

**Seguridad y
Privacidad para el
Ciudadano en la
Era digital
Posterior al 11 de
Septiembre: una
Visión
Prospectiva**

**Resumen Ejecutivo
Versión española**

Julio 2003



EUROPEAN COMMISSION
DIRECTORATE-GENERAL
Joint Research Centre

Seguridad y privacidad para el ciudadano en la era digital posterior al 11 de septiembre: una visión prospectiva

RESUMEN EJECUTIVO

El presente informe analiza algunas tendencias tecnológicas en auge y explica sus posibles efectos sobre la privacidad y la seguridad del ciudadano.

Las hipótesis del estudio son:

- el equilibrio entre la libertad individual, reflejada en la protección de la privacidad, y la necesidad del Estado de mantener la ley y el orden mediante políticas de seguridad, ha sido construido lentamente en el marco de las sociedades democráticas;
- este equilibrio se está viendo alterado principalmente por dos factores: la implantación de las tecnologías de información y comunicación (TIC), junto a sus aplicaciones comerciales y gubernamentales, y por las respuestas de los gobiernos al aumento en delincuencia y terrorismo. En particular, los trágicos acontecimientos del 11 de septiembre de 2001 marcaron el punto de partida para la adopción de medidas de seguridad, basadas en gran parte en avances tecnológicos.

La influencia de estos dos factores sobre la privacidad, la seguridad y el equilibrio entre ambas es abordado por este informe en el ámbito de tecnologías de identificación en distintos estados de desarrollo y comercialización, tomando tres ejemplos concretos como base del estudio.

El equilibrio entre privacidad y seguridad se está viendo alterado por la implantación de tecnologías de información y comunicación y por las respuestas de los gobiernos al aumento en delincuencia y terrorismo.

El trabajo concluye señalando los desafíos que la tecnología supone para la privacidad y la seguridad identificando aspectos críticos sobre los que habrá que posicionarse políticamente.

1. Bases del informe

Internet fue, durante sus primeros 25 años de existencia, el coto privado de especialistas e investigadores universitarios, que disponían de ella gratuitamente, en gran medida sin riesgos para la integridad de la información y libre de controles o protecciones reglamentarias. Su transición a un medio de comunicación generalizado ha sido reciente, y ha sorprendido al mundo de las telecomunicaciones tradicionales. La rápida comercialización y crecimiento de Internet llevó a una explosión de servicios basados en la información y al uso del correo electrónico como una nueva forma de comunicación escrita.

El atractivo de Internet como un medio global de comunicación e información se hace patente en su número de usuarios, unos 600 millones, y en su utilización para una gama

ilimitada de servicios y aplicaciones que están transformando el modo de vida y trabajo de la población, creando también comunidades *virtuales* en torno a áreas de interés común. Su impacto en la sociedad es comparable, en cuanto a magnitud, al impacto que tuvieron la introducción del teléfono, la radio o la televisión, pero con una velocidad de crecimiento muy superior a la de cualquiera de los tres.

Pero el crecimiento vertiginoso de Internet también creó expectativas desmesuradas, incluyendo la “irracional” era “punto.com” que llevó al estallido de la burbuja bursátil. Entre las razones detonantes, cabe señalar la frustración de los inversores cuando no se produjo el esperado crecimiento del comercio electrónico empujado por el consumo. La creciente preocupación por la fiabilidad, la confianza, la privacidad y la seguridad en el uso tanto de este medio como de los proveedores de servicios en el mismo, se ha considerado como el principal obstáculo para la adopción generalizada del comercio electrónico.

La creciente preocupación por la fiabilidad, la confianza, la privacidad y la seguridad en el uso de Internet es el mayor obstáculo para la adopción generalizada del comercio electrónico.

Los usuarios acceden a Internet a través de una gran variedad de tecnologías de comunicación fijas y móviles y de dispositivos inteligentes, pero las tecnologías de acceso han supuesto hasta ahora un “cuello de botella”, ya que las estructuras tradicionales de mercado y de tarificación han sobrevivido a la liberalización más tiempo que otras partes de la red. Sin embargo, con el tiempo y con nuevas innovaciones, se espera que la diversidad tecnológica se extienda permitiendo mayor movilidad y menor dependencia de dispositivos como teclados o pantallas. Éstos van a ser reemplazados como medios dominantes de acceso a Internet por dispositivos más fáciles de utilizar por el usuario e incorporados de forma invisible en nuestro entorno, con las consecuentes implicaciones en seguridad.

Las tecnologías digitales e Internet se están utilizando, pues, para beneficiar a millones de ciudadanos y empresas. Sin embargo, aunque proporcionan un mayor control sobre los contenidos y los servicios a sus usuarios, pueden tener precisamente el efecto opuesto en cuanto a los mecanismos de seguridad y privacidad subyacentes, que rigen el intercambio de datos. De hecho, cuando se realizan transacciones por Internet, los usuarios toman parte involuntariamente en interacciones que permanecen, en gran medida, fuera de su control.

