

Telemática y Sociología. Apuntes para una Investigación Multidisciplinar: Tarjetas de Crédito Anónimas y Democracia Electrónica.

Justo A. Carracedo Gallardo, *Departamento de Ingeniería y Arquitecturas Telemáticas (DIATEL), Universidad Politécnica de Madrid*; Jose-David Carracedo Verde, *Departamento de Ciencias Políticas y de la Administración III, Universidad Complutense de Madrid.*

Resumen-- Se parte de la idea de que para el desarrollo de sistemas telemáticos avanzados concebidos para satisfacer determinadas necesidades de los ciudadanos, tendrán que tenerse en cuenta tanto los requisitos *técnicos* como los *sociales* y se propone el trabajo conjunto de equipos *multidisciplinares* que abarquen ambos campos de conocimiento. Se pretende resumir las principales características de la *Estratificación Digital (digital divide)* generada por la instalación masiva de los sistemas telemáticos y se describe el *servicio de anonimato* necesario para la implantación de la aquí llamada *seguridad cívica*, necesaria para el desarrollo ecuaníime de la *Democracia Electrónica*. Por último, se presentan dos casos de estudio referidos a dos experiencias de aplicación práctica de estos conceptos, abordadas conforme a la *metodología multidisciplinar* antes descrita: las *Tarjetas de Crédito Anónimas* y el *Voto Electrónico*

Palabras clave— Anonimato, Democracia Electrónica, Estratificación Digital, Privacidad, Seguridad Cívica, Tarjetas de Crédito Anónimas, Tarjetas Inteligentes, Voto Electrónico.

I. INTRODUCCIÓN. TRES CONSIDERACIONES DE PARTIDA.

A. Los sistemas “bien” desarrollados y que no sirven.

No merece la pena desarrollar un sistema telemático técnicamente perfecto que incluya innovaciones notables y use las más avanzadas técnicas, si el entorno social al que va dirigido, es decir, los ciudadanos para los cuales ha sido concebido, no confían en él o no responde a sus necesidades reales. Será necesario, para un diseño global adecuado, tener en cuenta los requisitos tanto técnicos como sociales. Por tanto, en el desarrollo actual de las aplicaciones telemáticas, se considera imprescindible que al mismo tiempo que se realiza los trabajos de ingeniería correspondientes, se hagan análisis sociológicos para determinar la viabilidad de los sistemas.

La incorporación de servicios de seguridad en las redes telemáticas ha de servir, al menos, para garantizar que los derechos y salvaguardas actualmente reconocidos en las comunicaciones convencionales, sean respetados también en la proyección y plasmación que éstos tienen en las Comunicaciones Mediante Computadores (CMC). Pero siendo esto necesario, no es suficiente: Mediante una adecuada utilización de los servicios de seguridad en redes los ciudadanos podrían disponer de herramientas que les

permitiesen alcanzar niveles de independencia y privacidad como jamás antes en la Historia se le habían presentado. Al entorno configurado conforme a esta perspectiva es lo que denotamos como *Seguridad Cívica*, acepción que ampliaremos más adelante.

B. Telemática y Sociología: Tomar en cuenta a los ciudadanos.

En los últimos años se ha producido un cambio tecnológico que ha tenido en las llamadas Tecnologías de la Información y las Comunicaciones (TIC), uno de sus más claros exponentes. En concreto, ha sido espectacular el aumento de las CMC. El uso del ordenador tiene un crecimiento exponencial y su penetración prosigue extendiéndose cada vez a más esferas sociales, ya sean relacionadas con el mundo laboral o con el tiempo de ocio [1].

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” [2]. Los estudios relacionados con la Sociedad Red, pretenden analizar el impacto social de este cambio y su potencial de transformación. Para cumplir adecuadamente con este objetivo, proponemos utilizar una perspectiva multidisciplinar que sea capaz de tomar en consideración diferentes enfoques científicos.

Por todo ello, consideramos que resulta necesario que investigadores pertenecientes al ámbito de las TIC, tanto en el campo de la ingeniería telemática, como en el campo sociopolítico, trabajen de forma conjunta. Y ello no sólo para estudiar estos fenómenos desde una doble perspectiva [3], sino también para aprovechar la sinergia generada por la combinación de estas dos perspectivas [4].

C. Democracia, voto electrónico y tarjetas de crédito anónimas.

Los autores de la presente ponencia se encuentran comprometidos en una línea de investigación que pretende la indagación, desarrollo e implementación de sistemas que contribuyan a la mejora de los derechos ciudadanos y

minimicen los efectos negativos que pueden tener sobre ellos la implantación de la Sociedad de la Información. Estos sistemas se apoyan en las ventajas proporcionadas por los servicios telemáticos de seguridad avanzados y los requisitos de usuario detectados mediante análisis sociológicos.

Esta línea de investigación actualmente se centra en dos campos. Por una parte, el desarrollo de sistemas de *votación* y *participación* de los ciudadanos en la gestión política de sus propias vidas, apoyándose en modelos de Democracia Electrónica. El otro campo está enmarcado en el estudio y promoción del uso de Tarjetas de Crédito Anónimas, ACT (en inglés, Anonymous Credit Cards), que eviten la extensión de las capacidades de vigilancia, monitorización y rastreabilidad de las rutinas diarias, inherentes al uso masivo de las actuales tarjetas de crédito.

Postulamos, como punto de partida, que la introducción de las TIC en la vida política, económica y social **permite** expandir la democracia (en su sentido estricto de *gobierno del pueblo*) a ambitos y posibilidades anteriormente vedados.

II. ESTRATIFICACIÓN DIGITAL (*DIGITAL DIVIDE*). POR UN DESARROLLO SOCIALMENTE ECUÁNIME DE LOS SISTEMAS TELEMÁTICOS.

Una problemática socio-política generada directamente por la implantación masiva de servicios telemáticos es lo que denominamos **Estratificación Digital** (en inglés *Digital Divide*). Se centra en el estudio de los discursos y prácticas asociadas con las desigualdades y diferencias en el acceso a computadores, infraestructura de entrada a la red y adquisición de conocimientos, que se dan entre las distintas clases sociales, así como por etnia, género, nivel educativo, convicciones políticas o religiosas, etc.

