

Vigilancia Privacidad y Seguridad

¿CUÁL ES SU OPINIÓN?

surprise
surveillance
privacy
security



Índice

1	Bienvenidos a SurPRISE	5
1.1	Instrucciones para la lectura de este folleto	6
2	Resumen	7
3	Un día cualquiera...	9
3.1	Vigilancia, privacidad y seguridad	10
3.1.1	Vigilancia	10
3.1.2	Privacidad y protección de datos: ¿son cuestiones importantes?	11
3.1.3	Seguridad	11
4	Tres nuevas tecnologías de seguridad	13
5	CCTV Inteligentes	15
5.1	¿Por qué se desarrollaron los CCTV inteligentes?	15
5.2	¿Cómo se utilizan los CCTV inteligentes?	17
5.3	Mejoras en la seguridad	18
5.4	Problemática	18
6	Cibervigilancia mediante inspección profunda de paquetes	21
6.1	¿Por qué se desarrollo la inspección profunda de paquetes?	21
6.2	¿Cómo se utiliza la inspección profunda de paquetes?	22
6.2.1	Usos comerciales	23
6.2.2	Usos relativos a la seguridad pública y nacional	24
6.3	Mejoras en la seguridad	24
6.4	Problemática	24
7	Sistemas de localización y seguimiento a través de smartphones	27
7.1	¿Por qué se desarrollaron los sistemas de localización y seguimiento a través de smartphones?	27
7.2	¿Cómo se utilizan los sistemas de localización y seguimiento a través de smartphones?	29
7.2.1	Usos comerciales	29
7.2.2	Usos relativos a la seguridad pública y nacional	30
7.3	Mejoras en la seguridad	30
7.4	Problemática	31
8	¿Es la tecnología la única alternativa?	33
8.1	Soluciones locales	33
8.2	Soluciones nacionales o internacionales	33
9	Le cedemos la palabra...	35
	Información sobre el documento	

1 Bienvenidos a SURPRISE

Bienvenidos a SurPRISE: un proyecto de investigación a nivel europeo. SurPRISE es la versión abreviada de 'Surveillance, Privacy and Security' (Vigilancia, Privacidad y Seguridad). El objetivo de este proyecto es recopilar el punto de vista de los ciudadanos con respecto a las llamadas tecnologías de seguridad. La mayor parte de este tipo de tecnologías se basa en la vigilancia a personas y las actividades que llevan a cabo. La policía y el personal de seguridad se valen de ellas para controlar lo que pasa, para así detectar y evitar problemas de seguridad. Las tecnologías de seguridad basadas en la vigilancia están presentes, por ejemplo, cuando usted va al aeropuerto y los escáneres comprueban su equipaje o cuando la cámara de un circuito cerrado de televisión (CCTV) graba lo que ocurre en una calle por la que va caminando. SurPRISE tiene por objetivo asegurar que estas tecnologías resultan efectivas y seguras y que respetan los derechos humanos. Para alcanzar dicho objetivo SurPRISE necesita contar con su colaboración.

Le hemos invitado a formar parte del proyecto SurPRISE porque la Comisión Europea desea conocer qué opinan los ciudadanos que se debería hacer para garantizar su seguridad y conseguir que se sientan protegidos. Si acude a la cumbre ciudadana sobre SurPRISE podrá compartir su punto de vista acerca de las nuevas tecnologías de seguridad con otros ciudadanos. SurPRISE recopilará las opiniones de los ciudadanos con respecto a las tecnologías de seguridad y las compartirá con la Comisión Europea.

Las cumbres ciudadanas se celebrarán en nueve países europeos: además de en España, los ciudadanos podrán participar en Austria, Dinamarca, Alemania, Hungría, Italia, Noruega, Reino Unido y Suiza. Los resultados de estas cumbres se entregarán a la Unión Europea en junio

de 2014 y se podrán a disposición de los medios de comunicación, gobiernos y ciudadanos.

El presente folleto incluye información básica sobre aquellas cuestiones que se tratarán en la cumbre española de SurPRISE y que tendrá lugar en febrero de 2014. Además, en él podrá encontrar información relativa a las nuevas tecnologías de seguridad que el proyecto SurPRISE está estudiando. Asimismo, se facilita información de referencia sobre la vigilancia, seguridad y privacidad en Europa.

Somos conscientes de que la lectura de este folleto puede resultar complicada, pero no se trata de aprobar ningún examen ni de convertirse en un experto. El objetivo del presente folleto es ofrecerle información sobre las cuestiones que se van a abordar en la cumbre ciudadana y facilitar que se vaya formando una idea sobre sus puntos de vista en materia de vigilancia, privacidad y seguridad. Su participación en la cumbre ciudadana resulta valiosa precisamente porque no es experto en la materia. Le hemos pedido que forme parte porque usted es un ciudadano de a pie cuya vida diaria se ve afectada por las decisiones que toman los políticos europeos y los de su país.

SurPRISE hará llegar las opiniones de los ciudadanos, que se recogerán de manera anónima, a sus representantes electos y legisladores. Las tecnologías de seguridad están estrechamente relacionadas con los derechos humanos, cuestiones relativas a la justicia y a la confianza depositada en las instituciones y su efectividad. Por eso es necesario involucrar al público general y no solo a legisladores, sectores, expertos y organizaciones benéficas. Los políticos se encargan de establecer las políticas de seguridad, pero usted, como ciudadano, tiene que vivir con las consecuencias derivadas de dichas decisiones. Por tanto, su opinión es de vital importancia.

**La ciencia es fuente de información.
No nos dice lo que tenemos que hacer.
La decisión es nuestra.
¡Tome la palabra!**

1.1 Instrucciones para la lectura de este folleto

Tras el resumen que encontrará en el apartado siguiente, este folleto cuenta con cinco apartados principales. El primero es una introducción general a la vigilancia, seguridad y privacidad en Europa. Los tres apartados siguientes describen las tecnologías de seguridad sobre las que se hablará en la cumbre ciudadana. Aunque el folleto incluye tres tipos diferentes de tecnología, en la cumbre solo se tratarán dos de ellas. La carta de invitación le informará de las tecnologías a tratar durante la cumbre.

Cada apartado describe la razón por la que se desarrollaron, cómo se usan, los avances en materia de seguridad que ofrecen y sus limitaciones. Asimismo, en el apartado relativo a cada tecnología hemos incluido un cuadro informativo en el que se explica con mayor detalle su funcionamiento, además de un cuadro en el que se describe la problemática que suscita la tecnología en cuestión. El apartado final introduce de manera breve algunas alternativas a las tecnologías de seguridad.

Si no desea leer el documento completo, hemos incluido un resumen de los puntos principales.

2 Resumen

El objetivo de SurPRISE consiste en comprender los diferentes puntos de vista de los ciudadanos europeos en relación con las nuevas tecnologías de seguridad. La preocupación de los gobiernos europeos con respecto al terrorismo, el crimen organizado y los delitos electrónicos es cada vez mayor, por eso invierten en el desarrollo de nuevas tecnologías de seguridad.

La mayoría de estas tecnologías analizan la información generada por parte de los ciudadanos en su vida cotidiana. Por ejemplo, utilizan información obtenida de teléfonos móviles, internet y de tecnologías “inteligentes” como los CCTV digitales con el fin de identificar a delincuentes y terroristas, a veces incluso antes de que comentan un delito.

Puesto que este tipo de tecnologías manejan información personal, podemos referirnos a ellas como “tecnologías de seguridad basadas en la vigilancia”.

Las tecnologías de seguridad basadas en la vigilancia son aquellas que:

utilizan la información recopilada en diferentes contextos en relación con la población general y sus actividades para abordar problemas de seguridad.

En las cumbres ciudadana sobre SurPRISE examinaremos en profundidad tres tecnologías de este tipo:

- > **CCTV inteligentes:** sistemas de CCTV que no sólo se limitan a vigilar espacios públicos. Los CCTV inteligentes incluyen además cámaras digitales conectadas entre sí mediante un sistema capaz de reconocer el rostro de las personas, analizar su comportamiento y detectar objetos.
- > **Cibervigilancia mediante inspección profunda de paquetes:** utilizan dispositivos de hardware y un software especial. Toda la información y los mensajes transmitidos a posible averiguar la ubicación y movimientos del usuario del teléfono durante un periodo de tiempo concreto. La ubicación de los teléfonos se puede establecer a través de las antenas a las que se conectan los teléfonos móviles, o de manera más exacta a través de los sistemas de geoposicionamiento global (GPS) o de la conexión de datos inalámbrica. través de

internet pueden ser leídos, analizados y modificados.

- > **Sistemas de localización y seguimiento a través de smartphones:** mediante el análisis de los datos de localización de teléfonos móviles, es

Cada una de estas tecnologías mejora la seguridad mediante la identificación de sospechosos o actividades delictivas o ilegales. Algunos piensan que también pueden facilitar mucho la vida cotidiana. Sin embargo, cada una de estas tecnologías conlleva una serie de inconvenientes. Por ejemplo, los CCTV inteligentes únicamente funcionan bajo determinadas condiciones y pueden producir un gran número de “falsas alarmas”. La inspección profunda de paquetes compromete la privacidad de la comunicación online. El control de los sistemas de localización y seguimiento a través de smartphones resulta complicado puesto que la mayoría de las aplicaciones transmiten información relativa a la ubicación desde el teléfono sin el conocimiento del usuario. La falta de control con respecto a la obtención y utilización de la información es una de las cuestiones asociadas con estas tecnologías que procederemos a examinar.

A pesar de las mejoras en la seguridad que ofrecen este tipo de tecnologías, algunos ciudadanos no terminan de forjarse una opinión cuando su información se utiliza con fines de seguridad. Si la seguridad de todos es mayor, a lo mejor su uso es legítimo. Sin embargo, si se violan los derechos humanos fundamentales, tal vez nunca puedan utilizarse de forma legítima. La opinión de las personas también puede variar dependiendo de lo que crean acerca de una serie de cuestiones, como por ejemplo:

- > ¿Funcionan de verdad estas tecnologías?
- > ¿Hasta qué punto son invasivas?
- > ¿Se puede confiar en el uso que les dan las instituciones?
- > ¿Están debidamente reguladas?
- > ¿Quién vigila a los vigilantes?
- > ¿Cuáles son las alternativas? ¿Son funcionales?

Estos son algunos de los puntos que abordaremos durante la cumbre ciudadana.