El creciente uso de interacciones subliminales en la red, cuya finalidad es observar a los usuarios y el uso de Internet, lleva consigo nuevos riesgos y posibles abusos de la privacidad de los datos personales. Gestionar las consecuencias de estos riesgos requiere una comprensión de las posibilidades que ofrecen las tecnologías actuales y futuras, respaldada por un análisis de los factores – beneficios económicos, comodidad, seguridad, privacidad, etc. – que influyen en las interacciones en este nuevo y complejo entorno. Este es un mundo donde la información digital y la información real se entremezclan, y el riesgo, las vulnerabilidades, los actores y los aparatos cambian de un modo dinámico. El papel de la tecnología, como instigadora del cambio y como portadora de soluciones, necesita, pues, definirse mejor. Lo que está en juego, en último término, es el futuro mismo de la Sociedad de la Información en Europa; los ciudadanos no aceptarán los servicios,

posibles gracias a las nuevas tecnologías, a menos que puedan confiar en su utilización tanto como en los actuales servicios del “mundo real”.

El papel de la tecnología como instigadora de cambio y como portadora de soluciones, necesita una mayor definición.

2. El impacto del 11 de septiembre

Los acontecimientos del 11 de septiembre de 2001 conmocionaron al mundo y sacaron a la superficie preocupaciones latentes sobre las amenazas a la seguridad mundial. La respuesta inmediata del gobierno de EEUU fue reforzar la seguridad mediante un conjunto de programas de recogida de información, utilizando sistemas de vigilancia de masas. Se aprobaron por abrumadora mayoría varias medidas legislativas destinadas a ampliar los poderes de las agencias de seguridad de EEUU, para ayudarlas a combatir el terrorismo, y los proyectos que reforzaban las capacidades de control tecnológico de las fuerzas de seguridad de EEUU también recibieron financiación extra.

Tras los acontecimientos del 11 de septiembre, la respuesta inmediata por parte del gobierno de EEUU fue la implantación de sistemas de vigilancia de masas.

La mayoría de los países de la Unión Europea también respondió a los acontecimientos del 11 de septiembre implementando varias medidas operativas y legislativas destinadas a elevar sus niveles de seguridad. Se incrementó la seguridad “en tiempo real” en los puntos de control de las fronteras y se mejoró la coordinación entre la policía y otros servicios. Se tomaron medidas legislativas con el objetivo de reforzar los mecanismos judiciales dentro de los estados miembros y armonizar los procedimientos de las políticas antiterrorismo dentro de ellos. Además, la Unión Europea y EEUU mejoraron su cooperación legal y los mecanismos operativos en las áreas de cumplimiento de la ley y de coordinación de los servicios de inteligencia.

Es importante sin embargo señalar que, aunque el 11 de septiembre ha reforzado la potestad de los estados para tomar con frecuencia medidas de seguridad intrusivas –medidas que antes no se hubiesen tolerado fácilmente– muchos de los cambios aparentes ya se estaban discutiendo con anterioridad a dicha fecha. A este respecto, los acontecimientos del 11 de septiembre pueden considerarse más como la ocasión que como la causa de la introducción de un nuevo paradigma de seguridad. La principal característica del nuevo paradigma es un cambio de los modos de protección de la seguridad de “reactivos” a “activos”, utilizando sistemas basados en las TIC para facilitar la recogida de datos y para compartirlos entre múltiples fuentes, en apoyo de los servicios de inteligencia. Este cambio no hubiera podido llevarse a cabo en tan poco tiempo si no hubiese habido un respaldo público generalizado a las políticas destinadas a incrementar la seguridad de los ciudadanos tras el 11 de septiembre.

Los acontecimientos del 11 de septiembre pueden considerarse más como la ocasión que como la causa de la introducción de un nuevo paradigma de seguridad, cambiando los modos de protección de la seguridad de “reactivos” a “activos”, utilizando sistemas basados en las TIC en apoyo de los servicios de inteligencia.

Las iniciativas de seguridad, así tomadas, también han reforzado los poderes de los gobiernos y de los cuerpos encargados del cumplimiento de la ley, para acceder a los datos personales, para fines que van más allá de aquéllos para los que los datos se suministraron originariamente. De hecho, el acceso normal a muchos servicios comerciales y gubernamentales se condiciona ahora a que el ciudadano suministre datos personales mucho más completos que antes.

Puede haber pocas dudas de que el efecto combinado de las medidas operativas y legislativas descritas ha sido inclinar la balanza seguridad/privacidad a favor de los intereses de seguridad. El hecho de que las medidas se basen principalmente en la aplicación masiva de diferentes tecnologías, lleva a plantear la cuestión de hasta qué punto son eficaces estas tecnologías para conseguir tales objetivos.

3. Seguridad

Los acontecimientos del 11 de septiembre han sido un catalizador para la aceptación pública de medidas de seguridad que invaden la privacidad y facilitadores de un movimiento hacia una recogida masiva de información por parte de la policía, mediante la utilización de tecnologías de vigilancia generalizadas.