La mayoría de los estudios a este respecto son de origen norteamericano. El nombre bajo el cual se conoce este campo de estudios es Digital Divide. Este término es ya centro de una fuerte polémica en cuanto su falta de precisión: es vago y no abarca la complejidad del problema. En español, ha empezado a traducirse como “brecha digital”, denominación que mantiene las limitaciones y carencias del término inglés. A nuestro juicio, el término *estratificación* aquí propuesto refleja más claramente la multiplicidad de factores y su jerarquización social.

Precisamente, en la problemática de la Estratificación Digital se percibe netamente la dependencia entre Telemática y Sociedad. El desarrollo de la Sociedad Red, está condicionado por las tecnologías que se apliquen, y las líneas de investigación tecnológicas abren y cierran puertas a posibles escenarios sociales. La mayor parte de las veces, estas actuaciones se producen sin motivación consciente y sin percatarse de sus posibles implicaciones. No de forma automática todo avance tecnológico conlleva un avance

socialmente positivo. Al igual que se hacen estudios de *impacto medio-ambiental*, proponemos que se tenga en consideración el *impacto social* de la implantación de las innovaciones tecnológicas y se analicen las perspectivas que promueven o vedan.

Se presenta en este apartado un resumen de los puntos técnicos y sociales en los que debiéramos concentrar nuestra atención a la hora de intentar construir una Sociedad Red de pleno acceso para todos y con las mismas oportunidades [5]. De forma inherente al desarrollo de la *Democracia Electrónica*, y para que esta sea **universal**, han de solucionarse los problemas que conlleva la *Estratificación Digital*.

Evidentemente, la conceptualización de ésta difiere en su enfoque y características dependiendo de las zonas que se consideren. Obviamente, las situaciones en los EE.UU., Europa o Latinoamérica contienen diferencias de fondo que deben de ser tenidas en cuenta en las soluciones propuestas. La construcción de una Sociedad Red igualitaria está íntimamente ligada a las problemáticas socioeconómicas que se dan actualmente en nuestras sociedades.

Podríamos establecer cinco puntos o categorías de análisis para entender, comprender y poder corregir las diversas facetas de la *Estratificación Digital*.

1. En primer lugar, cabe fijarse en el **equipamiento** o **hardware**. Es decir, el ordenador y sus accesorios, por ejemplo el módem. Resulta obvio que dependiendo del tipo de ordenador, memoria, velocidad y equipo accesorio, se tendrán diferentes posibilidades de rentabilizar los recursos que ofrece la Red.

2. La **Infraestructura de Acceso**. En este punto, en apariencia meramente técnico, es posible identificar diversos proyectos políticos y económicos que condicionan las posibilidades “socio-digitales”. Mitchell plantea: “conectarse a una nueva clase de utilidad plantea un problema obvio. Como con el agua, el gas o la electricidad, las comunidades de bajos ingresos necesitan conseguir tuberías –en este caso, tuberías electrónicas para la información digital- para conectarse a puntos de distribución potencialmente importantes”[6].

Así, en el término *infraestructura de acceso*, englobamos dos aspectos: por una parte, la **calidad** de estas “tuberías” digitales, y por otra, su **topología** o **diseño**. En cuanto a la *calidad* hemos de distinguir, la velocidad de acceso, el “caudal” (throughput) que permite, el grado de protección (privacidad de las comunicaciones), el modelo de “tuberías” que conectan con el servidor (línea telefónica, ADSL, satélite, cable óptico, etc.), y la disponibilidad o capacidad del servidor (tanto horaria, como en lo que se refiere a sus posibilidades para hacer frente a una concurrencia masiva).

En cuanto al *diseño de su estructura*, nosotros abogamos porque ésta debiera de huir del **modelo de difusión** (un emisor productor del contenido, y varios receptores casi sin capacidad de decisión sobre la información recibida). Según Mitchell “las conexiones debieran de ser de dos sentidos, y simétricas [...]. Conexiones de dos sentidos asimétricas, como aquellas establecidas por las televisiones por cable, permiten que grandes cantidades de información fluyan en una dirección pero tan solo permiten que una pequeña cantidad fluya de vuelta. Conexiones de dos direcciones simétricas, como las que se dan en la línea telefónica, permite intercambios de información desde posiciones iguales: esta es una importante dimensión de equidad en el mundo digital” [6].

3. Conectividad a la Red. Hace referencia a dos aspectos. Uno es el relativo a los costes y el otro a la garantía de permanencia en el tiempo de la conexión pactada. En el primer aspecto, la conectividad tiene unas cuotas de acceso: desde la mera tarifa de conexión telefónica hasta el precio que muchos servidores cobran por proporcionar acceso. La tendencia indica que buenas calidades de conexión conllevan tarifas elevadas en el mercado. Dependiendo de cuanto se esté dispuesto a pagar, se podrá tener acceso a mejores y más rápidos servidores.

El segundo aspecto esta también ligado a lo pecuniario, pero más orientado hacia lo que se ha venido en denominar **ciberderechos**. En la conectividad a Internet se obtiene una puerta de entrada a la Red. Ese acceso, permite tanto explorar la red como ser localizado en ella; es decir, tener una localización virtual, ya sea una dirección de correo electrónico o una página Web. Es razonable pedir ciertas garantías de la permanencia en el tiempo de esta ubicación virtual. Actualmente, este ciberderecho, se ve amenazado, al menos, en tres aspectos. Para aquellos que utilicen servidores privados gratuitos, estos podrían unilateralmente cambiar su carácter y exigir una cuota de pago. Para aquellos que pagan cuota, ésta puede ser alterada en función de criterios de rentabilidad y mercado. Por ultimo, también puede darse que los contenidos de una página web incomoden a algún poder, y este pueda presionar (lobby) al servidor y obligarle a rescindir el acuerdo y a descolgar la página web en cuestión.

4. Disponibilidad de la Información. Acerca de Internet, una de las suposiciones de origen que aparecen más frecuentemente, es considerar que toda la información está disponible para todo el mundo. No obstante, en la red se puede observar un creciente proceso de restricciones en el acceso a la información. Este proceso está relacionado con el desplazamiento de Internet desde tendencias sin ánimo de lucro, hacia la creciente comercialización que sufre hoy en día [7]. Son muchas las Páginas Web que piden al usuario un pago previo al acceso a la información. Esto implica desventajas para las clases populares. De forma similar, en muchas páginas Web comerciales, el acceso a la información es gratuito pero se requiere un número de

tarjeta de crédito para acceder al contenido. Así, aquellos sectores de la población que carecen de tarjeta de crédito quedan imposibilitados para acceder a estas páginas. Internet, definida por muchos como un nuevo mundo, con nuevas reglas, libre de las constricciones del mundo material, va imitando de forma creciente las reglas y características del mundo “real”.