Por favor, continúa leyendo para tener más información sobre estas cuestiones

3 Un día cualquiera...

En algún punto del sur de Budapest, Aisha se incorpora a la Ruta Europea E-75 en dirección al Aeropuerto Internacional de Budapest. Se acuerda perfectamente de la primera vez que utilizó esa carretera. En aquel momento, pagó el peaje en efectivo; ahora se le carga automáticamente en su cuenta corriente. Las cámaras del sistema de reconocimiento automático de matrículas (ANPR en inglés) leen su número de matrícula mientras que el sistema del peaje se encarga del resto. Hasta ese momento Aisha no había reparado en las cámaras. En esta ocasión se fija en ellas y se plantea cómo conectan esa información con su banco.

Aisha aparca el coche y se sube al autobús lanzadera que la llevará a la terminal. Una vez allí, factura su equipaje utilizando una máquina de facturación automática. Coloca su pasaporte en la máquina, que se encarga de extraer los datos de su reserva. Cuando recibe la tarjeta de embarque, Aisha se da cuenta de que ahí también hay almacenada información relativa a su persona.

Una vez pasado, Aisha suelta su equipaje de mano en una cafetería. Pide un café; de nuevo se detiene antes de entregarle la tarjeta de crédito al camarero. Piensa: “es un trozo de plástico muy práctico pero, ¿quién registra esta transacción? ¿Y por qué?”.

Mientras Aisha espera a que se le enfríe el café, saca su smartphone para leer los mensajes. En el momento en el que se ilumina la pantalla, la ubicación indicada en la pantalla de inicio cambia inmediatamente de “Kecskemét”, el lugar donde vive, a “Ferihegy”. “¿Cómo lo sabe? Supongo que debe de haber una explicación bastante obvia, pero no se me ocurre ninguna”, reflexiona.

Aisha tiene el tiempo justo de mandar un correo electrónico a un compañero de trabajo antes de embarcar en el avión. Pone el teléfono en modo avión mientras se plantea qué pasará con su correo mientras viaja a través de internet.

El viaje de Aisha es bastante normal. Estos hechos son muy comunes en la vida de cualquier viajero. La tecnología le ofrece ciertas ventajas a Aisha, haciendo que su viaje sea más cómodo y práctico. No obstante, también provoca que se planteen algunas cuestiones: “¿Quién utiliza mi información personal y en qué me afecta que esa información se encuentre ‘dentro del sistema’?”

La mayoría de las tecnologías con las que se ha encontrado Aisha también están presentes fuera del mundo del aeropuerto. Casi nadie podría imaginarse la vida sin smartphones, tarjetas de crédito o internet. De hecho, una gran parte de nuestras actividades diarias generan los tipos de registro electrónico de los que toma conciencia Aisha. Quizá usted tenga en mente las mismas preguntas que Aisha. Los registros mencionados indican dónde estamos desde un punto de vista espaciotemporal, y a veces incluso lo que estamos haciendo. Por ejemplo, las operaciones bancarias, incluyendo las que se realizan con tarjetas de débito, pueden indicar los tipos de compra que realizamos y con quién las llevamos a cabo. Dicha información se almacena en las bases de datos bancarios y se puede consultar en nuestros extractos.

La información relativa a las reservas de viajes que conservan las aerolíneas indican si viajamos desde o hacia una zona de riesgo. Los datos de los teléfonos móviles revelan nuestra ubicación, con quién hablamos y la frecuencia con la que lo hacemos. Esta información queda registrada en las bases de datos de facturación de operadores de telefonía y servicios de internet. La normativa europea establece que esta información debe ser almacenada por un período de tiempo de entre seis meses a dos años. Por tanto, es posible identificar, seguir y localizar a la mayoría de personas en diferentes momentos de sus vidas. A lo mejor esto es precisamente lo que preocupa a Aisha, aunque al mismo tiempo su opinión se encuentra dividida debido a las ventajas que ofrecen estas tecnologías.

El tipo de tecnología que acabamos de describir y la información que recaba también puede resultarle beneficiosa a otros. Tras los ataques terroristas profesionales que tuvieron lugar en Europa y en otros lugares, los Gobiernos comenzaron a invertir en tecnologías de seguridad que se valen de este tipo de información. Asimismo, han modificado las leyes en vigor y aprobado otras nuevas que permiten el acceso a este tipo de información con fines de seguridad.

Aunque cuentan con un gran número de fuentes de inteligencia “oficiales”, los gobiernos se han dado cuenta de que se podrían detectar actividades de posibles terroristas o delincuentes por otras vías. Como la mayoría de los ciudadanos, los delincuentes y terroristas tienen cuentas corrientes, son titulares de documentos nacionales de identidad, usan internet y tienen teléfonos móviles. Además, también utilizan el sistemas de transporte, frecuentan espacios públicos y consumen productos y servicios. Es posible que obtener más información sobre estas actividades sea la clave para encontrar a terroristas y delincuentes. Muchos gobiernos opinan que hacer uso de las nuevas tecnologías de seguridad no solo facilita la detención de criminales, sino que también hace posible su identificación antes de que cometan delitos. Puesto que este tipo de tecnologías utilizan la información en este sentido, el proyecto SurPRISE se refiere a ellas como “tecnologías de seguridad basadas en la vigilancia”.

Las tecnologías de seguridad basadas en la vigilancia son aquellas que:

utilizan la información recopilada en diferentes contextos en relación con la población general y sus actividades para abordar problemas de seguridad.

Si Aisha pensase que su información se va a utilizar en ese sentido, ¿seguiría teniendo su opinión dividida? Si conllevara un aumento de su seguridad y de la de los demás, puede que llegase a aceptarlo. No obstante, el uso de estas tecnologías suscita conflictos relativos a los derechos humanos, privacidad, legislación y confianza. En ocasiones, dichas tecnologías recopilan y comparten información de una persona sin su conocimiento. Es inevitable que se obtenga y analice información de personas inocentes y, en el caso de algunos sistemas, de manera intencionada. Como tal, tienen potencial para invadir nuestra intimidad, un derecho humano fundamental en Europa. También pueden erróneamente identificar a personas inocentes como criminales con graves consecuencias para sus vidas.

Surgen, por tanto, una serie de preguntas:

- > ¿Se puede confiar en el uso que le dan las instituciones a los datos?
- > ¿Están debidamente reguladas las instituciones que utilizan dichos datos?
- > ¿El uso que se da a estas tecnologías se ajusta a

la ley?

- > ¿Las instituciones son transparentes y responsables en cada infracción sobre la privacidad que se comete en nombre de la seguridad?
- > ¿De verdad estas tecnologías mejoran la seguridad?

Estos son algunos de los puntos que abordaremos durante la cumbre ciudadana.

En los próximos párrafos introduciremos algunos términos y definiciones clave antes de pasar a describir las tres tecnologías que se analizarán durante la cumbre.

3.1 Vigilancia, privacidad y seguridad

3.1.1 Vigilancia

Si hablamos de “vigilancia”, probablemente nos vengan a la cabeza ciertas imágenes: a lo mejor se acuerda de “Gran Hermano”, tanto del *reality* de televisión como del personaje de la novela de George Orwell, 1984. Por tanto, es posible que asocie el concepto vigilancia con la incómoda sensación de que le observa una organización o persona desconocida y poderosa.

En SurPrise, cuando hacemos referencia a la “vigilancia” lo hacemos en el sentido de “supervisión de personas para regular o regir su comportamiento”, lo cual puede perseguir distintas finalidades. La vigilancia puede utilizarse por motivos de seguridad. Por ejemplo, la policía utilizaría sistemas de CCTV para localizar a delincuentes en la calle. Asimismo, la vigilancia podría tener fines comerciales. Por ejemplo, el uso que le dan los supermercados a las tarjetas de fidelización para conocer las preferencias de consumo de distintos grupos, lo cual influiría en las futuras ofertas especiales que se realizarían a los consumidores. La vigilancia puede ser una herramienta para evitar la delincuencia y arrestar a criminales pero también sirve para ofrecer productos y servicios a los consumidores.

Si la vigilancia es una parte tan importante de la sociedad, entonces cabría plantearse qué es lo que falla. Los reportajes de las noticias relativos a la “sociedad de la vigilancia” siempre parecen hacer hincapié en el lado más oscuro. La cuestión

principal es que controlar sistemas de vigilancia concede un gran poder. Es importante que aquellos que se encuentran en dichas posiciones de poder, como las fuerzas del orden, corredores de datos o minoristas ejerzan ese poder de manera justa y con el debido respeto a las libertades civiles y la ley.

Aunque usted piense que no tiene nada que esconder o nada que temer, en el fondo todo depende de quién observe, la razón por la que le están observando y la manera en la que se perciben sus acciones. Si carece de control o capacidad de decisión en ese proceso y de repente las reglas se ponen en su contra (debido a su origen étnico, religión, orientación sexual, género u opiniones políticas), ¿qué haría? Esta es la razón por la cual una vigilancia excesiva puede tener un impacto negativo en determinados derechos humanos como la libertad de expresión. En ese sentido, la vigilancia también causaría perjuicios a nivel de confianza social, puesto que los unos tendríamos miedo de los otros. Son muchas las cuestiones que poner en la balanza a la hora de utilizar diferentes tipos de datos de vigilancia en el contexto de la seguridad.

3.1.2 Privacidad y protección de datos: ¿son cuestiones importantes?

Uno de los factores principales a considerar son la privacidad y la protección de los datos que generan y emplean las nuevas tecnologías de seguridad. Aunque la privacidad tiene un significado diferente para cada uno, es una parte fundamental de la vida cotidiana. Existen ciertos aspectos que seguramente preferiría que permaneciesen en el ámbito privado en determinados momentos:

- > Qué hace, piensa o siente.
- > Información relativa a sus relaciones personales, con quién está, qué les dice a los demás -por carta o por e-mail-, sus características personales y su imagen.
- > Su cuerpo: cuánto muestra, si tiene derecho a evitar contactos no deseados o inspecciones corporales así como el acceso de terceros a elementos provenientes de su cuerpo como el ADN.

Piénselo: ¿le gustaría que una compañía de seguros de vida tuviese acceso ilimitado a su historial médico? ¿O que la policía pudiera escuchar sus

llamadas telefónicas? ¿Su casa tiene cortinas? Si ha contestado que no a las dos primeras preguntas y sí a la tercera es que le preocupa su privacidad. No es el único. Se han realizado estudios entre los usuarios más jóvenes de redes sociales que demuestran que, debido a su preocupación por la privacidad, solo exponen una parte bien elegida de ellos mismos. La gente sigue queriendo compartir información, pero con unos límites bien marcados. Para el individuo todo aquello situado más allá de estos límites representa las áreas de su vida que desea que se mantengan libres de toda interferencia externa: es su vida privada.