Aunque la dinámica del delito sigue fundamentalmente inalterada- dirigida como siempre por motivación, oportunidad y vulnerabilidad –la explotación delictiva de las nuevas tecnologías abrirá nuevas fronteras. La tecnología transformará el modo de funcionamiento del delito y del terrorismo, y su organización se desarrollará y responderá a nuevas formas de control y persecución. En último término, esto influirá sobre el modo en que las fuerzas de seguridad (así como los delincuentes y los terroristas) utilizan la tecnología. Sin embargo, cualesquiera que sean los resultados de la “carrera armamentista” tecnológica en la lucha contra el delito, el factor humano para conseguir la seguridad es aún, con mucho, el más importante. Incluso los controles de seguridad más estrechos pueden socavarse mediante una ingeniería social adecuada o por la negligencia humana. Cualquier solución a un problema de seguridad debe por tanto considerar tanto la tecnología como el comportamiento humano.

En este nuevo entorno, el impacto de las tecnologías de vigilancia debe evaluarse con cuidado, tanto en relación con su eficacia como en la sensibilidad de los datos generados. Aparte de las cuestiones de proporcionalidad, la relación básica coste-eficacia de los sistemas de vigilancia es una preocupación primaria. En algunos casos, los beneficios de la tecnología pueden no compensar los costes, dado el nivel de riesgo y los resultados alcanzados. En segundo lugar, los sistemas de vigilancia son ellos mismos vulnerables al mal uso y pueden desviarse a fines que los apartan de su pretendido uso -la identificación y el seguimiento de los delitos y del terrorismo. Mientras que las posibilidades de mal uso derivan actualmente de amenazas internas, las que se deban a terceras partes llegarán a ser más importantes conforme las actividades de vigilancia se difundan entre las organizaciones comerciales. El tipo de vigilancia llamada “pequeño hermano”, tanto de clientes como de empleados, y el control de los niños por parte de los padres o cuidadores con “*Web cams*”, plantearán importantes problemas de invasión de la privacidad.

El tipo de vigilancia llamada “pequeño hermano”, tanto de clientes como de empleados, así como el control de niños por parte de padres o cuidadores con web cams, plantearán importantes conflictos en cuanto a la invasión de la privacidad.

Estos y otros factores van a configurar el futuro de las tecnologías de vigilancia. En general, una mejor evaluación del impacto de los costes y beneficios del control tecnológico, y la educación pública sobre los resultados, darán lugar a mecanismos de vigilancia más adecuados. Otros factores incluyen la evaluación de la proporcionalidad de las medidas antiterroristas (es decir, en qué medida una invasión mucho mayor de la privacidad se traducirá en una protección más adecuada) y sus posibles efectos colaterales (en relación con la comodidad y el probable impacto financiero), así como el seguimiento por auditoría de los procesos de implementación. El desplazamiento de los delitos y del terrorismo hacia áreas menos controladas, la globalización de los delitos y el impacto de los desarrollos tecnológicos sobre la actividad delictiva y terrorista, también deben considerarse cuando se definen mecanismos de seguridad eficaces.

Otra cuestión a tratar es si la balanza de la responsabilidad descansa en el ciudadano o en el Estado. Los ciudadanos tienen una responsabilidad individual (por ejemplo estar vigilantes como individuos y asegurar su propiedad privada o comercial) y cada vez más empresas privadas están gestionando sus propios sistemas de vigilancia. Sin embargo, el Estado parece estar mejor situado para la recogida y evaluación de información sobre riesgos y para la comunicación a los ciudadanos cuando proceda. Además, puesto que muchos de los datos necesarios están en manos de entidades comerciales, será necesario desarrollar relaciones público-privadas que garanticen que los cuerpos de seguridad puedan acceder a ellos y evaluarlos. Esto requerirá adaptaciones en el marco legal sin contar con mayor apoyo por parte del consumidor ni con incentivos económicos para que las empresas lo aborden. Tampoco hay mayor impulso desde la profesión jurídica, ya que los riesgos adicionales en seguridad puestos de manifiesto por la cooperación entre los sectores público y privado van a supondrán nuevas demandas en el sistema judicial.

Es necesario desarrollar relaciones público-privadas para garantizar que los cuerpos de seguridad tengan acceso a datos sobre delincuencia y puedan evaluarlos, algo que requerirá modificaciones en el marco legal.

4. Privacidad

La naturaleza omnipresente de los sistemas de información “on line” hace extremadamente difícil que los usuarios finales puedan identificar el uso indebido de sus datos personales. No sólo eso: los múltiples procesos de identificación y autorización implicados en las transacciones por Internet dan lugar a una cantidad creciente de información personal recogida y almacenada en un número cada vez mayor de sistemas de información, con el consiguiente crecimiento del riesgo de abuso de la privacidad.

Como ya se ha discutido anteriormente, la mayoría de las tecnologías utilizadas para vigilar o establecer el perfil de las personas, son invisibles para el usuario de Internet, facilitando así la recogida, la agregación y el cruce de datos por parte de terceros con fines comerciales. Esta falta de concienciación de los procesos subyacentes al uso de Internet

justifica la preocupación de los ciudadanos sobre la posibilidad de intromisión en sus asuntos personales, revelación de información personal delicada o atribución incorrecta de acciones. Además, el abuso de la privacidad no es sólo consecuencia de lo que algunos consideran un patrón familiar en gobiernos e instituciones públicas, sino que el sector privado y cada vez más otros ciudadanos perpetran cada vez más este abuso.