5. Objetivos y formas de aprendizaje. Se trata de analizar un aspecto frecuentemente olvidado o relegado al hablar de Estratificación Digital: la determinación de qué objetivos y qué fines se persiguen con los proyectos de desarrollo de la Sociedad de la Información, es decir, para qué se quieren los computadores. Estos objetivos y posibilidades, se encuentran en gran medida determinados por los programas que se enseñan a manejar y la forma en que son usados.

Por desgracia, con demasiada frecuencia, cuando se trazan estrategias para favorecer el desarrollo de la Sociedad de la Información, y establecer puentes para salvar la supuesta “brecha” que separa de ella a muchos ciudadanos, sólo se plantea la compra y distribución masiva de ordenadores, y la impartición de cursos convencionales de manejo de herramientas del oligopolio Microsoft. Por contra, hay proyectos que parten de las necesidades de las comunidades que van a utilizar las redes y en base a ellas, diseñan programas que, además, tienden a ser abiertos (permiten la extensión y particularización de funcionalidades). En este punto podemos distinguir dos modelos básicos:

5.1. Planteamiento Bloqueado o Cerrado. Es aquel software que se sitúa bajo el *modelo de difusión* y que generalmente no permite al usuario crear sus propias aplicaciones. Este software esta diseñado por empresas que generalmente producen en función de lo que creen apropiado y rentable. Los usuarios han de elegir entre aquello que está disponible, se ajuste o no a sus necesidades reales. En cuanto al aprendizaje, actualmente, en la mayoría del mundo, aprender a manejar un computador se traduce en aprender a desenvolverse en el sistema operativo Windows y sus aplicaciones, así como las sucesivas actualizaciones de las mismas. Desde ésta perspectiva, se concibe a las comunidades más como clientes o consumidores que actúan como estudiantes pasivos, que como posibles productores activos de información.

5.2. Planteamiento Expansivo. Aquí incluiremos el conjunto de prácticas y software diseñado de acuerdo con las demandas específicas de las comunidades. Así, los grupos de vecinos debieran de definir sus demandas sociales y materiales. A partir de estas peticiones se analizaría la forma en que la telemática pudiera ayudar, aplicando o incluso creando los programas requeridos para alcanzar los objetivos propuestos. La diferencia inicial con lo descrito en el epígrafe anterior radica en el proceso de diseño de los programas y en **quién** determina los objetivos perseguidos. Otra diferencia estriba en la forma en que se enseñan y como se aplica y desarrolla este conocimiento. Estos programas están pensados para que la comunidad

usuaria, tras una pequeña fase de entrenamiento, sea capaz de generar sus propias aplicaciones y hacerlas funcionar. La idea es que el grupo aplique los programas, y si es posible, sea pronto reconstruido, en función de nuevas necesidades. De esta manera, el software está diseñado en una forma que permite su expansión. A un nivel local, existe la experiencia en comunidades de New Jersey, con programas base como el MUSIC (Multi-User Sessions In Community)[8]. A nivel global, existen iniciativas para la generación libre de sistemas software (LINUX, GNU, etc.), que carecen de patentes de uso y son construidos de forma colectiva por el conjunto de usuarios.

Como corolario de este apartado y su clasificación de cinco puntos, cabe decir que la amplísima problemática relacionada con la Estratificación Digital no queda aquí en absoluto cubierta: tan sólo dibujan un marco de partida desde el cual poder empezar a investigar. Decíamos al principio de este punto que elegíamos el término Estratificación Digital frente al de “brecha digital” porque refleja más claramente la multiplicidad de factores involucrados y su jerarquización social. De hecho, creemos que la forma de estudiar esta temática, lejos de ser binaria (cada lado de la brecha y un “puente” como solución) debiera de ser de múltiples variables. No hay una brecha, sino muchas; superpuestas y solapadas, y por tanto no necesitamos un puente, sino muchos.

Así, creemos que la Estratificación Digital tiene que ser conceptualizada a modo de función multivariable, donde los parámetros serían los cinco puntos anteriores. Y algunas de las variables serían conceptos tales como *democracia, clase social, pobreza, privacidad, trabajo, género, etnia, nivel de educación, Sociedad de la Información, ciberespacio y ciberderechos*.

III. UN NUEVO SERVICIO DE SEGURIDAD QUE REFUERZA Y EXTIENDE LAS POSIBILIDADES DE LA DEMOCRACIA: ANONIMATO

Para hacer frente a los *ataques* que puedan presentarse, en la norma ISO 7498-Part 2, *Security Architecture* [9] se definen cinco servicios básicos de seguridad:

- *Servicio de Autenticación (Authentication)*. También denominado de *Autenticación* (ambas palabras son perfectamente válidas en español), este servicio garantiza que una entidad comunicante *es quien dice ser*.

Podrían distinguirse en este servicio dos calidades, una de las cuales sería la *Autenticación débil* y estaría apoyada en el uso más o menos sofisticado de palabras de paso (*passwords*) o de identificadores, mientras que cuando el resultado es más eficaz la denominamos **Autenticación Fuerte** (*Strong Authentication*), que requiere del intercambio de mensajes cifrados y, posiblemente, del concurso de una Tercera Parte de Confianza, **TTP** (*Trusted Third Party*). Las TTPs son agentes especializados que intervienen en las comunicaciones seguras.

- *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.

- *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. Cuando el Servicio de Integridad es ofrecido, el receptor de la información (o el proveedor del servicio) detectará si se han producido alteraciones en los datos enviados por el emisor.

- *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. Podríamos distinguir tres situaciones:

a) *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.

b) *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.

c) *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.

- *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. De hecho, no existe un conjunto de mecanismos de seguridad claramente definidos para cubrir este supuesto servicio, relación que sí puede determinarse para todos y cada uno de los restantes servicios.

Lo que sí que consideramos, es que debe existir un nuevo servicio de seguridad en las redes telemáticas: el servicio de **Anonimato** (*Anonymity*). En efecto, en la vida real hay situaciones en las cuales es conveniente y necesario mantener oculta la identidad de la persona que protagoniza una determinada acción. Por ejemplo en situaciones como el ejercicio del voto, el anonimato es un derecho.