En SurPRISE, la privacidad se define como: la capacidad de un individuo para que no le invadan, para permanecer fuera del ojo público y para controlar su propia información.

El derecho a la privacidad es un derecho humano básico en la Unión Europea. Todos necesitamos nuestro derecho a la privacidad: para poder actuar, reunirnos y hablar libremente en una sociedad democrática. Las personas no podrían ejercer sus libertades democráticas si todos sus pensamientos, intenciones o acciones fuesen públicos. La nueva legislación europea en materia de protección de datos va a hacer hincapié en que la privacidad “se diseñe” en base a las nuevas tecnologías, de manera que resulten menos invasivas desde un principio. Se fomentará que todas aquellas empresas que se dediquen a las nuevas tecnologías tengan en cuenta la privacidad en todas las fases de sus procesos. Este nuevo enfoque se conoce como “privacidad desde el diseño”

3.1.3 Seguridad

En el proyecto SurPRISE la seguridad se define como:

la condición de estar protegido de cualquier peligro o evitar la exposición al mismo; la sensación de seguridad o ausencia de peligro.

La seguridad no solo hace referencia a la protección de cosas físicas como edificios, sistemas de información, fronteras nacionales, etc., sino que también hace referencia a la sensación de las personas de saberse seguras. En un mundo perfecto, unas medidas de seguridad efectivas redundarían en un aumento de la sensación de seguridad, pero no siempre es así.

Resulta extraño, pero como los nuevos sistemas de seguridad cuentan con el potencial de poner en peligro nuestra privacidad, pueden acabar

haciéndonos sentir menos seguros, en lugar de más. No obstante, puede que no todo el mundo tenga esa sensación. Como en el caso de la privacidad, la seguridad cuenta con un significado diferente para cada persona. Cada uno tenemos nuestra propia percepción de lo que consideramos una amenaza para la seguridad y de lo que estaríamos dispuestos a hacer para proteger aquello que es importante para nosotros.

Lo anterior también es aplicable para aquellos que gestionan la seguridad. Necesitan identificar y abordar amenazas de gran envergadura. Todos los gobiernos cuentan con unos recursos económicos, humanos y técnicos limitados para invertir en seguridad, por lo que se ven obligados a elegir. Para la Unión Europea, las prioridades básicas de seguridad son las siguientes:

- > [aumentar la seguridad electrónica de ciudadanos y empresas de la UE;](#)
- > [desmantelar redes criminales internacionales;](#)
- > [prevenir el terrorismo;](#)
- > [aumentar la capacidad de Europa para sobreponerse a cualquier tipo de crisis o catástrofe.](#)

Por tanto, puesto que Europa ha decidido centrarse en la recuperación tras cualquier tipo de crisis o catástrofe, la seguridad va más allá de prevenir la delincuencia o el terrorismo. A Europa también le preocupan las amenazas al medio ambiente, los recursos naturales, las infraestructuras, las actividades económicas y la salud. Para los legisladores, la seguridad se ha extendido a casi todas las áreas de la vida pública. Muchos estados europeos han adoptado este mismo enfoque. No obstante, ¿es acaso posible prometer la seguridad

en todos estos ámbitos? La industria de la seguridad es uno de los principales sectores en desarrollo en Europa en abordar esta necesidad. Incluye grandes empresas de defensa como Airbus, BEA Systems y Finmeccanica, así como muchas otras pequeñas empresas. Estos son algunos de los avances más recientes en relación con las tecnologías de seguridad basadas en la vigilancia:

- > [CCTV inteligentes, basados en la localización de delincuentes conocidos y en la identificación de comportamientos sospechosos,](#)
- > [cibervigilancia, centrada en la prevención de daños causados por virus, hackers o suplantadores de identidad;](#)
- > [sistemas biométricos, desarrollados con el fin de evitar que sujetos no deseados accedan a un determinado territorio así como para tramitar el acceso de aquellos que el gobierno considera “viajeros de confianza”;](#)
- > [vigilancia aérea con drones, capaces de detectar actividades peligrosas desde el aire sin ser vistos desde la tierra. Este tipo de información se puede utilizar para enviar personal de seguridad a zonas con conflictos emergentes;](#)
- > [sistemas avanzados de información de pasajeros, orientados a la detección de aquellos individuos que puedan suponer una amenaza antes de que viajen;](#)
- > [tecnologías de localización y seguimiento, desarrolladas para minimizar el daño a objetos en movimiento y localizar a sospechosos.](#)

4 Tres nuevas tecnologías de seguridad

Las tres tecnologías de seguridad que el proyecto SurPRISE está examinando son:

- > **CCTV inteligentes**
- > **Cibervigilancia mediante inspección profunda de paquetes**
- > **Sistemas de localización y seguimiento a través de smartphones**

Estas tecnologías de seguridad se encuentran todavía en fase de desarrollo por lo que la legislación relativa a las mismas aún puede decidirse.

En los apartados siguientes del presente folleto describiremos el funcionamiento de cada tecnología, el motivo de su desarrollo, quién las

utiliza y cómo. También describiremos las mejoras en la seguridad que ofrecen y la problemática en torno a la privacidad, así como otras cuestiones que conlleva el uso de cada tecnología de seguridad.

Tanto para este proyecto como para la Unión Europea es importante entender el punto de vista de los ciudadanos sobre las tecnologías de seguridad y hasta qué punto les resultan aceptables. Por eso su opinión es tan importante. A lo mejor usted ya tiene una opinión bien formada a favor o en contra de estas tecnologías. Durante la cumbre sobre SurPRISE se le ofrecerán muchas oportunidades de expresar su opinión, pero en concreto nos gustaría conocer su punto de vista sobre las cuestiones siguientes:

¿Qué influye en que una determinada tecnología de seguridad resulte más o menos aceptable para usted?

Por ejemplo:

- > Contar con más información sobre la tecnología en cuestión y su funcionamiento.
- > Contar con más información sobre las distintas instituciones que utilizan la tecnología y la información que genera.
- > Que exista una regulación legal y mecanismos de control.
- > Contar con más información sobre las distintas amenazas a las que nos enfrentamos en la actualidad y para las cuales se ha desarrollado esta tecnología.

O a lo mejor depende de lo invasiva que le parezca la tecnología. Por ejemplo:

- > Si provoca sentimientos de vergüenza.
- > Si vulnera sus derechos fundamentales.
- > Si divulga información a terceros sin su conocimiento o tiene consecuencias en otros aspectos de su vida privada.

O a lo mejor depende de la efectividad de la tecnología en cuestión:

- > Si facilita la vida.
- > Si le hace sentir más seguro.
- > Si cree que identifica a sospechosos de manera precisa.

Puede que solo repare en las tecnologías de seguridad cuando se encuentran físicamente cerca de usted. Por ejemplo, en un aeropuerto, en la calle o cuando utiliza el móvil o internet. Quizá el resto del tiempo no le molesten. O quizá las tecnologías de seguridad actuales le parezcan bien pero está preocupado sobre el uso que se les dará en el futuro.

5 CCTV Inteligentes

Anteriormente en este folleto hemos visto que Aisha, mientras se desplazaba al aeropuerto, se planteaba el funcionamiento de las cámaras que le cobraban el peaje. Las cámaras eran del tipo de reconocimiento automático de matrículas o cámaras ANPR. Las cámaras ANPR son un claro ejemplo de una nueva tecnología de seguridad conocida como “CCTV Inteligentes”.

La mayoría de los europeos están familiarizados con la idea de los sistemas de CCTV. Un sistema “tradicional” de CCTV incluye cámaras instaladas en el mobiliario urbano en zonas públicas o tiendas. Las cámaras se encuentran conectadas a una sala de control a través de sistemas de telecomunicaciones. Una vez en la sala de control, una serie de pantallas de televisión muestran a los técnicos especialistas las imágenes recogidas por las cámaras. Las imágenes se graban, almacenan y, tras un periodo de tiempo determinado, se borran. Se trata de un sistema “cerrado” puesto que las imágenes no se emiten en ningún lugar a excepción de la sala de control. Si los técnicos observan algo que les resulte sospechoso, avisan a los guardias de seguridad o a la policía por teléfono o radio para que intervengan.



5.1 ¿Por qué se desarrollaron los CCTV

Inteligentes?

Los CCTV se desarrollaron en un principio para observar los lanzamientos de misiles durante la Segunda Guerra Mundial y para dirigir procesos industriales peligrosos a distancia. Se vendieron por primera vez como tecnología de seguridad en los EE.UU. durante la década de los cincuenta. Los departamentos de policía de EE.UU. y el Reino Unido los adoptaron en los sesenta.

El uso de los CCTV aumentó de manera constante en Europa en los noventa, con el Reino Unido a la cabeza y seguido de cerca por Francia y los Países Bajos. Su aparición en los noticiarios es muy frecuente. En 2013, los sistemas de CCTV de Boston fueron fundamentales a la hora de identificar a los responsables de las bombas del maratón.

Los CCTV inteligentes se han diseñado para solventar el problema que presentaban los CCTV desde el principio. Es decir, el hecho de que existen muchas cámaras pero pocos ojos para vigilar lo que sucede. A diferencia de los sistemas de CCTV “tradicionales”, un sistema de CCTV inteligente utiliza una red de cámaras digitales conectada a un sistema capaz de analizar imágenes digitales. El software se encarga de analizar lo que sucede en la imagen. Si se trata de algo fuera de lo común, suena una alarma para dirigir la atención del técnico del CCTV hacia la imagen. También se conserva un registro de las alarmas. Las imágenes vinculadas a la alarma se almacenan en un ordenador de manera que se puedan recuperar y compartir fácilmente.