El marco legal (ya sea a nivel local, nacional o internacional) ha protegido en el pasado, y sigue protegiendo, a los ciudadanos del uso indebido de sus datos personales. Ciertamente, uno de los pilares principales de la nueva Constitución Europea es la Carta de Derechos Fundamentales, en la que se reafirma claramente el derecho a la privacidad y a la protección de los datos personales. Tanto las herramientas de privacidad como las de protección de datos defienden a los individuos frente a intromisiones excesivas por parte de autoridades gubernamentales o de actores privados, protegen a las personas frente a un equilibrio desigual del poder que erosiona su libertad individual y limitan prácticas como el establecimiento de perfiles o el cruce y rastreo de datos, que llevarían a un control total de los ciudadanos. Por ello, la privacidad y la protección de datos ganan importancia a medida que nuestras sociedades evolucionan hacia lo que podrían llamarse sociedades de “vigilancia”.

Tanto las herramientas de privacidad como las de protección de datos defienden a los individuos frente a las medidas de intromisión excesiva por parte de autoridades gubernamentales o actores privados.

Sin embargo, existen problemas que no quedan totalmente cubiertos en este marco legal. Uno de ellos es el problema del “efecto horizontal” de los derechos humanos contemporáneos, ya que la privacidad no es amenazada sólo por los gobiernos, sino también por empresas patronos u otros ciudadanos. De hecho, los derechos de los ciudadanos están mejor protegidos frente a las infracciones gubernamentales que frente a las infracciones de otros ciudadanos o del sector privado. También se podría reforzar la protección que ofrece la legislación actual de la UE en el caso de que una persona comercie con su privacidad, a cambio de ciertos beneficios comerciales.

La legislación actual define unas “categorías especiales de datos” que recibe una protección mayor, si bien todos los datos (incluidos datos ordinarios como nombres y direcciones) están también protegidos. Además, en los casos en los que una determinada tecnología suponga una amenaza especial por la sensibilidad de los datos procesados, cabe redactar una legislación específica, habitualmente de tipo limitador, que contemple el posible abuso o uso indebido. Por ejemplo, aunque el tratamiento de muestras de ADN está completamente cubierto por la Directiva de Protección de Datos, las graves implicaciones de cualquier acceso no autorizado a la información contenida en estas muestras son tales, que se estiman necesarias medidas adicionales concretas. Así, los estados miembros han decidido completar la Directiva de Protección de Datos con cláusulas específicas de prohibición sobre la utilización de esta tecnología y de los datos a los que da lugar.

Cuando una tecnología suponga una amenaza especial para datos procesados, cabe elaborar una legislación específica, habitualmente de tipo limitador, que contemple el posible abuso o uso indebido.

De acuerdo con las medidas legales vigentes en Europa, la tecnología tiene un papel complementario que desempeñar en la protección contra el abuso de la privacidad. Una nueva categoría de tecnologías, las Tecnologías para Reforzar la Privacidad (“*Privacy Enhancing Technologies*”, PET's), se está empleando para combatir la erosión de la privacidad llegando de la mano de las tecnologías de seguridad, ya que la protección de datos delicados de privacidad, en tránsito o en almacenamiento, necesita mecanismos de seguridad (si bien es cierto que existe una tensión inherente entre privacidad y seguridad). Es de suponer una expansión en el desarrollo de las PET's, especialmente en las áreas de minimización de datos, preferencias de privacidad y sistemas de gestión de la identidad. Sin embargo, actualmente existe una limitada demanda de mercado de las PET's debido a sus altos costes de desarrollo y a la falta de un modelo empresarial viable.

De acuerdo con las medidas legales vigentes en Europa, la tecnología tiene un papel complementario que desempeñar en la protección contra el abuso de la privacidad.

5. Algunas áreas tecnológicas que influyen sobre la privacidad y la seguridad

Las tecnologías que refuerzan la seguridad y la privacidad aumentarán la confianza en los servicios de la Sociedad de la Información y capacitarán al ciudadano mediante el fortalecimiento de su control sobre los intercambios de datos llevados a cabo a través de Internet. Sin embargo, como cualquier otra tecnología, también pueden volverse en contra del ciudadano, en este caso porque facilitan nuevas formas de delito o abuso.

En este estudio se han seleccionado tres áreas concretas que implican la aplicación de tecnologías nuevas y emergentes, para un análisis de la medida en que cada una de ellas compromete el equilibrio tradicional entre seguridad y privacidad individual. Las tres áreas son:

- **Tecnologías relacionadas con la identidad**, que permiten nuevos modos de definir y expresar la identidad. Incluyen sistemas de gestión de la identidad (“*Identity Management Systems*”, IMS), dispositivos de identidad basados en radiofrecuencia (“*Radio-Frequency based IDentity devices*”, RFID) y biométrica;
- **Servicios basados en la localización**, en los que los dispositivos móviles de comunicación, normalmente teléfonos móviles, se utilizan para proporcionar a los usuarios servicios basados en el lugar donde éstos se encuentren en un momento determinado (por ejemplo en la proximidad de restaurantes o tiendas);
- **Tecnologías de Inteligencia Ambiental**, incluyendo el concepto de “residencia virtual”. La Inteligencia Ambiental está en la vanguardia de la investigación en tecnologías de la Sociedad de la Información en el Sexto Programa Marco de investigación y desarrollo tecnológico de la UE. Estas tecnologías, si se implementan con éxito, facilitarán cambios radicales en los futuros patrones de trabajo y estilo de vida.

