

Vigilancia, Privacidad y Seguridad

¿CUÁL ES SU OPINIÓN?

surprise
surveillance
privacy
security



Este proyecto ha recibido financiación del Séptimo Programa Marco de la Unión Europea para acciones de investigación, desarrollo tecnológico y demostración en virtud del acuerdo de subvención nº 285492

Índice

1	Bienvenidos a SURPRISE.....	5
2	Resumen	6
3	Vigilancia, privacidad y seguridad	8
3.1	Vigilancia.....	8
3.2	Privacidad y protección de datos: ¿son cuestiones importantes?.....	8
3.3	Seguridad.....	9
4	Cinco tecnologías de seguridad.....	11
5	CCTV inteligentes.....	12
5.1	¿Por qué se desarrollaron los CCTV Inteligentes?	12
5.2	¿Cómo se utilizan los CCTV inteligentes?	13
5.3	Mejoras en la seguridad.....	14
5.4	Problemática	14
6	Drones.....	16
6.1	¿Por qué se desarrollaron los drones?	16
6.2	Cómo se utilizan los drones	17
6.3	Mejoras en la seguridad.....	18
6.4	Problemática	18
7	Cibervigilancia mediante inspección profunda de paquetes	20
7.1	Por qué se desarrollo la inspección profunda de paquetes	21
7.2	¿Cómo se utiliza la inspección profunda de paquetes?.....	21
7.2.1	Usos comerciales.....	22
7.2.2	Usos relativos a la seguridad pública y nacional	22
7.3	Mejoras en la seguridad.....	23
7.4	Problemática	23
8	Sistemas de localización y seguimiento a través de smartphones	24
8.1	¿Por qué se desarrollaron los sistemas de localización y seguimiento a través de smartphones?	24
8.2	¿Cómo se utilizan los sistemas de localización y seguimiento a través de smartphones?.....	26
8.2.1	Usos comerciales.....	26
8.2.2	Usos relativos a la seguridad pública y nacional	26
8.3	Mejoras en la seguridad.....	27
8.4	Problemática	27
9	Biometría.....	28
9.1	¿Por qué se desarrolló la biometría?	28
9.2	Cómo se utiliza la biometría.....	28
9.3	Mejoras en la seguridad.....	30
9.4	Problemática	30
10	¿La tecnología basada en la vigilancia es la única alternativa?	32
10.1	Medidas de seguridad alternativas: a nivel global.....	32
10.2	Medidas de seguridad alternativas: a nivel local.....	33
11	Le cedemos la palabra.....	35
	Información sobre el documento	36
	Miembros del Proyecto	37

1 Bienvenidos a

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 reunión ciudadana sobre SurPRISE podrá compartir su punto de

SURPRISE

vista acerca de las nuevas tecnologías de seguridad con otros ciudadanos. SurPRISE recopila las opiniones de los ciudadanos con respecto a nuevas tecnologías de seguridad en nueve países europeos: Alemania, Austria, Dinamarca, España, Hungría, Italia, Noruega, el Reino Unido y Suiza.

El presente folleto incluye información básica sobre aquellas cuestiones que se tratarán en España el encuentro ciudadano de SurPRISE en Junio 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.

Su participación en la reunión 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.

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!

2 Resumen

Casi nadie podría imaginarse la vida sin smartphones, tarjetas de crédito o internet. Sin embargo, quizá no hayan caído en la cuenta en que este tipo de tecnologías genera distintos tipos de registros electrónicos. Dichos registros 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 operadores de telefonía y servicios de internet. La legislación europea dispone que dicha información se puede almacenar desde un mínimo de seis meses hasta dos años. Por tanto, es posible identificar, seguir y localizar a la mayoría de personas en diferentes momentos de sus vidas.

El tipo de tecnología que acabamos de describir y la información que recaba también puede resultarnos beneficiosa a nosotros mismos y a los demás. 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 han 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 bienes 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 comentan delitos. Puesto que este tipo de tecnologías utilizan la información en dicho 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.

Estas tecnologías analizan la información generada por parte de los ciudadanos durante su día a día. Por ejemplo, utilizan información obtenida de teléfonos móviles, internet y tecnologías "inteligentes" como los CCTV digitales con el fin de identificar a delincuentes y terroristas, a veces incluso antes de que comentan un delito.