Veamos varios casos sencillos 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.

Otro caso interesante es el del dinero electrónico. Es latoso tener que llevar dinero en los bolsillos, pero tiene una enorme ventaja: podemos comprar de forma anónima. 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.

En la discusión sobre servicios de anonimato, un caso particularmente interesante es el del **voto electrónico**. Sin duda acabará imponiéndose a medida que se extienda el uso de las redes telemáticas: tendría múltiples ventajas. En la proyección electrónica del esquema convencional, habría 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 opción. Además, el votante debe de disponer de mecanismos que le permitan comprobar que su voto ha sido contabilizado adecuadamente en la opción que eligió. No obstante, las posibilidades de los sistemas telemáticos permiten diseñar o idear otros esquemas de votación, consulta y participación que superan en mucho los modelos convencionales actuales.

Por lo general, para proveer el servicio de anonimato se necesitan Agentes Telemáticos especializados (TTPs) y la utilización de mecanismos criptográficos avanzados (firma ciega, secreto compartido, secreto dividido, etc.) algo más complejos que los que se requieren para la provisión de los servicios básicos.

IV. PROTECCIÓN DE LAS COMUNICACIONES HABITUALES DE LOS CIUDADANOS: LA SEGURIDAD CÍVICA.

Sin pretender hacer una definición rigurosa y precisa, podríamos decir que lo que aquí se entiende por **seguridad cívica** es el conjunto de mecanismos, protocolos, servicios, políticas de seguridad, reglas de comportamiento, análisis de riesgo 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.

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, podemos afirmar 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 electrónica, o, desde otra perspectiva, proporcionando mecanismos que pueden contribuir a solventar diversos problemas relacionados con las desventajas y amenazas de la estratificación digital. Una ciudadanía capaz de usar y demandar plenamente sus ciberderechos, tan solo puede dar lugar a una sociedad más justa y democrática.

El tipo de intercambios que pueden presentarse entre ciudadanos, exige un nivel de protección o confianza en los sistemas que ha de ser proporcional al *bien* o *valor* que se intenta proteger. Multitud de ciudadanas y ciudadanos podrían demandar sistemas de seguridad que le permitiesen algunas de estas actividades:

- (1) Comunicarse con amigos fuera del alcance de miradas indiscretas (básicamente, solo un servicio de confidencialidad es necesario);
- (2) escribir a un o a una amante sin el conocimiento de su pareja (los servicios de autenticación y confidencialidad deberían proveerse);
- (3) consultar el balance de una cuenta bancaria o un registro personal contenido en la base de datos de una agencia gubernamental (sería necesaria la autenticación de usuario y un adecuado control de acceso);
- (4) realizar operaciones bancarias convencionales y ordenar transferencias de fondos en conexión con su oficina bancaria, a salvo de la curiosidad o intromisión

de posibles ladrones u otras agencias financieras (el usuario ha de estar seguro de que la otra parte de la comunicación es realmente su banco y no otra entidad maliciosa, por lo que necesita servicios de autenticación mutua, confidencialidad, integridad y no-repudio);

- (5) realizar gestiones administrativas con las administraciones públicas, obteniendo pruebas, demostrables posteriormente, de que dichos trámites han sido llevados a cabo y la administración en cuestión no pueda negar su tramitación (serían requeridos los mismos servicios que en el caso anterior);
- (6) realizar compras a través de la red obteniendo determinados bienes a cambio de una cantidad de dinero deducible de una cuenta bancaria o a través de otro procedimiento de dinero electrónico (además de confidencialidad, integridad y no-repudio, debería poderse asegurar el anonimato del comprador para evitar que puedan confeccionarse listas que relacionen su nombre con todos los productos que compra y con el dinero que en esas operaciones se gasta, por lo que los procesos de autenticación deberán regularse separadamente para conseguir este objetivo), o
- (7) participar en procesos de reflexión y/o toma de decisiones que afecten a su vida diaria, ya sea en un entorno local o a niveles más amplios. Este tipo de actividades incluye, y va más allá, de la emisión de voto, ya sea en referendos o en elección de representantes (dada la multiplicidad de operaciones que es necesario llevar a cabo, se demandan los cinco servicios básicos, más el de anonimato).

El término *seguridad cívica* se propone aquí en contraposición con otros requisitos, tanto para los algoritmos como para los procedimientos de trabajo, que pueden darse en ámbitos militares o de espionaje o de cualquier otro entorno cerrado, y en los que los bienes o valores puestos en juego puedan ser muy elevados y, por supuesto, muy diferentes a los que se manejan en la vida ordinaria. Por ello, aunque en los ejemplos que antes se han enumerado sólo aparecen actividades que tienen como protagonistas a usuarios finales, también entrarían dentro de esta categoría las transacciones que se realicen entre empresas o las comunicaciones que se efectúen entre los distintos departamentos de una de ellas.

En este contexto, 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 [10], “*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.

Es posible, y bastante probable, que las agencias gubernamentales de inteligencia puedan estar en posesión de potentísimas máquinas y evolucionadísimas técnicas de descifrado 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 las comunicaciones.

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.

Por ello, a pesar de su vaguedad, esta lúcida propuesta de Diffie resulta esclarecedora para hacerse una idea del tipo de cosas con que han de lidiar los **ingenieros** que se dediquen al diseño, implementación y puesta a punto de sistemas que garanticen, para usos civiles, la seguridad y **privacidad** en las redes telemáticas.

En algunas publicaciones en español 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.

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. Naturalmente, para que esta privacidad del ciudadano sea garantizada, es necesario también que tanto los bancos como las oficinas de las Administraciones Públicas a que se ha hecho referencia en los ejemplos anteriores no hagan posteriormente un uso indebido de los registros obtenidos; pero esa exigencia, que en muchos países es objeto de regulación legislativa, no es planteable solamente para el caso de las redes, sino que aparece en igual medida en las operaciones convencionales.

V. CASO DE ESTUDIO. TARJETAS DE CRÉDITO ANÓNIMAS.

En un mundo globalizado, subsumido en la Sociedad de la Información, el uso de dinero en metálico resulta a veces incómodo y sujeto a múltiples limitaciones. No obstante, es necesario resaltar que el dinero en metálico es un viejo mecanismo que permite mantener el anonimato del comprador. El vendedor tiene una garantía razonable de que el comprador está en posesión de un recurso que le permite llevar a cabo una determinada transacción comercial, siendo habitualmente desconocida la identidad del cliente. El banco puede conservar un registro de todas las cantidades de dinero que hemos sacado de la cuenta corriente, pero no puede saber en qué hemos gastado ese dinero.