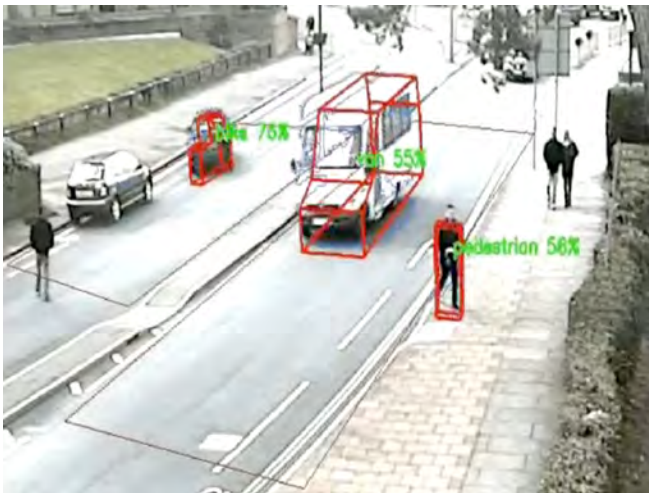
El software de los CCTV inteligentes es capaz de realizar una serie de procesos. Se utiliza principalmente para:

- > identificar objetos que aparecen en imágenes, como vehículos, mediante la identificación de su matrícula, que se cruza con información contenida en una base de datos;
- > identificar el rostro de una persona cuando dicho rostro aparece tras un fondo liso y despejado. Para identificar a la persona se compara la grabación con imágenes almacenadas en bases de datos de individuos conocidos;

- > identificar maletas abandonadas si dicha maleta se encuentra en un espacio vacío.

Aunque los CCTV inteligentes aún no son capaces de realizar las acciones siguientes de manera efectiva, se están desarrollando softwares dedicados a:

- > identificar a personas entre la multitud por medio de su ropa;
- > identificar comportamientos sospechosos o comportamientos poco frecuentes en el tipo de escena que se observa, como por ejemplo merodear con fines delictivos. Los comportamientos de las imágenes se comparan con patrones de comportamiento conocidos que se encuentran almacenados en una base de datos.



No obstante, no todos los sistemas de CCTV inteligentes son iguales. El nivel de “inteligencia” de un determinado sistema depende de la efectividad con la que el software analice la imagen y el proceso que siga una vez compartida. Los sistemas se instalan por diversos motivos, por lo que un determinado sistema de CCTV puede no ser capaz de hacer todo lo señalado anteriormente. Es posible que el propietario del sistema no necesite que realice algunos de esos procesos.

¿Cómo funcionan los CCTV?

Un ordenador conectado al sistema de CCTV inteligente aprende a reconocer determinados tipos de comportamiento público por medio de “algoritmos inteligentes”. Dichos comportamientos se conocen como “desencadenantes”, como, por ejemplo, cuando una persona empuña un arma o permanece quieta en medio de la multitud. Los algoritmos son un conjunto de cálculos que clasifican los datos contenidos en la imagen digital. Los algoritmos inteligentes son aquellos capaces de aprender lo que deben buscar conforme analizan un número creciente de datos.

Los algoritmos inteligentes en sistemas de CCTV inteligentes están diseñados para imitar el funcionamiento del ojo y el cerebro humanos. El software fragmenta la imagen en partes minúsculas conocidas como “píxeles”. Si tiene una cámara digital o un smartphone seguro que reconoce el término “píxel”. Si una cámara digital tiene “8 megapíxeles” significa que cada imagen que captura contiene hasta 8 millones de píxeles.

Así pues, el algoritmo es capaz de calcular el grado de movimiento de cada píxel de la imagen, lo cual permite al software identificar las zonas activas de la escena. A partir de ahí aprende a reconocer los patrones de movimiento de una imagen. Así, el sistema puede identificar y clasificar sucesos de acuerdo a patrones conocidos. Por ejemplo, el software es capaz de diferenciar entre espectadores pasivos e hinchas que no paran de saltar en un partido de fútbol.

5.2 ¿Cómo se utilizan los CCTV inteligentes?

Los sistemas de CCTV inteligentes son productos comerciales vendidos por empresas de seguridad y tecnología de defensa. Existen muchos sistemas disponibles. En la actualidad, los organismos de transportes, como organismos ferroviarios, portuarios, de aeropuertos o autopistas, así como organismos locales y la policía son los principales usuarios institucionales de los CCTV inteligentes.

A finales de 2012, el departamento de policía de Budapest comenzó a utilizar cámaras de CCTV inteligentes para observar carriles bus. La policía puede utilizar las imágenes de manera legal siempre y cuando no se grabe a los pasajeros y se informe debidamente al público. Las cámaras de reconocimiento facial se llevan utilizando en el aeropuerto de Zúrich desde 2003. Ese momento, era la primera vez que se utilizaba el reconocimiento facial para el control fronterizo. En la actualidad es un sistema permanente.

La Unión Europea ha financiado 16 proyectos independientes para el desarrollo de algoritmos y funciones de sistemas de CCTV inteligentes. Actualmente todavía se están desarrollando y mejorando usos más complejos, como el reconocimiento de comportamientos sospechosos o rostros entre la multitud. Su uso aún no está muy extendido, además, se están probando nuevos sistemas constantemente. Por ejemplo, los organismos de transporte de Roma, Londres, París, Bruselas, Milán y Praga han participado recientemente en pruebas de un sistema

inteligente de vigilancia de pasajeros que utiliza CCTV inteligentes. Este sistema alerta a los técnicos de paquetes sospechosos, movimientos anormales de los pasajeros o comportamientos poco frecuentes. Aún no se utilizan puesto que en este momento continúan en fase de pruebas.

Seguramente el uso más habitual de los CCTV inteligentes es el reconocimiento automático de matrículas. Mediante la imagen digital de la matrícula de un coche se puede cruzar la información con bases de datos gubernamentales de propietarios de coches, de seguros o policiales.



Es sencillo identificar al propietario del coche y la dirección registrada del vehículo, por lo que las cámaras ANPR son capaces de ubicar a un determinado individuo en el tiempo y el espacio.

El sistema se puede utilizar para identificar vehículos robados o aquellos que circulan sin seguro o sin haber abonado las tasas, o bien aquellos que sobrepasan los límites de velocidad.

Una cuestión que se plantea es si los diferentes tipos de delitos merecen el mismo nivel de vigilancia, ¿deberían reservarse las CCTV inteligentes para los delitos más graves? En Europa existen diferentes puntos de vista sobre este asunto. En Alemania, por ejemplo, en 2008 el tribunal constitucional restringió el uso de sistemas de ANPR por parte de la policía en zonas privadas.

Polémica en torno a los CCTV inteligentes: cámaras ANPR en Birmingham, Reino Unido

En 2011, la policía británica de Birmingham, Reino Unido, tuvo que retirar las cámaras ANPR de tres zonas de la ciudad con población musulmana. Las cámaras se financiaron con los fondos de un programa antiterrorista llamado "Project Champion", pero se justificaron por motivos de seguridad ante la opinión pública. Los dirigentes de la comunidad y miembros locales del parlamento se opusieron con firmeza a estas cámaras y las relaciones de la comunidad se deterioraron. Se instalaron doscientas cámaras que nunca llegaron a conectarse. Sesenta y cuatro de esas cámaras estaban escondidas y se instalaron sin consultar a la opinión pública. Al final, parte de las cámaras se destruyó y la otra parte se destinó a otras fuerzas policiales del Reino Unido. El fracaso del proyecto y la pérdida de cámaras costó a la policía 300.000£ (351.414€).

El tribunal hizo hincapié en que las fuerzas policiales solo podían conservar datos digitales obtenidos por medio de cámaras ANPR si se realizaban inspecciones inmediatas de las bases de datos y se actuaba en base a las mismas. Los sistemas ANPR también se utilizan para cobrar los peajes, pero este punto también genera controversia puesto que existen otros medios menos basados en la vigilancia para ello. En Gran Bretaña, los ANPR también se utilizan para cobrar los peajes de Londres, pero estos se integran en las estrategias para mantener el orden a nivel local y nacional. Desde 2010, se han instalado 5.000 cámaras ANPR en el Reino Unido; el centro de datos nacional de la policía procesa entre 10 y 14 millones de registros ANPR al día.

5.3 Mejoras en la seguridad

Los CCTV inteligentes pueden mejorar la seguridad en los siguientes sentidos:

1. Es más fácil detectar problemas de seguridad en el momento en el que surgen:
 - > El sistema detecta cualquier cosa fuera de lo normal y avisa al técnico del CCTV con una alarma. Esto facilita la interpretación de las imágenes por parte del técnico.
 - > Las alarmas ayudan al técnico a tomar decisiones más eficientes y más rápidas sobre si deben o no tomarse medidas para abordar un problema de seguridad.

- > Los algoritmos del sistema en algunas ocasiones captan detalles que un técnico podría no ver. Esto se debe a que tienen la capacidad de manejar grandes volúmenes de información.

2. Reducen el miedo ante posibles delitos y el grado de intromisión:

- > Cuando una tecnología de seguridad es eficaz, los ciudadanos se sienten más seguros porque saben que un sistema de CCTV inteligente captará rápidamente cualquier cosa fuera de lo común que ocurra a su alrededor.
- > Las cámaras CCTV inteligentes digitales captan muchos más detalles que las cámaras CCTV tradicionales. Esto significa que hacen falta muchas menos cámaras para vigilar un espacio. Como resultado, la vigilancia de los CCTV inteligentes resulta menos molesta por la menor presencia de cámaras.
- > El nivel de privacidad mejora puesto que es posible oscurecer ciertas partes de las imágenes, como las vistas de propiedades privadas, de forma que el técnico no las vea.

5.4 Problemática

Los CCTV inteligentes plantean ciertas pegadas que deben tenerse en cuenta:

1. Los algoritmos de CCTV inteligentes que se utilizan hoy en día presentan una serie de fallos. Estos fallos pueden resultar en una "falsa alarma"

que identifique por error un incidente de seguridad. Esto puede incluir confundir a una persona inocente con un sospechoso. Los fallos actuales son:

- > Solo identifican de forma fiable ciertos tipos de objetos, como el número de una matrícula o una bolsa desatendida en un lugar vacío.
- > Las cámaras tienen más dificultades para identificar qué está sucediendo en una multitud.
- > Los delitos disimulados, como el robo de carteras o los robos en tiendas, son difíciles de detectar.
- > Los algoritmos son susceptibles de estar sesgados puesto que los programan humanos para identificar lo que ellos consideran “fuera de lo normal”. Existe el riesgo de que los sistemas, ya sea de forma deliberada o accidental, estén programados para centrarse en minorías de un modo discriminatorio.
- > Si, en el futuro, el uso de CCTV inteligentes fuese conocido por potenciales criminales, alguien podría evitar ser vigilado tan solo con cambiarse de ropa, puesto que los algoritmos funcionan mediante el reconocimiento de la ropa que llevan los sospechosos.
- > El nivel elevado de falsas alarmas que se envían a los técnicos humanos podría hacer que perdiesen la confianza en el sistema e hiciesen caso omiso de lo que les comunican.