En el presente folleto examinaremos en profundidad cinco 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.
- **Drones "civiles":** los drones civiles son vehículos aéreos no tripulados (VANT o UAV, por sus siglas en inglés) destinados a aplicaciones no militares. Pueden utilizarse en un gran número de actividades de vigilancia. Se pueden instalar cámaras y otro tipo de sensores adicionales en los drones, por lo que se podrían considerar versiones móviles de las cámaras de los CCTV.
- **Cibervigilancia mediante inspección profunda de paquetes:** utilizan dispositivos de hardware y un software especial. Toda la información y los mensajes transmitidos a 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 posible averiguar la ubicación y movimientos del usuario del teléfono durante un período 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.
- Biometría: la biometría consiste en sistemas de reconocimiento de individuos basados en mediciones de sus características físicas o conductuales. El uso más extendido de la biometría es el pasaporte biométrico, basado en el reconocimiento facial, de las huellas dactilares y/o del iris.

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 o los drones civiles equipados con cámaras 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. Los datos obtenidos a través de bases de datos biométricos podrían conducir a la identificación de robos. 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.

El uso de estas tecnologías suscita conflictos relativos a los derechos humanos, privacidad, legislación y confianza. Normalmente, 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, cuentan con potencial para invadir nues-

tra intimidad, un derecho humano fundamental protegido en Europa. Asimismo, también pueden provocar, por error, que se identifique a personas inocentes como delincuentes, con consecuencias graves para sus vidas.

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:

- ¿De verdad estas tecnologías mejoran la seguridad?
- ¿Hasta qué punto son invasivas?
- ¿Están debidamente legisladas?
- ¿El uso que se da a estas tecnologías se ajusta a la ley?
- ¿Se puede confiar en el uso que les dan las instituciones?
- ¿Están debidamente legisladas las instituciones que utilizan dichos datos?
- ¿Gozan de transparencia dichas instituciones y responden de cualquier vulneración de la privacidad que comentan en nombre de la seguridad?
- ¿Quién vigila a los vigilantes?
- ¿Cuáles son las alternativas? ¿Son funcionales?

Estos son algunos de los puntos que abordaremos durante el encuentro ciudadano.

La educación en ciencia, en tendencias de consumo y, en concreto, los conocimientos sobre las polémicas relativas a ciencia y tecnología son sin duda aspectos importantes que influyen en la capacidad de los ciudadanos para participar en los debates y ejercer sus derechos democráticos.

En los próximos párrafos introduciremos algunos términos y definiciones clave antes de pasar a describir las cinco tecnologías que explicaremos con más detalle.

Continúe leyendo para obtener más información sobre estas cuestiones.

3 Vigilancia, privacidad y seguridad

3.1 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. Por ejemplo, la policía podría hacer uso de sistemas de CCTV o drones equipados con cámaras de CCTV para localizar o seguir a delincuentes. Asimismo, la vigilancia podría tener fines comerciales. Por ejemplo, las empresas de motores de búsqueda pueden analizar el comportamiento de navegación a través de métodos de vigilancia online con el fin de mejorar sus motores de búsqueda. 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, orienta-

ción 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.

3.2 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”.

3.3 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;
- dismantelar 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, así como muchas otras empresas de menor envergadura. 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 Cinco tecnologías de seguridad

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

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

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 reunión 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

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. La Policía comenzó a utilizarlos en los sesenta. 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.

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.

Por ejemplo, a finales de 2012, el departamento de policía de Budapest comenzó a utilizar cámaras de CCTV inteligentes para observar carriles bus. La policía está autorizada legalmente a utilizar estas imágenes para penalizar a los que conducen por el carril bus.

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.

Una de las cuestiones que se plantean es si estos diferentes tipos de crímenes o delitos justifican el mismo nivel de vigilancia. ¿Se deberían utilizar los CCTV inteligentes para todo tipo de delitos o solo para los crímenes más peligrosos? En Europa existen diferentes opiniones a este respecto. En Alemania, por ejemplo, en 2008 el tribunal constitucional restringió el uso de sistemas de ANPR por

Funcionamiento de 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.

parte de la policía en zonas privadas. 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.

5.3 Mejoras en la seguridad

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

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.

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 pegs que deben tenerse en cuenta:

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.