El uso masivo de tarjetas de crédito ha alertado a amplios sectores de la sociedad y atraído la atención de muchos investigadores sociales, ya que está siendo sumamente pernicioso para la conservación de la privacidad. De hecho, ha sido “el instrumento a través del cual se han establecido perfiles sobre las vidas de las personas, se han analizado y utilizado para fines comerciales” [2].

Por otra parte, es relativamente fácil falsificar la autenticación que le es exigida al usuario cuando éste accede a un cajero automático o a una máquina de pago ubicada en un punto de venta. Cuando las tarjetas de crédito son usadas para adquirir bienes a través del teléfono o de Internet, el simple conocimiento del número de la tarjeta y de su fecha de caducidad suelen ser suficientes para llevar a cabo la operación. Otras veces, el mecanismo de “autenticación” se “refina” y se exige un fax firmado. Obviamente, todos estos mecanismos resultan manifiestamente insuficientes para garantizar que el comprador es realmente el titular de la tarjeta. La estadística sobre el número de fraudes y deficiencias que se producen es mal conocida porque son precisamente las entidades bancarias emisoras de estas tarjetas las primeras interesadas en no informar acerca de la inseguridad de un producto financiero que, a juzgar por la insistencia con que nos lo ofertan, es de gran valor para sus intereses.

Otra característica sumamente perniciosa de las tarjetas de crédito la constituye el hecho de que el banco conoce el PIN del usuario y pueden aparecer problemas cuando un comprador rechaza o niega haber realizado una cierta compra. El banco puede aducir que esa transacción fue

realizada usando la identificación personal del usuario, pero éste puede rechazarla argumentando que el secreto de su PIN no ha sido adecuadamente custodiado, o ha sido interceptado en una comunicación debido a las insuficientes medidas de protección establecidas, o, incluso, que el banco está simulando una falsa operación de compra con fines maliciosos. Todo está confuso y revuelto: nadie tiene pruebas contundentes de nada.

Los problemas derivados de la simple existencia de un PIN y de la falsa imputación de transacciones a que se ha hecho referencia en los párrafos anteriores pueden ser resueltos mediante el uso de *tarjetas inteligentes* dotadas de mecanismos criptográficos asimétricos. En el siguiente apartado se comenta brevemente su estructura y los servicios que ofrecen. No obstante, los principales problemas relacionados con el uso de tarjetas de crédito e identificadores electrónicos son los relacionados con el riesgo que conllevan contra la privacidad y las consecuencias socialmente negativas que ello genera.

A. *Tarjetas de crédito inteligentes.*

Una tarjeta inteligente (*smart card* o *IC*, en inglés) es una tarjeta de plástico de aspecto similar a las tarjetas de crédito convencionales, dotada de un circuito integrado (por eso se las ha llamado también *tarjetas chip*) que contiene una CPU o microprocesador, memoria volátil y memoria no volátil. Esta memoria aloja las pequeñas aplicaciones de usuario y un reducido Sistema Operativo, el SCOS o *Smart Card Operating System*, también denominado *máscara* o *Smart Mask*. Utilizando estos componentes y una circuitería adicional, la tarjeta permite guardar datos particulares de cada usuario y datos para la aplicación específica. Dependiendo de la capacidad de la tarjeta, también se puede almacenar en ella la clave pública, certificada o no, e incluso una serie de informaciones asociadas al entorno en el que se use la tarjeta, haciendo que ésta funcione como memoria *caché* de una aplicación o de una serie de aplicaciones.

La comunicación exterior se realiza a través de unos pequeños contactos físicos del Chip que la ponen en contacto con la **ULE**, *Unidad de Lectura-Escritura*, en inglés, *WRW*, *Writing-Reading Unit* (algunas tarjetas carecen de contactos y la transmisión se realiza mediante radiofrecuencia). La tarjeta puede llevar a cabo un conjunto limitado de funciones criptográficas y una serie de funciones de comunicación con el exterior a través de la ULE. Estos periféricos son muy simples y de bajo coste, de forma que su instalación en los PCs o terminales de usuarios no presentan relevantes problemas técnicos o económicos. Además, existen ULEs que se pueden insertar en la ranura destinada a los disquetes portátiles, con lo cual se reducen aún más los requisitos de equipamiento necesarios. Aunque existen varias generaciones de tarjetas inteligentes que han ido resolviendo sucesivamente distintos problemas de seguridad, las que se proponen para ser usadas como

tarjetas de crédito inteligente están dotadas de mecanismos criptográficos, tanto de clave secreta como de clave pública (tipo RSA). Garantizan el almacenamiento de la *clave privada* del usuario de forma segura, ya que las operaciones de cifrado que deban realizarse usando esta clave se llevarán a cabo **dentro de la tarjeta**, garantizando que la clave nunca viaje por la red, ni salga de los estrictos límites de la tarjeta. También pueden almacenar el *certificado* de su *clave pública* y un número de certificados de otros agentes que intervienen en la comunicación.

Algunas veces, la generación del par de claves de cada usuario (privada y pública) se realiza en un centro especializado y autorizado para ello dentro del dominio de seguridad. En este caso, las claves son introducidas en la tarjeta en la fase de personalización, siendo ésta entregada al usuario para su uso y custodia. En ese momento, el centro generador de claves debe borrar la clave privada del usuario para que sea él, y solo él, quien posea esta clave, responsabilizándose (incluso jurídicamente) de todas las operaciones de cifrado que con ella se realicen. Un problema asociado a este método consiste en que el usuario ha de confiar en que su clave privada ha sido efectivamente borrada, no pudiendo obtener una **prueba** robusta de ello.