2. Las cámaras CCTV inteligentes son más potentes y más pequeñas:

- > Pueden captar más información y por eso son potencialmente más invasivas en términos de privacidad. Esto se debe a una mayor probabilidad de captar y analizar actividades de personas inocentes. Para contrarrestar esto, un CCTV inteligente siempre debería aplicarse de un modo muy limitado para dirigirse a una amenaza muy específica.
- > Las cámaras son más difíciles de ver, lo que dificulta que los ciudadanos sepan que los está vigilando un CCTV inteligente. Por lo tanto, también es más difícil para los ciudadanos evitar o cuestionar la vigilancia.
- > Si los ciudadanos son conscientes de que su conducta en lugares públicos está vigilada por esta combinación de software y personas, eso podría afectar a la libertad de expresión y a su dignidad.

3. Todavía necesitan personas que manejen los sistemas. Esto significa que:

- > Es necesario que una persona interprete las imágenes y confirme que existe un problema real. Si bien el sistema puede identificar comportamientos fuera de lo común, no puede explicar cuál es la causa de ese comportamiento.
- > Es necesario que las autoridades regulen en detalle los tipos de búsqueda que se llevan a cabo para evitar que los datos se usen con otros fines.



**Tiene que haber
transparencia sobre las
razones por las que se**

instalan sistemas de CCTV inteligentes. Los ciudadanos deberían tener derecho a contactar con el responsable del sistema para informarse sobre su uso. Deben sentir que la cámara está ahí por una buena razón y deben poder confiar en su uso.

Chris Tomilnson, Asesor de Seguridad Independiente

6 Cibervigilancia mediante inspección profunda de paquetes

Mientras estaba sentada en la cafetería del aeropuerto, Aisha se preguntaba qué pasaría con el e-mail que le había enviado a su compañero en su viaje a través de la red. No sería raro que se hubiese encontrado con una técnica de cibervigilancia llamada “inspección profunda de paquetes”.

Los proveedores de servicios de internet, operadores de redes de telecomunicaciones y empresas de telecomunicaciones siempre han tenido la capacidad de vigilar sus redes. Saber quién se comunica con quién, qué páginas se visitan y los servicios que se utilizan son datos útiles a efectos de facturación, gestión de red y de actividades de marketing de estas compañías. No obstante, la técnica denominada “inspección profunda de paquetes” (DPI por sus siglas en inglés) permite a las compañías, servicios de inteligencia y gobiernos leer el contenido de las comunicaciones enviadas a través de internet. Para establecer un paralelismo, en el servicio de correo postal, la DPI sería el equivalente a abrir las cartas, leerlas y, en algunas ocasiones, cambiarlas, borrarlas o no entregarlas. La DPI es capaz de controlar cada uno de los aspectos de las comunicaciones digitales. Esto abarca desde la información que usted lee online, las páginas web que visita, los vídeos que ve y las palabras que busca, hasta con quién se comunica por e-mail, mensajería instantánea o redes sociales. Las aplicaciones DPI funcionan detectando y determinando la manera en la que los mensajes viajan a través de una red. Abren y analizan los mensajes en tránsito, identificando aquellos que podrían suponer un riesgo especial. No es necesario ser sospechoso para ser susceptible de una DPI; la DPI intercepta y lee todos los mensajes que viajan a través de la red de un proveedor de servicios de internet.



6.1 ¿Por qué se desarrollo la inspección profunda de paquetes?

La DPI se desarrolló en primera instancia para detectar virus y malware que pudieran dañar redes informáticas. Hoy en día, al usar la DPI para analizar el contenido de mensajes en tránsito, no solo se pueden interceptar los virus, sino que también permite detectar actividades dañinas, peligrosas o delictivas que tienen lugar a través de internet.

Funcionamiento de la inspección profunda de paquetes

Cuando envía o recibe información a través de internet, ésta atraviesa un proceso muy complejo y pasa por múltiples ordenadores.

Los ordenadores conectados a través de la World Wide Web desglosan la información que usted envía y la reciben en pedazos más pequeños llamados “paquetes”. Esto se hace para que la información pueda viajar con facilidad por internet. Cuando los paquetes llegan a su destino, se reúnen, como si de un rompecabezas se tratase, para formar el mensaje. Cada paquete tiene una etiqueta que se llama “encabezado” y describe qué es el paquete, quién lo envía y adónde va, igual que una carta en el sistema de correos. Dentro del paquete se encuentra el contenido del mensaje, que se llama “carga útil”.

Cada paquete tiene varias capas y cada una de ellas contiene información distinta sobre el mensaje. Las capas se encajan una dentro de otra, como si fueran muñecas rusas. Los proveedores de servicios de internet necesitan inspeccionar algunos de los paquetes de mensajes para poder entregarlos. En la mayoría de los casos, solo necesitan consultar los encabezados (el exterior del sobre) y no la carga útil (el interior del sobre) para garantizar que un mensaje se entrega. Este proceso se conoce como “inspección superficial de paquetes”. La inspección profunda de paquetes, por el contrario, conlleva inspeccionar todos los paquetes de un mensaje y analizar no solo los encabezados, sino también la carga útil.

Los paquetes se inspeccionan utilizando algoritmos informáticos que escanean los mensajes en busca de cierto tipo de datos. Al abordar el tema de los circuitos cerrados de televisión (CCTV) inteligentes, hemos descrito los algoritmos como series de cálculos que clasifican y analizan datos. En la DPI también se utilizan, aunque de un modo distinto.

En la inspección profunda de paquetes, un algoritmo puede programarse para buscar “palabras clave” concretas, como cuando hacemos búsquedas en buscadores web. Los tipos de datos que se buscan dependen de quién realice la búsqueda y con qué fin. Las palabras clave utilizadas pueden estar relacionadas con actividades delictivas o sospechosas, con un nuevo virus informático que está circulando por la red o incluso con saber si se ha adquirido o no un producto concreto.

La inspección profunda de paquetes tiene lugar en los “routers”. Un router es un ordenador que redirige los mensajes a través de las distintas redes que conforman internet. Todos los equipos que contienen la tecnología que lleva a cabo la inspección profunda de paquetes son propiedad de las compañías de internet. Dichas compañías pueden controlar el funcionamiento local, regional, nacional o internacional de internet. Son estas compañías las que poseen los routers que cuentan con la tecnología pionera que realiza la inspección profunda de paquetes. Por supuesto, las compañías quieren utilizar esta tecnología para sus propios fines, pero también pueden lucrarse de ella vendiendo esta innovación a terceros. Otras empresas, como las corporaciones del sector

de defensa, también han desarrollado la tecnología DPI y quieren hacer lo mismo. Hoy en día, existe un mercado para la tecnología DPI.

6.2 ¿Cómo se utiliza la inspección profunda de paquetes?

En Europa, el uso legal de los sistemas DPI está muy limitado. Bajo las leyes actuales se puede utilizar para “filtrar” el tráfico de internet en la búsqueda de virus. Además puede ayudar a las empresas de Internet en la gestión del flujo de tráfico de sus redes. Pero la tecnología DPI también es capaz de analizar toda el contenido de las comunicaciones en línea. Cuando se utiliza de esta manera se pueden detectar delitos muy específicos, tales como la distribución de pornografía infantil. Pero este uso de la tecnología DPI es jurídicamente controvertido ya que no existe una ley detallada

que lo regule. Esta situación se debe a que las leyes europeas sobre tecnologías de la comunicación se elaboraron en un momento en que la DPI no existía. El Tribunal de Justicia Europeo y el Supervisor Europeo de Protección de Datos han interpretado las leyes en referencia a la “filtración” limitada de las comunicaciones en línea. Deben desarrollarse nuevas leyes que regulen de forma detallada los usos permitidos de la tecnología DPI.

Como resultado la DPI no puede utilizarse legalmente para monitorizar las comunicaciones generales, para detectar infracciones en los derechos de autor, para bloquear contenido políticamente sensible o para dirigir publicidad, aunque sea una tecnología capaz de hacer todas estas cosas. Incluso en los casos en los que su uso está permitido no puede utilizarse de forma indiscriminada. La Ley de Protección de Datos Europea y la Carta de Derechos Fundamentales de la Unión Europea protegen la confidencialidad de las comunicaciones. La tecnología DPI violaría el Convenio Europeo de Derechos Humanos porque se comprende vigilancia indirecta masiva sin orden judicial: puede leer cada bit de información que se envía y recibe entre ordenadores. El panorama es muy diferente en EEUU, allí no existe regulación y muchas empresas la utilizan para orientar la publicidad. Si usted tiene una dirección de correo electrónico Gmail o Yahoo sus mensajes seguramente viajarán vía Estados Unidos y serán objeto de la DPI. Según se reveló en el verano de 2013 la Agencia de Seguridad Nacional de Estados Unidos (NSA) y el Cuartel General de Comunicaciones del Reino Unido (GCHQ) habrían utilizado supuestamente DPI en los programas de vigilancia masiva (Upstream y Tempora respectivamente).

La manera de detectar, limitar o controlar la DPI es un terreno pantanoso. Se está regulando de forma desesperada en un intento de ponerse al día con lo que la tecnología es capaz de hacer. Es muy complicado saber en qué medida tiene lugar la DPI. Cualquier mensaje que usted envíe o reciba puede viajar por todo el mundo antes de llegar a su destino. Podría haber sido objeto de una DPI llevada a cabo por un proveedor de servicios de internet o por los servicios de seguridad de un gobierno en un número indeterminado de países. Es casi imposible saberlo. La DPI genera información adicional que los proveedores de servicios de internet y los gobiernos pueden a su vez compartir, por lo que es difícil saber qué ocurre con los resultados de las búsquedas DPI. Sin regulación, esto es como una ciudad sin ley en la que

compañías y gobiernos podrían estar beneficiándose de este vacío legal.

Lo que sí podemos afirmar es que muchas instituciones de diversa índole utilizan la DPI en todo el mundo. Proveedores de servicios de internet, compañías de marketing, policía y organismos de seguridad del gobierno la han utilizado en diversos momentos. Existen algunos usos documentados de DPI -aparte de las vastas actividades de vigilancia de las agencias de seguridad que Estados Unidos reveló el año pasado-, algunos son con fines comerciales y otros se refieren a la seguridad pública y nacional.