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.

- 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.

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.

6 Drones

Un drone es el elemento volador de un sistema aéreo no tripulado (SANT). Lo dirige un piloto a través de un sistema de control en tierra, o vuelan automáticamente por medio de un ordenador de a bordo. Los drones también se conocen como Aeronaves Remotamente Pilotadas (ARP) o Vehículos Aéreos No Tripulados (VANT). El uso de drones causó mucha polémica cuando los Estados Unidos comenzaron a intensificar su uso en su guerra contra el terrorismo en Afganistán, Pakistán, Yemen y Somalia tras los atentados del 11 de septiembre. En los últimos tiempos, muchos estados europeos están rearmando sus fuerzas militares con drones.

Los drones no se emplean únicamente con fines militares en contextos bélicos; los servicios de seguridad también los usan para llevar a cabo tareas de reconocimiento y vigilancia con las que garantizar la seguridad ciudadana. Estos drones "civiles" con fines no militares se usan cada vez más como cámaras voladoras para vigilar lugares públicos con el objetivo de prevenir o detectar una serie de amenazas para la seguridad. Los drones civiles también se usan en campos distintos al de la seguridad, como en cartografía, fotografía inmobiliaria o como elementos de ocio. Otro aspecto relevante, es que permiten que se realicen labores de vigilancia en zonas de gran peligro para las personas como, por ejemplo, en zonas donde han ocurrido avalanchas, terremotos o accidentes nucleares. Por ejemplo, se utilizaron drones tras el accidente de Fukushima tanto para vigilar el estado de la central como para controlar el nivel de radiación.



El proyecto SurPRISE explora las posibilidades de tecnologías de seguridad basadas en la vigilancia, tanto las existentes como las que están en desarrollo, como medidas para potenciar la seguridad; por tanto, nos centraremos principalmente en los drones civiles destinados a acciones de seguridad.

6.1 ¿Por qué se desarrollaron los drones?

Al principio, los drones se diseñaron con fines militares para labores de reconocimiento y para fijar objetivos a los que dirigir los ataques. La tecnología para el control remoto de vehículos aéreos no tripulados se utilizó por primera vez durante la Primera Guerra Mundial; el primer vehículo lo concibió el Prof. A. M. Low en el Reino Unido en 1916. Se diseñó con el objetivo de servir de defensa contra los zeplines controlados desde tierra y como bomba voladora para la cual se consideró el control desde una aeronave de acompañamiento tripulada.

Aunque hoy en día los drones se suelen asociar a acciones militares, cada vez más agencias gubernamentales civiles, empresas y particulares utilizan vehículos aéreos no tripulados.

En la Unión Europea, el uso de drones "ligeros" que pesan menos de 150 kg, así como el uso de todo tipo de drones para fines militares, está regulado por los Estados Miembros. Actualmente, la Comisión Europea está estudiando la legislación relativa al uso de drones de mayor tamaño para fines comerciales puesto que el objetivo es comenzar a integrar los drones en el espacio aéreo civil europeo en 2016. En 2028, se espera que los drones estén integrados por completo en el espacio aéreo civil de la Unión Europea.

Las investigaciones actuales se centran en conseguir que los drones del futuro dependan incluso menos de la supervisión humana, de modo que se cruzan las fronteras hacia la robótica. Los drones están equipados con sensores que les permiten volar con autonomía en el espacio urbano. Asimismo, se están desarrollando procesos de producción masiva de micro drones. Las capacidades

tecnológicas en el campo de los drones se están desarrollando a gran velocidad puesto que los costes de producción y despliegue son cada vez menores.

A los drones se les puede instalar una gran variedad de equipamiento complementario, lo que facilita la vigilancia, así como la intervención. El tipo de equipamiento complementario que se puede instalar depende de la capacidad de carga del vehículo en cuestión.

6.2 Cómo se utilizan los drones

Los drones pueden complementar con eficiencia cualquier infraestructura existente (aeronaves tripuladas o satélites) que utilicen los organismos públicos para la gestión de cualquier crisis, aplicación de leyes, control fronterizo, control de tráfico u operaciones de extinción de incendios.