5.1 Tecnologías relacionadas con la identidad

Cuanto más se implica un ciudadano en actividades “on line”, más expuesto está a posibles riesgos para su privacidad y seguridad. Las tecnologías relacionadas con la identidad permitirán que los ciudadanos gestionen estos riesgos y, como tales, se convertirán en una parte esencial de la comunicación a través de Internet para cualquier propósito. Por esta razón, la adopción de estas tecnologías tendrá un efecto catalizador directo sobre la adopción de los servicios de la Sociedad de la Información en su conjunto.

Los Sistemas de Gestión de Identidad multipropósito y multilaterales permitirán a los ciudadanos gestionar los estrechamente entrelazados riesgos de seguridad y privacidad.

La digitalización de la identidad puede considerarse un "cuello de botella" para la adopción por parte de los ciudadanos de los servicios de la Sociedad de la Información. Sólo la exclusión de los servicios proporciona al ciudadano protección real de su privacidad, lo que puede llevar a exagerar las reticencias por parte de los ciudadanos a adoptar tecnologías de identidad.

Un análisis de los dos procesos de creación e identificación de identidad en la Sociedad de la Información indica que aunque los proveedores de tecnología influyen sobre la creación de identidad “on line”, se exige que el usuario desempeñe un papel cada vez más importante en la construcción y gestión de su personalidad. Esto pone de relieve la responsabilidad de la elección informada y presupone formación, cosa que los usuarios actuales ni tienen ni están interesados en adquirir.

Los Sistemas de Gestión de la Identidad multipropósito y multilaterales reflejan las entrelazadas necesidades de seguridad y de privacidad y sobre ellas se debate qué diseños arquitectónicos pueden abarcar todas las características beneficiosas, y qué entorno legislativo apoyaría una adopción generalizada. Opcionalmente, estos sistemas podrían hacer uso también de las tecnologías biométricas, que mejoran la seguridad pero dan lugar a otros problemas de privacidad,¹ y plantean retos tecnológicos en lo que respecta a su implementación.

Aunque un marco legal apropiado facilitaría la mayor difusión de los sistemas de gestión de la identidad, existen reservas sobre cuál sería la fiabilidad de su uso generalizado. Las primeras experiencias han demostrado que cuanto mayor es el tamaño del grupo de usuarios al que se aplica el sistema, mayor es el número de errores en su funcionamiento. La comodidad es otro factor que inhibe la adopción, en la medida en la que el uso fiable de los sistemas de gestión de la identidad requiere ciertas condiciones adicionales: cuanta más seguridad se exija más tiempo consumirá el proceso. Por último, a largo plazo, merecerán especial atención nuevos sistemas menos intrusivos e invisibles (tales como la identificación basada en la radio-frecuencia, los bioimplantes o los detectores de ADN) puesto que hacen surgir un nuevo conjunto de problemas de seguridad y de privacidad en relación con la identificación tanto “on line” como “off line”.

¹ Estos datos contienen con frecuencia información adicional, fácil de inferir; por ejemplo, la abundancia de información contenida en las muestras de ADN excede ampliamente a la que se necesita para fines de identificación.

5.2 Servicios basados en la localización

La posibilidad de localizar junto a la disponibilidad continua de banda ancha desde cualquier terminal móvil permitirán ofrecer Servicios Basados en la Localización (*"Location Based Services"*, LBS) que serán atractivos para los consumidores y proporcionarán ingresos útiles a los operadores. Sin embargo, tendrán también un impacto sustancial sobre el equilibrio seguridad/privacidad para el ciudadano.

La informatización precisa en tiempo real de la localización de un ciudadano tiene implicaciones importantes para su seguridad y su privacidad.

Es importante observar que existen beneficios evidentes, en lo que se refiere a la mejora de la seguridad: conocer dónde está una persona en un momento determinado, servicios de emergencia dotados de mayor eficacia, o localización de personas vulnerables en tiempo real para garantizar su seguridad. Sin embargo, la mayoría de las aplicaciones serán en servicios comerciales exponiendo a los usuarios a un posible acceso no autorizado a los datos, datos de los que se pueden inducir movimientos y hábitos personales. La capacidad para hacer estas deducciones aumentan con el uso de técnicas de cruce y rastreo de datos, que combinan información de diferentes fuentes y sacan conclusiones sobre el modo personal de comportamiento, más allá de lo que implican los propios datos de localización. La capacidad para deducir el comportamiento de los ciudadanos combinando datos de diferentes fuentes representa una grave vulnerabilidad de la privacidad, cuyas implicaciones tendrían que considerar los políticos y las fuerzas de seguridad.