6.2.1 Usos comerciales

Seguridad y gestión de la red: los mensajes se inspeccionan para garantizar que no contienen errores o virus, también se suelen filtrar los intercambios de archivos con destinatarios múltiples.

Publicidad comportamental: se basa en la recogida de datos de mensajes sobre las preferencias de una persona. Esto no está permitido en Europa, pero algunos consumidores de Estados Unidos, donde sí está permitido, lo ven con buenos ojos. Les permite acceder a productos y servicios que se ajustan a sus necesidades.

Gestión de derechos digitales: los mensajes se inspeccionan para identificar el intercambio ilegal de archivos y las infracciones de derechos de autor.

Polémica de las inspecciones profundas de paquetes: Phorm y los datos de consumidores del Reino Unido

En 2008, una empresa estadounidense llamada Phorm quiso lanzar un sistema junto con los proveedores de telecomunicaciones del Reino Unido British Telecom, Virgin Media y Talk Talk. Phorm utilizó una DPI para identificar hábitos de navegación web de los usuarios a medida que navegaban por internet. A continuación, analizó los datos y vendió la información a empresas de publicidad. Los proveedores de servicios dijeron a sus usuarios que las medidas estaban dirigidas a combatir los delitos electrónicos, pero no los informaron de que los datos se estaban utilizando con fines publicitarios. British Telecom llevó a cabo pruebas ocultas de esta tecnología y realizó más de 18 millones de interceptaciones. Los consumidores británicos se enteraron y protestaron porque los datos se habían tratado sin su consentimiento. Al final, todos los proveedores de servicios abandonaron la tecnología de Phorm. La Comisión Europea inició entonces acciones legales contra el gobierno británico por permitir el funcionamiento de este servicio. El caso se cerró en enero de 2012, después de que el Reino Unido modificase sus leyes para incluir sanciones por interceptación ilegal de comunicaciones.

6.2.2 Usos relativos a la seguridad pública y nacional

Supervisión de actividades delictivas por parte del gobierno: la inspección profunda de paquetes se propone como herramienta en la investigación de delitos muy concretos, aunque es polémica desde un punto de vista legal. Estos delitos incluyen:

- > delitos contra sistemas informáticos o cometidos mediante un ordenador (ej. distribución de pornografía infantil);
- > delitos en los que se ha compartido información

racista, o en los que se han realizado amenazas de índole racista;

- > delitos que incitan o están dirigidos a la organización de actos terroristas;
- > delitos en los que se comparte información que aprueba el genocidio o los crímenes contra la humanidad.

Censura: se ha especulado con que la DPI se ha utilizado para engañar a oponentes políticos en regímenes totalitarios de todo el mundo. La compañía estadounidense de defensa NARUS, filial de Boeing, vendió la DPI a Libia, que la utilizó para acallar a los disidentes durante la primavera árabe. Por el contrario, en los albores de la primavera árabe, el Reino Unido limitó la venta de tecnología DPI a Egipto, Bahrein y Libia mediante la revocación de licencias de exportación. Aunque no está claro quién suministra la tecnología que se está usando, Irán utiliza la DPI no solo para interceptar y censurar la información a la que los ciudadanos pueden acceder online, sino también para alterar el contenido online con el objeto de desinformar. China utiliza la DPI de una forma similar. La pregunta sigue siendo si la censura en internet también tiene lugar en Europa.

6.3 Mejoras en la seguridad

La Inspección Profunda de Paquetes puede mejorar la seguridad de la información y la lucha contra la delincuencia mediante la identificación y bloqueo de mensajes dañinos, perjudiciales o penados según lo descrito en el apartado anterior 6.2.2.

Aunque la DPI no puede impedir delitos graves, sí permite su detección y posibilita la presentación de pruebas en una investigación. También permite prevenir la propagación de virus informáticos y otras formas de delitos cibernéticos.

6.4 Problemática

La inspección profunda de paquetes plantea los siguientes problemas.

1. La DPI puede verlo todo.
- > Tiene la capacidad de analizar todos los mensajes y datos sensibles que contienen mientras viajan, lo que significa que con la DPI

- las comunicaciones electrónicas ya no son privadas.
 - > Saber que las comunicaciones ya no son privadas podría tener un “efecto amedrantador”, ya que la gente podría tener miedo de comunicarse abiertamente y expresarse libremente.
 - > El uso de la DPI debe regularse en detalle puesto que se trata de una herramienta muy potente.
2. Las capacidades tecnológicas van por delante de la regulación.
- > No existen disposiciones legales claras respecto a para qué se puede o no se puede utilizar la DPI.
 - > En la práctica, el uso de la DPI depende de la ética de quien la esté utilizando. Puede utilizarse para cualquier cosa, desde la opresión política a la detección de virus informáticos.
 - > En países en los que el gobierno central y los proveedores nacionales de comunicaciones están estrechamente relacionados, la información podría compartirse de forma que el
- Estado tenga acceso a todas las comunicaciones de los ciudadanos.
3. Es complicado saber exactamente quién y dónde se está utilizando la DPI.
- > Las disposiciones legales tendrían que ser las mismas para todo el mundo.
 - > El “órgano regulador de la DPI” debería ser un organismo internacional con competencia para castigar a los infractores.
4. La eficacia de la DPI es cuestionable:
- > Los ordenadores identifican los mensajes potencialmente peligrosos pero pueden cometer interpretaciones incorrectas y personas inocentes convertirse en sospechosos.
 - > Algunos expertos han cuestionado la eficacia de la DPI en la búsqueda de material ilegal.



Muchas de las compañías que utilizan la DPI se encuentran fuera de Europa, pero analizan datos de ciudadanos europeos. Por ello, no se les puede prohibir

que lo hagan.

Eva Schlehahn, Autoridad Independiente para la Protección de la Privacidad, Schleswig Holstein

7 Sistemas de localización y seguimiento a través de smartphones

Cuando Aisha encendió su smartphone, se dio cuenta de que la pantalla de inicio reflejaba que su ubicación había cambiado. Estaba segura de que esto tendría una explicación obvia. De hecho, todos los móviles necesitan conocer su ubicación para funcionar. Los smartphones, sin embargo, llevan esto mucho más allá.

Los nuevos móviles inteligentes han sustituido a la navaja suiza como paradigma de herramienta todo-en-uno y al mismo tiempo juguete. Hay casi 5.000 millones de móviles operativos en el mundo. De media, en Europa, salimos casi a 1,3 móviles por persona. Es un número enorme si tenemos en cuenta que los teléfonos móviles no llegaron hasta principios de los años 90.

7.1 ¿Por qué se desarrollaron los sistemas de localización y seguimiento a través de smartphones?

Los smartphones son una evolución reciente. Su gran popularidad se debe al hecho de que son capaces de hacer muchas cosas distintas, además de funcionar como un teléfono normal. De hecho, los smartphones se parecen más a un ordenador de bolsillo que tiene capacidad para hacer llamadas. Al igual que un ordenador de sobremesa o un portátil, cada tipo de smartphone tiene su propio sistema operativo, que permite instalar aplicaciones de e-mail, mensajería y navegación web. Los smartphones utilizan aplicaciones de software que permiten ofrecer servicios como juegos, mapas y noticias online. También cuentan con cámaras digitales y de vídeo, reproductores multimedia portátiles y pantallas táctiles, más grandes y con más colores.

La historia de los teléfonos móviles se remonta a la Segunda Guerra Mundial. Un teléfono móvil sencillo es básicamente una radio inalámbrica que puede enviar y recibir mensajes. Las primeras radios inalámbricas, los "walkie talkies", se utilizaron por

primera vez para ayudar a los soldados a mantenerse en contacto con la primera línea de combate. En la década de 1970 y 1980, las innovaciones en microprocesadores posibilitaron la aparición de los primeros microteléfonos. El primer microteléfono original tenía el tamaño y peso de un ladrillo y la batería solo duraba 20 minutos. ¡Cómo cambian los tiempos! De la década de 1980 en adelante, una creciente red de antenas de telefonía móvil mejoró la cobertura móvil tanto a nivel local como para distancias más largas. Seguramente recordarán como estas antenas se multiplicaron de forma muy significativa a mediados de los años 90. Hubo un gran debate sobre la colocación de estas antenas de telefonía antiestéticas que además despertaban preocupación sobre el aumento nocivo del nivel de radiación.



Las antenas de telefonía desempeñan un papel crucial para la localización de teléfonos móviles. Una antena de teléfono cubre una zona geográfica determinada. Para poder conectarse a la red, realizar llamadas y enviar mensajes, todos los teléfonos móviles deben registrarse en la antena de telefonía más cercana. La antena a la que el teléfono se conecta registra siempre la ubicación de ese teléfono. Si la persona que utiliza el teléfono se mueve al rango de acción de otra antena, el teléfono se registra allí. De este modo, los proveedores de telecomunicaciones pueden seguir la trayectoria de una persona. La regulación europea actual exige a los proveedores que almacenen esta información por un período de

entre 6 y 24 meses. Los smartphones también se pueden localizar de otras maneras. La persona que utiliza el teléfono puede configurarlo de manera que el teléfono determine su ubicación mediante satélites de posicionamiento global (GPS) o conectándose a redes inalámbricas.

Esto ha conllevado un crecimiento muy importante en la prestación de “servicios basados en la ubicación” para smartphones. Estos servicios normalmente están disponibles en forma de aplicaciones (“apps”) que pueden instalarse en el

terminal. Una app es una herramienta de software que puede llevar a cabo una función o servicio específico. Las apps basadas en la ubicación permiten al usuario obtener información sobre restaurantes o tiendas cercanas, o sobre cuáles de sus amigos están cerca. También existen juegos basados en la ubicación. Los servicios basados en la ubicación serán probablemente una de las funciones de smartphones que más crecerá en los próximos años.

Funcionamiento de los sistemas de localización y seguimiento a través de smartphones

Hoy en día, es posible localizar y realizar el seguimiento tanto de móviles normales como de smartphones. Existen tres maneras de localizar un teléfono móvil: a través de las antenas de telefonía móvil, mediante sistemas GPS o mediante redes inalámbricas. La primera es aplicable a cualquier teléfono móvil, mientras que las otras dos solo se pueden utilizar con smartphones.

