad y algoritmos criptográficos*, además del concurso de las varias y distintas *TTPs* que constituyen la *PKI* en la que se inscribe el dominio de seguridad.

De forma global, la **política de seguridad** que se defina en ese entorno, por quienes hayan sido comisionados para ello, debe tener en cuenta todos estos elementos y decidir cuales de ellos serán usados en cada caso, determinando, consecuentemente, qué tipos de claves que han de ser utilizadas, cómo han de ser distribuidas⁴, y en general, las reglas de comportamiento y las responsabilidades (legales o de carácter interno) de todos los actores que participan en la comunicación.

⁴ Por cuestiones de espacio y oportunidad, se ha optado por no abordar en esta ponencia la problemática de la distribución de claves y las intenciones que han aparecido (y no desaparecido del todo) respecto a la existencia de depósitos de las claves secretas (*Key Escrow*) en agencias accesibles por los poderes públicos, propuestas técnicas de importantísimas repercusiones políticas y sociales. Desafortunadamente, el debate acerca de los pros y contras de estos esquemas es un debate inexistente en nuestro país (no así en otros).

Parafraseando una sentencia famosa (cuya autoría ha sido adjudicada a más de un personaje), es fácil llegar a la conclusión de que *la Telemática es demasiado importante como para dejarla sólo en manos de telemáticos*⁵. Sobre todo en lo que a los servicios de seguridad se refiere, debido a lo mucho que pueden afectar a la privacidad de las comunicaciones y a la implantación de procedimientos digitales que posibiliten un reforzamiento y una mejora de las prácticas democráticas.

4. PRIVACIDAD Y DEMOCRACIA: SEGURIDAD CÍVICA

4.1 Los requisitos de los ciudadanos

Sin pretender hacer una definición rigurosa y precisa, podríamos decir que lo que aquí se entiende por **seguridad cívica** es el conjunto de algoritmos, mecanismos de seguridad, protocolos, servicios, determinación de riesgos y, en suma, políticas de seguridad y métodos de trabajo que son necesarios usar para establecer comunicaciones seguras sobre redes telemáticas, *teniendo en cuenta las necesidades de la vida diaria de los ciudadanos normales*, permitiéndoles el ejercicio de los derechos cívicos que les son reconocidos en otros ámbitos convencionales de comunicación, y mejorando (respecto de esos mismos ámbitos) los niveles de independencia y privacidad actualmente existentes.

Algunos sectores de la población temen que, inevitablemente, la informatización de la mayoría de las actividades de comunicación de los ciudadanos desembocará en una merma de su **privacidad** y de sus derechos. Por contra, nosotros afirmamos que la implantación de servicios de seguridad bajo la orientación de lo que aquí hemos denominado **seguridad cívica**, no sólo garantiza los derechos ya existentes, sino que permite expandir dichos derechos, ya sea en múltiples facetas de democracia digital, o, desde otra perspectiva, proporcionando mecanismos que pueden contribuir a solventar diversos problemas relacionados con las desventajas y amenazas de la *estratificación digital* (denominada hasta ahora *digital divide*[6] en inglés). Una ciudadanía capaz de usar y demandar plenamente sus ciberderechos, tan solo puede dar lugar a una sociedad más justa y democrática.

Multitud de ciudadanas y ciudadanos podrían demandar comunicaciones seguras a través de las redes telemáticas que les permitiese relacionarse entre sí fuera del alcance de miradas indiscretas, poder realizar operaciones bancarias, comerciales y administrativas sin pérdida de privacidad, y poder participar en procesos de reflexión y toma de decisiones sobre asuntos que afecten a su vida diaria, que pueden ir más allá de la mera emisión de voto electrónico para elegir entre propuestas predefinidas.

Por ello, el término **seguridad cívica** se propone aquí en contraposición con otros requisitos y otras soluciones que proceden de dos ámbitos distintos:

⁵ Tampoco será cuestión de dejarlos fuera de juego. Antes bien, deberían abordarse los problemas y las soluciones desde una perspectiva multidisciplinar, aprovechando la sinergia generada por una doble visión investigadora en las CMC: la tecnológica y la que se fija en los aspectos jurídicos, sociales y políticos.

Uno de ellos es el que tiene que ver con ámbitos militares, o de espionaje, o de mafias criminales, o de cualquier otro entorno cerrado, en los que los bienes o valores puestos en juego puedan ser muy elevados desde el punto de vista de los estados (cada vez más distantes del de los ciudadanos) y, por supuesto, muy diferentes a los que se manejan en la vida ordinaria. El otro se corresponde con los intereses y necesidades del sistema capitalista, tanto desde el punto de vista de las empresas en busca de beneficios (a costa de lo que sea) como de las actuaciones gubernamentales (cada vez más proclives a proporcionar lo que a las empresas les interesa).

4.2 Qué entendemos por privacidad

En algunos sitios se traduce la palabra inglesa *privacy* por *intimidad*. La idea de intimidad está más relacionada con la “zona espiritual íntima y reservada de una persona o grupo” como la define el ínclito Diccionario de la Real Academia. Aquí se ha optado por traducir “*privacy*” por el neologismo *privacidad* (no recogido en el diccionario de la Academia), resaltando su carácter de derecho ciudadano a mantener protegido aquello que afecta a comportamientos sociales que sólo incumben a una persona o un grupo reducido de ellas. Podríamos, por tanto, considerar que la privacidad es la extensión de la intimidad a aspectos más formales y públicos relacionados con las sociedades modernas y sus dinámicas de mercantilización.