Frente a esta forma de proceder, es menester hacer notar que para que se puedan resolver los problemas que tienen las tarjetas de crédito convencionales, se preconiza que cada usuario, una vez recibida una primera versión de su par de claves (privada y pública) esté facultado para **generar un nuevo par de claves**, almacenando por sus propios medios la clave privada en su tarjeta inteligente y haciendo llegar la clave pública a una Autoridad de Certificación para que genere el correspondiente de certificado. De esta manera, es insoslayable la responsabilidad que el usuario contrae en cuanto al uso y custodia de sus claves, **no existiendo resquicio alguno** que le permita atribuir a terceros una posible firma que haya sido realizada usando su propia clave privada. De igual forma, esa custodia de su clave privada le proporcionan la seguridad de que nadie, ni siquiera el banco, podrá imputarle la realización de transacciones que él o ella no hayan llevado a cabo. Algunas tarjetas inteligentes están capacitadas para generar de por sí un nuevo par de claves, con lo que se refuerzan estas salvaguardas de confinación de la clave privada en la tarjeta.

Visa y MasterCard, en colaboración con otras compañías involucradas en temas de seguridad, han propuesto y especificado el SET (*Secure Electronic Transactions*) que es un muy elaborado conjunto de procedimientos y protocolos que regulan la comunicación entre diversas entidades y agentes telemáticos implicados en la obtención de una autorización para realizar una compra. La arquitectura SET permite operaciones de Comercio Electrónico sin necesidad de que el usuario sea poseedor de una tarjeta, pero la configuración que aquí nos interesa es aquella en que los clientes (*cardholders*) constituyen

entidades comunicantes que en el futuro estarán en posesión de una tarjeta de crédito inteligente a través de la cual podrán realizar operaciones firmadas digitalmente. Gracias al uso de certificados emitidos por diversas CAs, las distintas partes que intervienen en la comunicación adquieren pruebas irrefutables acerca de las transacciones realizadas. La infraestructura de certificación está constituida por un conjunto de Autoridades de Certificación (CAs) organizadas jerárquicamente, que representan a las distintas partes implicadas en la operación de compra: clientes, comerciantes, bancos y entidades financieras emisoras de tarjetas. Aunque la especificación del SET apareció hace ya algunos años, la complejidad de la arquitectura y la multiplicidad de agentes telemáticos que conlleva hace que su implantación esté resultando más lenta de lo previsto.

Las tarjetas inteligentes están dotadas de mecanismos de protección tanto físicos como lógicos. Estos últimos regulan el control de acceso a los datos y a las funciones de la tarjeta. Si una tarjeta es extraviada o le ha sido sustraída a su legítimo propietario, no es técnicamente posible leer los datos en ella contenidos o realizar modificación o copia de éstos. Este tipo de protección física garantiza que aunque la tarjeta sea destruida, no sea posible acceder por medios electrónicos al contenido de la memoria del chip. (Esta propiedad se denomina, en inglés, *tamper-proof*). En cualquier caso, queda aquí abierto un tema importantísimo, como es el método de autenticación de la persona ante su tarjeta (pruebas biométricas) y sus implicaciones sociopolíticas.

B. Implicaciones sociales del uso de las tarjetas de crédito.

Actualmente, en las sociedades modernas observamos un paulatino asentamiento y aplicación de las lógicas de mercado a todos los niveles y, particularmente, en las prácticas de vigilancia. Ya que aparentemente todo es mercado y todo se puede comprar o vender, las prácticas de marketing tienen muy en cuenta la información que pueden aportar unos extensos y exhaustivos sistemas de vigilancia, como son, por ejemplo, aquellos basados en las tarjetas de crédito.

En la constatación de este hecho es donde hay que situar el origen de lo que Oscar Gandy llama el *panoptic sort* (la clasificación, el tipo o la marca, **panóptica**¹). “El *tipo panóptico* es una tecnología de discriminación compleja. Es

¹ **Panóptico**: Sistema arquitectónico en forma de círculo con una torre central cuyas paredes eran celosías, ideado por Bentham en el siglo XVIII y diseñado de forma que unos pocos vigilantes pudieran tener un control absoluto, día y noche, de todas las actividades y tareas de los internos sometidos a vigilancia. Posteriormente, Foucault, filósofo francés del 68, teorizó sobre la aplicación social de esta estructura y actualmente es una conceptualización recurrente en los estudios sobre vigilancia, control social y Sociedad de la Información. Son muchos los autores que teorizan sobre un panóptico electrónico.

panóptica en la medida en que considera **toda** la información sobre el status o conducta individual potencialmente útil para producir elementos de valoración sobre el potencial económico de una persona. Y decimos que es una tecnología discriminatoria porque se usa para clasificar a la gente en categorías construidas sobre estas estimaciones” [11]. Así, el mercado tiene una necesidad de generar evidencias dignas de crédito sobre la identidad de los individuos con los que se pretende hacer negocios. Y aunque en un principio los objetivos de identificación se asociaban a cuestiones de seguridad y protección de intereses, tanto del cliente como del vendedor, actualmente nos encontramos con unos procesos de demanda de identificación que no responden necesariamente a los criterios de seguridad. Por contra, responden al objetivo de aumentar las bases de datos sobre cada consumidor (nombre, dirección, hábitos de consumo, capacidad de endeudamiento, número de teléfono, número de pasaporte, etc.).

En suma, este modelo panóptico abarca no sólo a los sistemas de ordenadores y telecomunicaciones que facilitan la recolección, almacenamiento, procesamiento y comparación de la información personal, sino que también incluye las técnicas de análisis que diferencian, seleccionan objetivos, clasifican y segmentan individuos y grupos sobre las bases de los modelos, suposiciones y orientaciones estratégicas que demandan la optimización del beneficio económico y la minimización del riesgo.

Así, haciendo uso de los **sistemas telemáticos**, se han establecido prácticas cuyos objetivos se centran en *Identificación, clasificación y evaluación*, y en los que los ciudadanos son reducidos a la categoría de potenciales consumidores, y su vida diaria y privada es reducida a una variable que es necesario conocer, clasificar y prever. Actualmente, una de las fuentes principales de las que se extrae esta información son las tarjetas de crédito.

La sustitución de tarjetas de crédito convencionales por tarjetas inteligentes, operando en red, no soluciona en absoluto este problema sino que lo magnifica: el uso masivo de tarjetas para gran cantidad de actividades de la vida diaria representa un peligro tanto más acusado cuanto mayor sea el número de situaciones en las que se utilicen. Frente a esta orientación, la inclusión de servicios de anonimato puede representar un conjuro contra la pesadilla de vigilancia y totalitarismo que algunos investigadores sociales advierten en las tendencias actuales. [12], [13] y [14].