Antenas de telefonía móvil: todos los teléfonos se registran en la antena de telefonía más cercana para poder enviar y recibir llamadas, mensajes y correos electrónicos a través de la red móvil. Cada teléfono cuenta con un número de referencia único que relaciona el teléfono con una cuenta de una compañía telefónica y, por extensión, con un usuario. Esto permite generar la factura de teléfono. Si los servicios de seguridad o las fuerzas del orden quieren seguir los movimientos de una persona concreta en un periodo determinado, pueden solicitar la información de antenas de telefonía a las compañías telefónicas. Los registros de antenas de telefonía revelan si el teléfono de esa persona se encontraba en una zona geográfica determinada. Cuando esta operación se repite para todas las de antenas -como regula la UE- es posible realizar el seguimiento de la ubicación de una persona y de sus movimientos.

GPS: los smartphones contienen software y aplicaciones cartográficas que utilizan satélites de posicionamiento global. Cuando la función GPS de un smartphone está activada, el teléfono determina su ubicación en el planeta calculando lo lejos que se encuentra del satélite GPS espacial más cercano. Cuando esta función está desactivada, el teléfono no puede determinar su ubicación por GPS. Sin embargo, esta función puede activarse de forma remota sin ser notificado al usuario, por ejemplo, si tienen una aplicación instalada en su teléfono que le permite su localización en caso de pérdida o robo. Los proveedores de apps recogen esta información de ubicación y algunos de ellos la venden con fines comerciales. Si los servicios de seguridad y fuerzas del orden necesitan seguir los movimientos de una persona concreta, pueden solicitar los datos GPS a las compañías telefónicas.

Redes inalámbricas: los smartphones pueden conectarse a redes inalámbricas que funcionan en una zona determinada. Al conectarse a una red inalámbrica, el teléfono está localizado dentro de los límites de dicha red. Al igual que en el caso anterior, si esta función del teléfono está desactivada, el teléfono no se podrá localizar mediante este sistema. Normalmente, los puntos de acceso wi-fi tienen un rango de 20 metros en el interior y algo mayor en el exterior.

Los servicios basados en la ubicación ofrecen grandes ventajas a los usuarios de smartphones. No obstante, algunos defensores de la privacidad argumentan que el nivel de información que se puede obtener mediante la localización y seguimiento de un smartphone es preocupante. A título de ejemplo, cuando el político ecologista alemán Malte Spitz quiso obtener los registros sobre la ubicación de su teléfono durante seis meses, tuvo que llevar a la compañía telefónica a juicio para poder recibir la información. Cuando por fin recibió los datos, le parecieron una secuencia de números y letras carente de sentido. Sin embargo, cuando Malte pidió a un experto en estadística que analizase los datos, obtuvo un reflejo detallado de su vida. En colaboración con el periódico Die Zeit, Malte creó una animación que mostraba con exactitud dónde había estado durante esos seis meses. Malte empezó a preocuparse sobre el nivel de detalle que podía obtenerse sobre su vida, sobre todo si la información sobre su ubicación se combinaba con la información de redes sociales como Twitter o Facebook.

En un caso reciente del Tribunal Supremo de Estados Unidos, Estados Unidos contra Jones, el juez dictaminó que los datos GPS permitían revelar visitas que eran “sin lugar a dudas privadas”, como “visitas al psiquiatra, al cirujano plástico, a clínicas abortistas, a centros de tratamiento de SIDA, a clubes de strip-tease, a bufetes especializados en defensa penal, a moteles por horas, a reuniones sindicales, a la mezquita, sinagoga o iglesia, a un bar gay, etc.”

7.2 ¿Cómo se utilizan los sistemas de localización y seguimiento a través de smartphones?

Los datos relativos a la ubicación de smartphones tienen tanto aplicaciones comerciales como otras relativas a la seguridad.

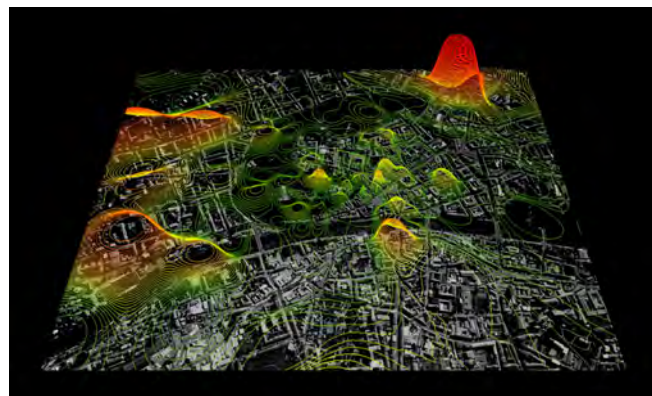
7.2.1 Usos comerciales

> **Gestión de facturas telefónicas:** las compañías

telefónicas necesitan datos relativos a la ubicación así como el número de identificación del teléfono para generar una factura. Las compañías también utilizan esos datos para diseñar tarifas de uso de servicios móviles adaptadas a las necesidades de sus clientes.

> **Marketing dirigido:** las marcas de software que producen apps, como Twitter, Angry Birds o FourSquare, recogen datos de ubicación y otros datos de contacto de los teléfonos y se los venden a empresas de publicidad. Las empresas de publicidad utilizan esos datos para diseñar anuncios de productos para los espacios que saben que frecuentan los distintos tipos de consumidores. Sin ir más lejos, Angry Birds se ha descargado mil millones de veces en todo el mundo. Sus usuarios se sorprendieron al saber que los creadores finlandeses, Rovio Entertainment Ltd, recogían y vendían regularmente datos sobre la ubicación de los jugadores. El cincuenta por ciento de las apps recogen datos de ubicación incluso si las apps no necesitan esa información para funcionar.

> **Urbanismo:** los datos de ubicación se pueden utilizar para determinar el uso de los distintos espacios urbanos. Puesto que en las zonas urbanas hay muchas más antenas de telefonía móvil que en las zonas rurales, los teléfonos son mucho más fáciles de localizar. Esta imagen tan extraña es un mapa del uso de teléfonos móviles en Graz, Austria. Los investigadores del Massachusetts Institute of Technology realizaron el seguimiento anónimo de teléfonos móviles para mostrar una imagen de por dónde se mueven los ciudadanos de Graz. Su objetivo era informar a urbanistas y gestores de transportes sobre el uso de la ciudad.



7.2.2 Usos relativos a la seguridad pública y nacional

- > **Búsqueda de personas desaparecidas y heridas:** en Estados Unidos y Canadá, un servicio denominado E-911 obliga, amparado por la ley, al uso del GPS en todos los teléfonos para que éstos (y sus usuarios) puedan ser localizados en caso de emergencia. En Europa, se realizan en torno a 180 millones de llamadas de emergencia al año. Entre el sesenta y el setenta por ciento de ellas se hacen desde teléfonos móviles. El teléfono comunica los datos sobre su ubicación al número Europeo de emergencias 112. A diferencia de estadounidenses y canadienses, los europeos no tienen la obligación de tener el GPS activado en su móvil en todo momento.
- > **Seguimiento de los movimientos de sospechosos:** los servicios de seguridad encargados de la aplicación de la ley pueden tener acceso a datos basados en la ubicación si les solicitan dichos datos a las compañías telefónicas. Hoy en día en Europa, este tipo de solicitudes se rigen por la ley. Al recibir una solicitud de este tipo, las compañías tienen la obligación de facilitar a los servicios de seguridad cualquier dato relativo a un sospechoso. Los servicios de seguridad también cuentan con otros métodos para el seguimiento de teléfonos que se pueden aplicar de forma específica a personas concretas.
- > **Seguimiento de familiares:** los ciudadanos también pueden beneficiarse de los servicios basados en la ubicación. Muchos padres estarán familiarizados con productos de seguimiento de teléfonos móviles que les permiten saber dónde están sus hijos en todo momento, por ejemplo.

Polémica de los sistemas de localización y seguimiento a través de smartphones

A raíz de las protestas del movimiento "Occupy" en Nueva York, Twitter se vio obligada a facilitar datos de ubicación al gobierno estadounidense para identificar a los manifestantes. Hace poco, Twitter ha lanzado un nuevo servicio llamado "Please Don't Stalk Me" ("Por favor no me sigas"). Esto permite a los usuarios trucar los datos de ubicación asociados a sus tweets. La app "Please Don't Stalk Me" permite a los usuarios escoger un punto del planeta, a través de Google Maps, y a continuación asociar esa información de ubicación falsa a sus tweets. Otras apps, como "My Fake Location", "Fake GPS Location" y "GPS Cheat" funcionan igual.

7.3 Mejoras en la seguridad

Los sistemas de localización y seguimiento a través de smartphones contribuyen al aumento de la seguridad de una serie de formas distintas:

1. Permiten encontrar y prestar ayuda a personas en situaciones de peligro.
2. Permiten a las familias vigilar a sus adultos vulnerables o niños.
3. La policía y las fuerzas del orden pueden utilizar datos de ubicación para determinar la presencia de individuos en la escena de un crimen o para descartarlos como sospechosos. También pueden seguir y vigilar a un sospechoso en el transcurso de una investigación.

7.4 Problemática

Los sistemas de localización y seguimiento a través de smartphones plantean los siguientes problemas en cuanto a la privacidad, la regulación y los derechos humanos:

1. Los usuarios no tienen un control total sobre la información que transmiten sus smartphones. Esto es especialmente delicado en el caso de los usuarios más vulnerables, como testigos protegidos, que pueden no querer compartir los datos sobre su ubicación, pero que necesitan un teléfono móvil. Algunos teléfonos, como los iPhones de Apple, almacenan de forma automática datos de ubicación en el teléfono y no es posible desactivar esta función.
2. Algunas apps recogen datos de ubicación aunque la app no los necesite para funcionar. Mientras no exista una presión pública firme, las compañías no parecen muy proclives a facilitar a los consumidores un mayor control sobre estos datos.
3. Muchos diseñadores de apps se encuentran fuera de Europa por lo que no están sujetos a los reglamentos europeos de protección de datos. Por ello, es difícil para la UE hacer hincapié en que las apps deberían respetar la privacidad. No obstante, una modificación reciente de la directiva sobre la privacidad en las comunicaciones electrónicas insiste en que los usuarios deben poder dar su consentimiento al tratamiento de sus datos por parte de apps de smartphones, independientemente de dónde tenga su sede la app.
4. Al igual que ocurre con la inspección profunda de paquetes, en países en los que el gobierno central y los proveedores de telefonía móvil están estrechamente relacionados, la información podría compartirse de forma que el Estado tenga acceso a la ubicación de todos los ciudadanos.
5. Puesto que los datos de ubicación ya se han utilizado para identificar a manifestantes, este uso tiene un “efecto amedrentador” potencial que podría disuadir a los ciudadanos de manifestarse y ejercer sus derechos democrático



Los sistemas de localización y seguimiento a través de smartphones tienen tanto un efecto capacitador como controlador sobre las personas. Pueden ofrecer muchos servicios que mejoran las relaciones sociales... pero la configuración de la recogida de datos de ubicación no es siempre tan evidente

o tan sencilla de controlar.