En el contexto de la seguridad, las fuerzas del orden de la UE han empleado drones sobre todo para vigilar multitudes en eventos a gran escala, como festivales de música, manifestaciones y even-

tos deportivos, con el fin de detectar sucesos fuera de lo común o movimientos bruscos dentro de la multitud. También se pueden utilizar para investigaciones en la escena del crimen. Su uso para el control de fronteras es una posibilidad que la UE explotará en un futuro cercano. Los drones también se han utilizado para detectar cultivos de droga y para dar apoyo a la policía en persecuciones.

Los drones de vigilancia empleados en el control de lugares públicos cuentan con una importante ventaja: son capaces de cubrir un espacio mucho más grande, son móviles y, a alturas de 50 a 200 metros permiten perspectivas distintas a las de las cámaras de CCTV estáticas ubicadas en lugares públicos.

Los drones pueden utilizarse en un gran número de aplicaciones comerciales. Se pueden utilizar para dar apoyo a la agricultura de precisión y piscifactorías, vigilancia de líneas de gas y electricidad, inspección de infraestructuras, servicios de comunicaciones y emisión, repetidores inalámbricos y sistemas de aumentación basados en satélites, vigi-

Funcionamiento de los drones

Los drones pueden presentar diversos formatos y pueden llevar prácticamente un número ilimitado de "cargas", es decir, los objetos que se instalan en el dron, como cámaras, sensores o misiles. Por lo general, uno o dos operadores se encargan de controlar los drones desde tierra y supervisan y monitorizan las actividades del vehículo y su carga. Es posible controlar un dron con un smartphone o tableta. En algunos casos es posible preprogramar el dron para una ruta de vuelo específica dentro de su alcance. Sin embargo, en comparación con los vuelos con piloto automático, la autonomía de la programación de los drones aún se encuentra en sus fases iniciales, aunque las investigaciones actuales se centran en este punto. La comunicación entre el dron y el operador se puede dar de varias formas aunque, para grandes distancias, se necesita un enlace por satélite para apoyar la transmisión de datos desde el vehículo y para retransmitir las órdenes.

Los sistemas estándar VANT cuentan con los elementos siguientes:

- Aeronave no tripulada (VANT)
- Unidad de control en tierra, que pueden ser móviles
- Enlace para transmisión de datos, que puede requerir apoyo vía satélite
- Equipamiento complementario.

El tamaño y equipamiento de los drones varía mucho y depende de los fines para los que se utilicen. Se puede equipar, por ejemplo, con cámaras de CCTV, sensores, equipamiento panóptico, radares, Wifi y otros sistemas de intercepción de comunicaciones, detención química o de radiaciones y armas. Puesto que las investigaciones se centran en gran medida en el desarrollo de micro o nano drones que puedan imitar el movimiento de insecto o aves, se puede predecir que, en el futuro, la capacidad de vigilancia de los drones será casi ilimitada, aunque las áreas de actuación permitidas están todavía muy limitadas desde un punto de vista legal.

lancia de recursos naturales, entretenimiento/medios de comunicación, cartografía digital, gestión del terreno, la flora y la fauna o gestión y control de la calidad del aire.

A pesar de estas impresionantes perspectivas, los drones cuentan con varios problemas técnicos aún sin resolver. Dichos problemas se refieren, por ejemplo, a las capacidades limitadas con respecto a la altitud de vuelo, velocidad y duración, así como cuestiones relativas al repostaje en vuelo de los drones. Los drones también son muy vulnerables a las condiciones atmosféricas desfavorables, como nubes espesas, viento y lluvia. Además, los drones que generan datos a través de equipamiento avanzado, como cámaras de CCTV o sensores, provocan sobrecargas y problemas de pérdida de ancho de banda. La grabación del CCTV puede estar borrosa debido al movimiento del drone.

6.3 Mejoras en la seguridad

1. Los drones facilitan la detección de problemas de seguridad.
 - Los drones pueden cubrir grandes áreas así como llegar a zonas inaccesibles. Por ejemplo, en operaciones de búsqueda y rescate, se pueden utilizar drones para la vigilancia de grandes áreas de difícil acceso como bosques densos. Los drones también pueden realizar inspecciones de grandes zonas fronterizas con el fin de detectar entradas no autorizadas y combatir el tráfico de personas.
 - Los drones son dispositivos móviles. No sólo son capaces de detectar y grabar objetos e individuos sospechosos sino que también pueden rastrear dichos objetos y personas mientras se mueven por espacios públicos. A diferencia de los equipos humanos que persiguen personas u objetos, los drones no se cansan y son menos visibles, por lo que pueden rastrear objetos y personas durante un periodo de tiempo más prolongado.
 - Los drones resultan más visibles que las cámaras de CCTV. Por tanto, es más difícil que los delincuentes potenciales

se percaten de su presencia.