C. Tarjetas con anonimato

El dinero metálico, siempre es anónimo. Por ello, cualquier proyección digital de los mecanismos de pago, debería preservar el anonimato del comprador. Existen muchas propuestas de Comercio Electrónico en las que esta condición no se garantiza, lo cual puede dar lugar, según se

ha comentado, a una situación de control social y vigilancia de masas. Para evitar este tipo de escenarios podemos distinguir al menos ocho características que sirven para catalogar un sistema anónimo de pago usando dinero electrónico:

1. **Verificabilidad** (*verifiability*). Todo participante en una transacción monetaria digital debe de ser capaz de verificar el valor del dinero recibido, la entidad financiera emisora y su autenticidad.
2. **Seguridad** (*security*). El dinero digital no puede ser copiado, o rehusado por el mismo comprador. Tanto el comprador como el vendedor tienen serias dificultades para perpetrar un fraude.
3. **Anonimato** (*anonymity*). La identidad del comprador debe de ser protegida. Esta característica ha sido ampliamente discutida en apartados anteriores.
4. **Irrastreabilidad** (*untraceability*). Nadie puede rastrear o detectar la relación entre el consumidor y los bienes adquiridos.
5. **Pago sin conexión** (*off-line payment*). Los protocolos de venta se llevan a cabo entre el consumidor y el comerciante sin necesidad de que el punto de compra establezca una conexión directa con cualquier banco o agencia financiera.
6. **Transferibilidad** (*transferability*). El dinero recibido puede a su vez ser utilizado por el vendedor para realizar él mismo otras compras o transacciones.
7. **Divisibilidad** (*divisibility*). Quien recibe una cantidad de dinero electrónico esta capacitado para transferir a terceros el total, o solamente una parte.
8. **Devolución de cambio**. Un comprador puede entregar al vendedor una cantidad de dinero superior al valor del bien adquirido y recibir del vendedor una transferencia monetaria correspondiente a la diferencia.

Estas ocho características pueden servir para evaluar las diversas propuestas y alternativas se han venido realizando para abordar esta cuestión. Existen propuestas, claramente insuficientes, que no utilizan mecanismos criptográficos para la implantación de los protocolos. Otras proponen utilizar algoritmos criptográficos clásicos, si bien sus soluciones no proveen servicios de anonimato, cosa que consideramos absolutamente inservible.

Entre las soluciones que sí contemplan el anonimato cabe destacar la propuesta de Chaum y Pedersen [15] sobre dinero electrónico (electronic cash), que plantea un modelo “off-line” que incluye la posibilidad de que las monedas sean transferibles entre varios usuarios antes de que lleguen de nuevo al banco, de forma que el proceso sea irrastreado. Otras propuestas [16] plantean sistemas con distintos grados de anonimato, dependiendo de la autenticación empleada.

Casi no existen referencias dignas de destacar en lo que se refiere a propuestas sobre tarjetas de crédito anónimas, a excepción de la realizada por Low y otros [17], que plantean un modelo en el que participan varios bancos y en

el que no se requiere el uso de mecanismos criptográficos especiales. El cliente mantiene una cuenta en un banco C, en la que se controla el saldo pero no las operaciones y otra cuenta anónima, en otro banco P, donde se identifica al cliente por un seudónimo y sí se recogen las operaciones que realiza. Mediante la interacción de estos bancos a través de una entidad mediadora se consigue el efecto buscado.

Durante los últimos años, los autores de la presente ponencia han estado involucrados en una serie de trabajos exploratorios [18] y [4] sobre las implicaciones sociales y las posibilidades tecnológicas del uso de tarjetas inteligentes para soportar servicios de anonimato. En concreto, se han especificado dos modelos distintos y se han desarrollado demostradores simplificados que permiten evaluar la validez de las soluciones aportadas. En estas propuestas se ha descartado totalmente la característica número 5 (operación off-line) porque, además de complicar enormemente los protocolos, consideramos más interesante los sistemas conectados en red. Cabe observar que en el uso de tarjetas de crédito convencionales los puntos de ventas están mayoritariamente conectados telemáticamente con las entidades bancarias.

Otro elemento arquitectural ha sido el considerar la presencia de un agente telemático en los puntos de venta ante el cual un cliente comparece en persona, portando su tarjeta inteligente. Se ha dejado para futuros trabajos el estudio del acceso remoto a estos puntos de venta vía Internet. Por tratarse de esquemas en los que el cliente se relaciona sólo con el vendedor y con la entidad financiera, la característica número 6 (transferibilidad) no se ha tenido en cuenta, excepto en la operación mediante la cual el vendedor recibe el importe del bien o servicio que ha cedido. En cuanto, a las características 7 y 8 (divisibilidad y devolución de cambio) son usadas más bien como mecanismos de astucia para ocultar operaciones y dificultar la **datavigilancia**, antes que como emulaciones digitales de la devolución de cambio del dinero en metálico. Así una sola operación de compra puede ser enmascarada bajo varias transacciones entre la tarjeta y el punto de venta, dificultando su rastreabilidad.

VI. ABORDANDO LA VOTACIÓN ELECTRÓNICA.

Ya se ha discutido en apartados anteriores la importancia de la utilización de la telemática en la edificación de una Sociedad de la Información que supere las desigualdades y a cuyas ventajas tengan acceso, de igual forma, la totalidad de las personas que constituyen la sociedad. Para una Democracia Electrónica universal es básico la construcción de estructuras telemáticas que posibiliten el voto electrónico en su doble acepción de votación y de participación de los ciudadanos. La primera, a imitación de la filosofía de los esquemas de votación construidos en los últimos siglos, consistente en la elección de representantes, o en la decisión sobre alternativas previamente planteadas. La segunda, consiste en dar apoyo a modelos en los cuales los miembros de una comunidad estén capacitados para proponer, discutir

y **consensuar** alternativas sobre la gestión y organización de los recursos que les son comunes (ya sean económicos, políticos, culturales, de ocio, etc.).

Existen una serie de aspectos básicos relativos a la seguridad del proceso de votación, presentes en los procesos convencionales, que habría que tener en cuenta para el desarrollo de un sistema de votación electrónica:

Autenticación: sólo los votantes autorizados pueden votar. Hay que resaltar que, en principio, consideramos aquí el concepto de *voto* y *votante* en sentido amplio, válido también para aquellos escenarios en los que un voto puede ser una opinión o una propuesta.

Fiabilidad: no se puede producir ninguna alteración fraudulenta de los resultados de la votación.