Por otro lado el aumento del número de actores con acceso a la información de localización de ciudadanos, principalmente para proporcionar servicios de valor añadido, introduce nuevos riesgos para la privacidad.

Además, en el desarrollo de políticas para abordar estos problemas es necesario considerar una serie de cuestiones fundamentales, tales como la propiedad de los datos de localización de los usuarios o el significado legal del consentimiento en este contexto. ¿Debe permitir la legislación el llamado modelo de "oferta" de provisión de servicios con valor añadido (es decir, suministrados sin una petición concreta) mejor que un modelo basado en una petición concreta o general del usuario? Otro conjunto de cuestiones se refiere a la retención de datos y a qué tipo de datos podrían utilizar legalmente las fuerzas de seguridad.

5.3 Tecnologías de inteligencia ambiental y residencia virtual

El concepto de Inteligencia Ambiental proporciona una amplia visión sobre el modo en que se desarrollará la Sociedad de la Información: destacan la mayor facilidad de uso, un mayor apoyo para servicios eficientes, la capacitación del usuario y el apoyo a las interacciones humanas. En esta visión, los seres humanos estarán rodeados por interfaces inteligentes intuitivas, incorporadas en toda clase de objetos. El entorno de Inteligencia Ambiental total (al que se denomina en el argot, Espacio AmI, por "*Ambient Intelligence*") será capaz de reconocer y adaptarse a la presencia de diferentes individuos trabajando sin discontinuidades, sin obstrucciones y a menudo de forma invisible.

El entorno de Inteligencia Ambiental será capaz de reconocer y adaptarse a la presencia de individuos, trabajando de un modo carente de discontinuidades, de obstrucciones y, a menudo, invisible; sin embargo podrá exigir nuevas medidas de seguridad y de privacidad

Esta visión, aunque aún lejos de ser realidad, exige nuevas formas de seguridad y nuevas medidas de privacidad. El nuevo entorno hará desaparecer las fronteras tradicionales entre lo público y lo privado. La Inteligencia Ambiental es un primer ejemplo de compromiso entre datos personales y beneficios útiles. De hecho, el éxito de su funcionamiento depende de la adopción generalizada de ese compromiso, por parte de los ciudadanos.

El concepto de Residencia Virtual es un punto de partida importante para identificar las futuras necesidades de seguridad y de privacidad en el nuevo entorno. La Residencia Virtual engloba tanto el hogar inteligente conectado del futuro y su infraestructura doméstica, como la vida del ciudadano móvil “on line”. Del mismo modo que la residencia física en el mundo real, la residencia virtual del individuo exigirá una protección legal adecuada. Las áreas de esta protección incluirán la seguridad de la infraestructura doméstica esencial; el tipo y contenido de los datos personales intercambiados; y la definición legal del “territorio digital” privado de un individuo.

La Residencia Virtual engloba tanto el hogar inteligente conectado del futuro y su infraestructura doméstica, como la vida del ciudadano móvil “on line”.

6. El equilibrio entre seguridad y privacidad

El equilibrio seguridad/privacidad se veía afectado incluso antes del 11 de septiembre por la aparición de avances tecnológicos, por los “ciberdelitos” y por la falta de un marco jurídico y político internacionalmente aceptado. A lo largo de este informe se citan numerosas fluctuaciones en este equilibrio a favor de más seguridad y control, ya sea como resultado de las nuevas tecnologías o simplemente como resultado de las iniciativas políticas tomadas a partir del 11 de septiembre.

Se distinguen dos tipos de medidas de seguridad:

- Medidas que invaden la privacidad, tomadas a partir de los acontecimientos del 11 de septiembre. Estas medidas son la respuesta a una necesidad inmediata de un entorno más seguro y deberían ser transitorias y limitadas; su eficacia se debe evaluar cuidadosamente.
- Medidas que facilitan el desarrollo de la Sociedad de la Información, las cuales deberían buscar un equilibrio adecuado a largo plazo entre seguridad y privacidad. Para conseguirlo, posiblemente sean necesarias algunas acciones de reequilibrio a favor de la privacidad, aunque es difícil imaginar que combatir el terrorismo no tenga también un efecto a largo plazo.

Como ya se ha observado, otro factor que ha contribuido a inclinar la balanza a favor de los intereses de la seguridad y a alejarla de la protección de la privacidad es el uso cada vez mayor de la tecnología, por parte de los agentes del mercado, con el fin de recoger y procesar datos personales en su beneficio. Sin embargo, el objetivo de este informe no es

definir un punto de equilibrio óptimo, sino destacar el hecho de que el equilibrio establecido durante años de proceso democrático está cambiando, evaluar el impacto de este cambio, e identificar los factores que podrían contribuir a restablecer el equilibrio.

Aún queda por ver qué papel podría desempeñar la tecnología en el diseño de medidas de seguridad para impedir el uso indebido de datos. Por ejemplo, si se anuncia la colocación de cámaras de vigilancia en lugares públicos, el instrumento de control funciona a la vez como mecanismo disuasorio y de vigilancia.