Gus Hosein, Privacy International

8 ¿Es la tecnología la única alternativa?

Es probable que a estas alturas usted se esté preguntando si las tecnologías de seguridad son la única solución a los problemas de seguridad. A veces parece que la seguridad consiste solo en el seguimiento y la identificación de sospechosos de entre la población general. Esto es cierto en parte, pero es una realidad incompleta.

Las prioridades europeas en materia de seguridad que hemos analizado nos enseñan que la seguridad es un factor presente en todos los ámbitos de la vida. Estas prioridades incluyen cuestiones de seguridad “clásicas” como los delitos o el terrorismo. Según la información recogida en estas páginas, es posible utilizar nuevas tecnologías de seguridad para encontrar a personas involucradas en ese tipo de actividades. Sin embargo, existen cuestiones subyacentes que son la causa primera de la aparición de estos problemas de seguridad, como por ejemplo la pobreza, conflictos nacionales e internacionales o diferencias políticas y religiosas. Las tecnologías de seguridad no sirven para abordar estas causas originarias.

Las prioridades europeas en materia de seguridad también contemplan crisis o catástrofes como problemas de seguridad. Estas catástrofes pueden ir desde escasez de agua o comida, crisis financieras, propagación de enfermedades, hasta catástrofes naturales: situaciones que ponen a prueba la seguridad humana a nivel global. Una vez más, las tecnologías de seguridad son menos efectivas a la hora de enfrentarse a estos problemas de seguridad más complejos a largo plazo.

Por lo tanto, aunque las tecnologías de seguridad se utilizan para localizar a delincuentes y terroristas y adelantarse a sus próximos movimientos, existen otras soluciones alternativas. Hemos enumerado algunos de ellos a continuación. Tal vez usted tiene sus propias ideas sobre cómo se podría mejorar la seguridad, o tal vez usted piense que el enfoque de seguridad de Europa debe alejarse de la delincuencia y el terrorismo y centrarse en otras prioridades.

8.1 Soluciones locales

- > Fomentar entornos más seguros a través de una mejor iluminación de las calles, la disponibilidad de teléfonos de emergencia públicos y una presencia policial mejorada.
- > Establecer mejores relaciones comunitarias locales con la policía mediante medidas comunitarias de prevención de delitos.
- > Facilitar la gestión local de problemas por parte de grupos comunitarios religiosos o de otra índole con el fin de aumentar la confianza social.
- > Contar con políticas locales de transparencia y rendición de cuentas.
- > Contar con oportunidades de empleo, formación y orientación suficientes para las personas más susceptibles de involucrarse en actividades delictivas.

8.2 Soluciones nacionales o internacionales

- > Fomento de sistemas globales justos de comercio, asistencia y alivio de la deuda.
- > Mejora de las infraestructuras y recursos de respuesta ante catástrofes.
- > Mejora de las infraestructuras de suministro de agua, comunicación e información y abastecimiento de alimentos en las partes del mundo que más lo necesitan.
- > Uso más eficiente de fuentes de energía sostenibles y alternativas.
- > Resolución de problemas de desigualdad y discriminación.

9 Le cedemos la palabra...

Esperamos no haberlo abrumado en exceso con tanta información. La buena noticia es que ha llegado al final del documento y ahora puede tomarse un tiempo para reflexionar sobre estos asuntos.

Hemos descrito las tres tecnologías de seguridad sobre las que se hablará en la cumbre ciudadana. Hemos explicado cómo funcionan, cómo se utilizan, las mejoras que suponen para la seguridad y la problemática que plantean. Asimismo, hemos analizado el contexto en el que se desarrollaron estas tecnologías: una Europa muy preocupada por la seguridad y en la que la seguridad está presente en el día a día. Las cuestiones relativas a vigilancia y privacidad también son importantes por la cantidad de datos personales que se manejan hoy en día en el ámbito de la seguridad. Por último, hemos analizado planteamientos alternativos, no tecnológicos, para garantizar la seguridad en la sociedad.

Ahora le corresponde a usted reflexionar sobre su opinión en relación con estos temas. Si estas tecnologías llegasen a utilizarse de forma rutinaria por motivos de seguridad, ¿hasta qué punto sería aceptable? Tal vez piense que cada una de ellas, a su manera, puede ser efectiva para el aumento de la seguridad y la reducción de delitos. Tal vez también considere que existen otras soluciones alternativas, no tecnológicas, que podrían ser mejores. Tal vez usted piense que deben seguir utilizándose los métodos más tradicionales de la policía y el personal de seguridad en lugar de la vigilancia exhaustiva de la información. Es posible que usted piense que la seguridad no constituye un problema

en realidad y que no deberíamos preocuparnos demasiado sobre eso.

Del mismo modo, puede que usted esté seguro de que estas tecnologías están en buenas manos porque las utilizan instancias gubernamentales obligadas a rendir cuentas. O tal vez tenga dudas sobre si esas autoridades son capaces de utilizar las tecnologías de seguridad de forma competente, ética y en favor de los intereses de todos los miembros de la sociedad.

A lo mejor opina que estas tecnologías no le afectan: después de todo, están dirigidas a otro tipo de personas que han obrado mal y se utilizan en espacios o lugares que usted no frecuenta. Sin embargo, es posible que usted sienta que todos deberíamos interesarnos por este tema en vista de la cantidad de datos que manejan estas tecnologías y de que todo el mundo es un sospechoso potencial. Tal vez se sienta cómodo con el uso actual de las tecnologías de seguridad pero le preocupe el uso que se les pueda dar en el futuro.

Sea como fuere, renunciar a parte de la privacidad en aras de una seguridad adicional no es una decisión sencilla para todo el mundo. El objetivo de SurPRISE es comprender los diferentes puntos de vista de los ciudadanos sobre las nuevas tecnologías de seguridad.

Lo invitamos a asistir a la cumbre ciudadana que tendrá lugar en las próximas semanas. Si quiere más información sobre el proyecto y sus miembros, visite la página web de SurPRISE en <http://surprise-project.eu>.

Información sobre el documento

El presente documento informativo se ha elaborado con el fin de informar a los ciudadanos que participarán en las cumbres ciudadanas organizadas en el marco del Proyecto SurPRISE. La publicación la ha llevado a cabo el Institute of Technology Assessment (Austrian Academy of Sciences, Strohgassee 45/5, A-1030 Vienna) para todos los miembros del consorcio SurPRISE.

El Proyecto SurPRISE está cofinanciado como parte del Séptimo Programa Marco (7PM). SurPRISE se dedica a revisar la relación entre seguridad y privacidad. SurPRISE facilitará datos nuevos sobre la relación entre vigilancia, privacidad y seguridad, tomando los puntos de vista de los ciudadanos europeos como eje principal. Asimismo, explorará opciones de tecnologías de seguridad que atiendan en menor medida contra la privacidad y alternativas de seguridad no orientadas a la vigilancia, con el objeto de fomentar debates mejor informados sobre las políticas de seguridad.

Para más información sobre el proyecto y los miembros de SurPRISE, visite la página web **<http://surprise-project.eu/>**.

La información contenida en el presente documento proviene de informes redactados por los miembros del proyecto SurPRISE, quienes, a su vez, se han basado en investigaciones e informes de científicos, responsables políticos y expertos en tecnología de todo el mundo.

- > Autor: Dr Kirstie Ball, The Open University
- > Consejo Asesor en Materias Científicas:
Dr Monica Areñas, Mr Robin Bayley Professor Colin Bennett, Dr Gloria González Fuster, Dr Ben Hayes, Dr Majtényi László, Mr Jean Marc Suchier, Ms Nina Tranø, Prof Ole Wæver
- > Diseño: Mr Peter Devine, Mr David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University; Mr Jaro Sterbik-Lamina, Institute of Technology Assessment, Austrian Academy of Sciences
- > Imágenes: Mr David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University.
Página 17 © iStockPhoto.com / EdStock,
página 28 © iStockPhoto.com / dpmike,
página 29 © iStockPhoto.com / alexsl,
página 30 Senseable City Lab, Massachusetts Institute of Technology.
- > Patrocinadores de SurPRISE: 7º Programa Marco de la Comisión Europea, proyecto nº 285492
- > Esta publicación se encuentra disponible en: <http://surprise-project.eu>
- > Datos sobre la elaboración del documento: la redacción del presente documento ha corrido a cargo de Kirstie Ball en estrecha colaboración con la Danish Board of Technology Foundation, el consorcio SurPRISE y su Consejo Asesor. El documento se sometió a cuatro revisiones internas, una revisión externa y a continuación se utilizó con carácter experimental en Dinamarca, Hungría y el Reino Unido.

Miembros del Proyecto

- > Institut für Technikfolgen-Abschätzung/Österreichische Akademie der Wissenschaften, Coordinador, Austria (ITA/OEAW)
- > Agencia de Protección de Datos de la Comunidad de Madrid*, España (APDCM)
- > Instituto de Políticas y Bienes Públicos/Agencia Estatal Consejo Superior de Investigaciones Científicas, España (CSIC)
- > Teknologirådet - The Danish Board of Technology Foundation, Dinamarca (DBT)
- > European University Institute, Italia (EUI)
- > Verein für Rechts-und Kriminalsoziologie, Austria (IRKS)
- > Median Opinion and Market Research Limited Company, Hungría (Median)
- > Teknologirådet - The Norwegian Board of Technology, Noruega (NBT)
- > The Open University, Reino Unido (OU)
- > TA-SWISS/Akademien der Wissenschaften Schweiz, Suiza (TA-SWISS)
- > Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein/Alemania (ULD)

* APDCM, la Agencia de Protección de Datos de la Comunidad de Madrid participó en el proyecto SurPRISE como miembro del consorcio hasta el 31 de diciembre 2012.

Como consecuencia de las políticas de austeridad en España, la colaboración con la APDCM finalizó a finales de 2012.

Vigilancia, Privacidad y Seguridad: una evaluación participativa a gran escala de criterios y factores que determinan la aceptación y aceptabilidad de las tecnologías de seguridad en Europa