Veracidad de la votación, de manera que si se descubre algún defecto en la publicación de los resultados, existan mecanismos para probar el fraude. Esta característica se puede considerar como una prueba global de la fiabilidad.

Anonimato: no se puede relacionar un voto con el votante que lo ha emitido.

Imposibilidad de coacción: ningún votante debe ser capaz de demostrar qué voto ha emitido. De esta forma se impide la compra masiva de votos y la presión sobre los votantes, ya que la persona que desea influir sobre otra u otras no tiene garantía del resultado de su acción.

Verificación individual: cada votante deberá poder asegurarse de que su voto ha sido considerado adecuadamente, de forma que el votante pueda obtener una prueba palpable de este hecho.

Imparcialidad: todos los votos deben permanecer en secreto mientras no finalice el tiempo de la elección. De este modo, los resultados parciales no afectarán a la decisión de los votantes que no han depositado su voto todavía.

Evidentemente estas características responden a las concepciones vigentes de votación. A la hora de diseñar nuevos esquemas de soporte telemáticos, una tarea de partida fundamental consistiría en definir los distintos dominios o ámbitos de aplicación del sistema, y el análisis y diseño de los esquemas de votación y participación que serían demandados.

El proyecto VOTESCRIPT.

Paralelamente a los estudios sobre la aplicación de los servicios de anonimato a las tarjetas de crédito, los autores han venido abordando el estudio de los sistemas de votación electrónica. Como consecuencia de ello, han tomado diversas iniciativas siendo una de ellas la participación en la promoción de un proyecto de investigación subvencionado dentro del Plan Nacional de I+D+I :*Votación Electrónica Segura basada en criptografía avanzada, VOTESCRIPT* (código TIC 2000-1630-C01). Este proyecto ha dado comienzo en Enero del presente año, de tal forma que, a la

hora de redactar el presente texto, se encuentra en su estado inicial.

De forma resumida, el objetivo del proyecto es el análisis, definición e implementación de un sistema capaz de soportar los diferentes pasos y elementos existentes en un proceso de votación electrónica: emisión y recuento automático de votos y opiniones.

Se espera conseguir que el sistema garantice la autenticidad de los participantes, asegurando que sólo las personas autorizadas puedan contribuir, al tiempo que salvaguardará su anonimato de manera que no sea posible conocer la identidad de los votantes que se han decantado por cada opción. Para poder ofrecer estas facilidades se emplearán mecanismos criptográficos avanzados, tarjetas inteligentes de nueva configuración y se desarrollarán terceras partes de confianza (TTPs) especializadas.

Para alcanzar estos objetivos, el desarrollo del proyecto se ha abordado mediante un equipo interdisciplinar. Está dividido en dos subproyectos coordinados: Uno con sede en el Departamento de Ingeniería y Arquitecturas Telemáticas, DIATEL (Universidad Politécnica de Madrid) y el otro en el Departamento de Ciencia Política y de la Administración III (Universidad Complutense de Madrid). La coordinación de los trabajos se llevará de forma que la elección de la arquitectura del sistema se realizará teniendo en cuenta las posibilidades tecnológicas y los condicionantes jurídicos y sociales que determinen su aceptación por el ciudadano y el adecuado respeto de los derechos democráticos.

VII. BIBLIOGRAFÍA.

- [1] Kubicek, H; Duton, W. & Williams R. *The Social Shaping of Information Superhighways*. Frankfurt-, Campus Verlag, 1997.
- [2] Castells, M. *The information Age. Economic, Society and Culture*. Vol I, II & III. Oxford. Blackwell Publishers, 1996-1997.
- [3] Agre, P. E. and Rotenberg M., Editors. *Tecnology and Privacy: The New Landscape*. The MIT Press. Cambridge, Massachuset, EEUU, 1998.
- [4] 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
- [5] Carracedo, JD. *Attempting to understand the 'Digital Divide'*. Civic Collaborative Center. University of California, San Diego. June, 2000
- [6] Mitchell, W. *The question of Access*, in Schon, D; Sanyal, B. & Mitchell, W. (eds). *High Technology and Low-Income Communities. Prospects for the Positive Use of Technology*. Cambridge, MIT Press, 1999.
- [7] Kahin, B & Keller J. (1995). *Public access to the Internet*. London, MIT Press.,1995
- [8] Shaw, A & Shaw, M. *Social Empowerment through Community Network*, in Schon, D; Sanyal, B. & Mitchell, W. (eds). *High Technology and Low-Income Communities. Prospects for the Positive Use of Technology*. Cambridge, MIT Press, 1999.
- [9] ISO/IEC JTC/SC 21. *OSI Reference Model. Part 2: Security Architecture*, 1992
- [10] Diffie, W y Landau, S.(1998). *Privacy on the Line. The politics of wiretapping and Encryption*, MIT Press,1998
- [11] Gandy, Oscar, 'Coming to terms with the panopticon sort. In *Surveillance, Computers and Privacy*, (ed) Lyon D. y Zureik, E. University of Minnesota Press, 1996.
- [12] Chaum, D. *Security Without Identification. Transaction system to make Big Brother obsolete*. Communication of the ACM, v. 28, n. 10, Oct 1985, pp 1030-44., 1985
- [13] Marx, G. T. (1986) *The iron fist in the velvet glove*. En *The Social Fabric*. Short, J. Sage, 1986. Marx, G.T. *Undercover: Police Surveillance in America*. Berkeley. University of California Press, 1988.
- [14] Lyon, D.. (1994). *The Electronic Eye. The rise of the Surveillance*, Society. Polity, 1994.
- [15] Chaum, D. and Pedersen, T. *Transferred Cash Grows in Size*, CWL, Netherlands, 1993
- [16] Bürk, H. and Pfitzmann, A. *Digital Payment Systems Enabling Security and Unoservability*, Karlsruhe Univerdity, 1989
- [17] Low, SH., Maxemchuck, NF and Paul, S. *Annoymous Credit Cards*, Proceeding of the Second annual ACM Conference on Computer and Communication Security, ACM Press, 1994.
- [18] Carracedo, JD. *To what extent is the scheme of panopticism useful in the age of global electronic communication to make sense of the concepts of power, discourse and surveillance*, En *Exploring Cyber Society*, Armitage, J.& Roberts J., Editors. University of Northumbria at Newcastle Press, 1999