Una nueva legislación y mejores políticas educativas podrían ser una contribución importante para el mecanismo de reequilibrio. En muchos casos, el abuso de la privacidad es resultado de la falta de conocimiento y de educación sobre el uso de las nuevas tecnologías y sus posibles efectos. Una mayor concienciación y un mayor control sobre los posibles efectos secundarios de las nuevas tecnologías podrían reducir estos riesgos al mínimo.

El actual marco jurídico de protección de la privacidad requiere una continua revisión para tener en cuenta los efectos de las nuevas tecnologías. El marco contempla tales mecanismos, por lo que resulta defendible que el marco actual es válido y lo seguirá siendo en el futuro.

7. Cuestiones políticas

La evolución de la tecnología y sus posibilidades es continua y rápida, por lo que conseguir un correcto equilibrio entre seguridad y privacidad es inevitablemente un objetivo móvil. En este informe se han estudiado ejemplos de tecnologías emergentes y sus aplicaciones, los tres ejemplos elegidos están relacionados con los posibles riesgos inherentes a la seguridad/privacidad y -aunque hay margen para que las políticas desplacen la I+D en ciertas direcciones- lo que más afecta al equilibrio entre seguridad y privacidad es la implantación de la tecnología y el uso que se haga de ella una vez disponible.

Como resultado del análisis de estos ejemplos, en el informe se apuntan diversas cuestiones políticas, que se enumeran a continuación.

- **Factores humanos, educación y concienciación.** Se ha destacado la importancia de los factores humanos, además de la tecnología, para combatir la delincuencia y el terrorismo, junto con la necesidad de educación y concienciación por parte de los ciudadanos.
- **Robo de identidad.** Los casos de robo de identidad están aumentando tanto en el mundo real como en el virtual, y es necesario adoptar salvaguardas adecuadas. Los riesgos cada vez son mayores a causa de las prácticas comerciales actuales que empujan a los consumidores a negociar con su identidad a cambio de beneficios comerciales, así como a causa de la ausencia de una regulación armonizada en Europa.
- **Prueba digital.** La necesidad de crear, normalizar y difundir herramientas de prueba digitales. Es necesario establecer métodos para que la prueba digital sea utilizable y sea

aceptados legalmente en procesos judiciales. Resulta también necesario asegurar un nivel de eficiencia aceptable en los procesos de persecución del delito, incluyendo la necesidad de responsabilidad y transparencia cuando se realizan estos procesos.

- **Bases de datos del sector privado.** El uso creciente de bases de datos del sector privado por parte de las fuerzas de seguridad (en forma de perfiles, tanto en la persecución como en la prevención de los delitos) ha puesto de manifiesto la falta de una legislación europea armonizada relativa al mantenimiento de estas bases de datos y a su integridad, precisión, seguridad y protección.
- **Incentivos para el sector privado.** No está claro la rentabilidad que el sector privado obtendría de crear y adoptar productos que cumplan y mejoren la privacidad o la seguridad. Entre las razones se encuentran los altos costes que acarrearán, la falta de concienciación y demanda por parte de los consumidores y la complejidad de la instalación y uso. Este es un aspecto de fracaso del mercado que podría justificar una intervención regulatoria.
- **Efectos horizontales.** La actual legislación sobre privacidad de la UE carece de “efecto horizontal”, lo que significa que es imposible que los ciudadanos presenten reclamaciones contra otros ciudadanos, sus patrones o un organismo comercial (empresas) basándose en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales.
- **Contrapesos de poder.** Es necesario disponer de mecanismos para “vigilar al vigilante”, ya sea un organismo público, privado o las fuerzas de seguridad, con el fin de preservar la privacidad de los ciudadanos.
- **Indicadores de la esfera privada-pública.** La falta de indicadores de la esfera privada-pública en la Sociedad de la Información y la necesidad de definir jurídicamente el territorio digital privado (véase el capítulo 4, Residencia Virtual) con el fin de facilitar una mayor aceptación del entorno tecnológico de la Sociedad de la Información.
- **Legislación específica para una tecnología.** Las amenazas que encierran ciertas nuevas tecnologías pueden dar lugar a la redacción de legislación específica en casos en los que se observe que la protección de la privacidad o de los datos es insuficiente.

La velocidad a la que se producen los cambios en los avances tecnológicos y la intensificación del uso de las tecnologías exigen una observación y evaluación continuas del equilibrio entre la privacidad y la seguridad y los riesgos asociados, así como la evaluación de la necesidad de una acción legislativa específica. Este informe también pone de manifiesto la necesidad de fomentar mejores prácticas y normas usos, así como la necesidad de una evaluación continua de las tecnologías emergentes para observar sus implicaciones en cuanto a seguridad y privacidad. Una forma de llevar a cabo estas funciones podría ser mediante la creación de un observatorio europeo de tecnologías en relación a la identidad en distintos entornos de red (Internet, teléfonos móviles, espacio de Inteligencia Ambiental) y los autores instan a que se preste especial atención al establecimiento de tal actividad.