Por otra parte, con frecuencia, principalmente en la literatura procedente de países de habla inglesa, se tiende a considerar *confidencialidad* como casi sinónimo de *privacidad*. Si bien es cierto que en multitud de casos la primera es fundamental para la obtención de la segunda, no deben confundirse, ya que, el *uso coordinado* de los servicios y políticas de seguridad es el que proporciona, en su conjunto y dependiendo de cada caso, la necesaria **privacidad** en las operaciones que realizan los ciudadanos a través de redes telemáticas. De hecho, en muchos casos es necesaria la inclusión del servicio de anonimato para obtener la privacidad

4.3 La robustez de los criptosistemas de la seguridad cívica

La doble contraposición, que comentábamos más arriba, entre la *seguridad cívica* y otros ámbitos poco proclives a satisfacer las necesidades reales de los ciudadanos, nos acerca a reflexionar sobre el grado de robustez que deben tener los algoritmos y los sistemas que deben dar soporte a las comunicaciones protegidas que se lleven a cabo teniendo en cuenta estos intereses. En líneas generales, en todos los casos, la confianza entre los distintos participantes en comunicaciones seguras está basada en el conocimiento que ellos tienen acerca de la fortaleza de los algoritmos criptográficos usados, de forma que les sea proporcionado un *razonable* nivel de seguridad. En palabras de Diffie y Landau [7], “*un criptosistema se considera seguro cuando un oponente no lo puede romper bajo razonables circunstancias, en una razonable cantidad de tiempo; a un coste razonable*”. Aunque el término *razonable* aquí utilizado resulta bastante vago, debemos interpretarlo bajo una óptica economicista, relacionándolo con el tipo de valores o bienes puestos en juego durante el proceso de comunicación.

Podemos afirmar que, los algoritmos “corrientes” operando en computadores “corrientes” están en condiciones de proporcionar una seguridad que es varios órdenes de magnitud superior a la que hoy en día se obtiene con las garantías legales que protegen las comunicaciones postales y telefónicas. La robustez de una firma digital es incomparablemente superior a que la que ofrece una firma caligráfica. Por esta razón, los criptosistemas que han de operar bajo los requisitos de la *seguridad cívica* no tiene porqué estar diseñados de tal manera que su fortaleza sea tal que no puedan ser violados por las potentísimas máquinas que en algunas agencias gubernamentales existen. Antes bien, deben estar pensados para hacer frente a las amenazas reales que se presentan en su ámbito.

Es posible, y bastante probable, que las agencias gubernamentales de inteligencia puedan estar en posesión de potentísimas máquinas y evolucionadísimas técnicas de descriptado y criptoanálisis capaces de violar la seguridad de los modestos mensajes que se intercambian bajo el paraguas de protección de la *seguridad cívica*. Es también posible que sean capaces de romper los códigos de unos pocos durante periodos no muy largos de tiempo, pero de lo que sí podemos estar seguros es de que no son capaces de vigilar a todos durante todo el tiempo. Además, cuanto más gente use los servicios de seguridad, más difícil será para estas agencias la violación masiva de la privacidad de las comunicaciones, cosa que en la actualidad es tarea rutinaria (y no hablamos a humo de pajas).

Además, cuando la potencia de cálculo de los ordenadores vaya en aumento y, consecuentemente, disminuya el tiempo que necesite un atacante malicioso para romper la seguridad de un sistema, siempre será posible (dado que también serán más potentes las máquinas de cifrado) aumentar el tamaño de las claves, lo que conlleva un aumento exponencial en la dificultad de su rotura. Es decir, en este cuento del ratón y gato, siempre gana el ratón. Al menos en los escenarios que aquí nos interesan.

REFERENCIAS

- [1] Castells, M. *The information Age. Economic, Society and Culture*. Vol I, II & III. Oxford. Blackwell Publishers, 1996-1997.
- [2] Carracedo, J. and Carracedo, J.D. *Use of Security Protocols for Privacy and Anonymity Protection in the Internet Communications*. En *Exploring Cyber Society*, Armitage, J.& Roberts J., Editors. University of Northumbria at Newcastle Press, 1999
- [3] Carracedo Gallardo, J.A. y Carracedo Verde, J.D. *Telemática y Sociología. Apuntes para una Investigación Multidisciplinar: Tarjetas de Crédito Anónimas y Democracia Electrónica*. Libro de Actas del I Congreso Iberoamericano de Telemática, Cartagena de Indias, Colombia, Agosto de 2001.
- [4] ISO/IEC JTC/SC 21. *OSI Reference Model. Part 2: Security Architecture*, 1992
- [5] 18915 REAL DECRETO-LEY 14/1999 de 17 de septiembre, sobre firma digital
- [6] Carracedo, JD. *Attempting to understand the 'Digital Divide'*. Civic Collaborative Center. University of California, San Diego. June, 2000
- [7] Diffie, W y Landau, S.(1998). *Privacy on the Line. The politics of wiretapping and Encryption*, MIT Press,1998.