8. Estructura del informe

Este informe analiza el posible uso de las futuras tecnologías y su posible efecto positivo o negativo en el equilibrio seguridad/privacidad en tres áreas diferentes de la vida cotidiana de los ciudadanos en la Sociedad de la Información: el futuro de la identidad, los servicios basados en la localización y el espacio de Inteligencia Ambiental (residencia virtual), tras el 11 de septiembre. Estas áreas constituyen los tres capítulos principales del informe, los capítulos 3, 4, y 5:

El futuro de la identidad, tratado en el capítulo 3, constituye el eje principal de las interacciones de los ciudadanos en la futura Sociedad de la Información. La importancia cada vez mayor de la expresión electrónica de las características del ser humano (identidad, comportamiento, rasgos biológicos, etc.) cuando se hace uso de las nuevas TIC, no sólo da lugar a nuevos indicadores de privacidad, sino que también puede poner en riesgo la integridad de los datos personales en el futuro. En la era posterior al 11 de septiembre, esta preocupación es cada vez mayor.

En este capítulo se estudian los procesos de creación e identificación de identidad en la Sociedad de la Información y se analizan tecnologías emergentes relacionadas, tales como las tecnologías biométricas para validación de la identidad, los sistemas multilaterales y con fines múltiples de gestión de la identidad, los implantes biométricos, las tecnologías para la protección de la identidad virtual y las tecnologías para la gestión de las pruebas digitales y la protección frente al robo de la identidad. Además, se revisan los retos tecnológicos, los problemas de seguridad y privacidad, así como la influencia de estas tecnologías sobre el equilibrio entre la privacidad y la seguridad de los ciudadanos.

Los servicios basados en la localización, tema del capítulo 4, tendrán efectos sobre el equilibrio seguridad/privacidad de los ciudadanos. La combinación de: tecnologías que proporcionan conexiones móviles de banda ancha siempre activas, la futura adopción generalizada de Internet móvil, y la futura demanda de servicios basados en la localización, cambiarán por completo el contexto de utilización. Por una parte, se podrá disponer de información precisa sobre la localización de los ciudadanos, lo que potenciará la seguridad del usuario (por ejemplo, facilitará los servicios de emergencia), y por otra parte, incrementará el número de personas que tengan acceso y hagan uso de la información de localización, generando nuevos riesgos para la privacidad de los ciudadanos.

Este capítulo describe los dos agentes principales de sistemas móviles de localización: en primer lugar, las tendencias en el acceso a través de banda ancha móvil, lideradas por los sistemas móviles y las redes WLAN ("*Wireless Local Area Network*"); y en segundo lugar, las diferentes tecnologías de localización. Se consideran, a continuación, los posibles efectos de estas tecnologías sobre el equilibrio entre privacidad y seguridad.

El capítulo 5 sobre la residencia virtual analiza las interacciones de los ciudadanos, tanto desde dentro como fuera del hogar, en el futuro "espacio de Inteligencia Ambiental". La "Inteligencia Ambiental" proporciona una visión de la futura Sociedad de la Información donde los seres humanos estarán rodeados de interfaces inteligentes, asistidas por una tecnología informática y de redes omnipresentes incorporadas en objetos cotidianos como

muebles, ropa, vehículos, carreteras o materiales inteligentes. Todo ello respaldado por avances en tecnologías de computación (miniaturización, portabilidad, almacenamiento), comunicaciones inalámbricas ubicuas e interfaces de fácil uso. El concepto de residencia virtual (es decir, el futuro hogar inteligente y sus infraestructuras domésticas básicas, en la vida del ciudadano móvil “*on line*”) contribuye significativamente a la forma que tomarán la seguridad y la privacidad en el futuro, en este nuevo espacio de Inteligencia Ambiental, llamando por nuevas formas de seguridad y protección de la privacidad y salvando la separación entre lo público y lo privado.

Por último, el capítulo 6 trata en detalle el equilibrio entre la seguridad y la privacidad. Estos capítulos van precedidos de una discusión introductoria (capítulo 1) y de una descripción de los avances tecnológicos de la Sociedad de la Información relevantes en el debate privacidad/seguridad (capítulo 2).

Se contó con la participación de expertos ajenos al Centro Común de Investigación (CCI, o JRC, de “*Joint Research Centre*”) completando el informe con dos análisis detallados y exhaustivos sobre los conceptos de privacidad y seguridad, tendencias y sus posibles problemas. Estas dos contribuciones externas se resumen en el capítulo 6 (secciones 6.1 y 6.2) y se reproducen en su totalidad en los anexos 1 y 2:

Anexo 1: "Crear conciencia sobre la privacidad y la protección de los datos: una visión prospectiva a la luz del futuro de la identidad, los servicios basados en la localización y la residencia virtual", por el catedrático Serge Gutwirth de la Universidad Libre de Bruselas y de la Universidad Erasmus de Rotterdam y el catedrático Paul de Hert de la Universidad de Leiden.

Anexo 2: "Delito y seguridad tras el 11 de septiembre: problemas de seguridad, privacidad y cumplimiento de la ley, relacionados con las nuevas tecnologías de la información y las comunicaciones", por el catedrático Michael Levi de la Universidad de Cardiff y el Dr. David S. Wall, director del Centro de Estudios de Derecho Penal de la Universidad de Leeds.

El Anexo 3 contiene una relación de bibliografía recomendada.