2. Reducen el riesgo ante posibles delitos y el grado de intromisión.
 - Cuando la gente se entera de que una zona concreta está vigilada por un drone, la gente se siente más segura porque saben que si ocurriera algo fuera de lo común a su alrededor el drone lo detectaría rápidamente.

6.4 Problemática

1. Los drones son menos visibles que los sensores o cámaras de CCTV estáticas; así pues tienen la capacidad de grabar y almacenar información de manera indiscriminada, lo que les convierte en una herramienta con potencial invasivo mayor en términos de privacidad.
 - Las capacidades de los drones superan las de las cámaras de CCTV (inteligentes) ya que los drones pueden obtener información de zonas privadas que sus propietarios han intentado cubrir para que no sean vistas por medio de muros, vallas y demás elementos. Así pues, los drones pueden tomar imágenes de propiedades privadas a las que las cámaras de CCTV no pueden acceder.
 - Como ocurre con la gran mayoría de sistemas de vigilancia, los drones también cuentan con la capacidad de grabar y almacenar información de forma indiscriminada, por lo que es probable que recojan y analicen las actividades públicas y privadas de personas inocentes. Lo anterior puede generar un efecto disuasorio.
 - En comparación con las cámaras de CCTV, los drones son más difíciles de localizar, por lo que a las personas no les resulta tan sencillo saber que les vigilan. Debido a su naturaleza intrínsecamente móvil, resulta difícil saber quién controla el drone. Por lo tanto, también es más difícil para los ciudadanos evitar o cuestionar la vigilancia.
 - Dicha dificultad puede generar una sensación permanente de

incertidumbre en las personas que se saben observadas y provoca cambios más o menos sutiles en su comportamiento con el fin de evitar una atención indeseada o negativa. El "efecto disuasorio" al que se hacía mención anteriormente se acrecentará cuando se instalen los drones las mismas características de los CCTV inteligentes, como la función de reconocimiento de patrones conductuales o anormales que podría afectar en gran medida a los derechos básicos de libertad de expresión y reunión en lugares públicos.

- El uso de drones en combinación con sistemas de CCTV y sistemas de localización ubicados en tierra supone una vigilancia mucho más integral de los ciudadanos haciendo posible un análisis detallado de movimientos, comportamientos y perfiles sociales.
2. Los drones equipados con instrumentos de registro de datos como sistemas de CCTV o sensores pueden ser vulnerables a piratería por parte de terceros debido a la falta de encriptación y al hecho de que pueden aprovechar posibles interrupciones en la comunicación con la base o el piloto.
 3. Además, existen cuestiones de seguridad pública relativas al uso de drones en zonas habitadas.
 - La tasa de accidentes de los drones es todavía mucho más elevada que la de las aeronaves tripuladas y resultan más vulnerables a las condiciones atmosféricas (viento, lluvia), lo cual supone un mayor riesgo para las personas en tierra.

7 Cibervigilancia mediante 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 factu-

ración, 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

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.



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 pueden abrir y analizar 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.



7.1 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.

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. Estas 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.

7.2 ¿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. La legislación europea protege la confidencialidad de las comunicaciones. La DPI también incumple el Con-

venio Europeo de Derechos Humanos porque conlleva una vigilancia indiscriminada, masiva y sin garantías: puede tener acceso a toda la información que se envíe y reciba 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.

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. 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 pocos usos documentados de la DPI aparte de las extensas actividades de vigilancia que llevan a cabo las agencias de seguridad de los EE.UU. según reveló el informático Edward Snowden el año pasado: algunos de estos usos son comerciales y otros están relacionados con la seguridad pública y nacional.

7.2.1 Usos comerciales

- *Seguridad y gestión de 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.

7.2.2 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 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 tiene lugar en Europa también.

7.3 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 7.2.2.

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.

7.4 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.

- Las capacidades tecnológicas van por delante de la regulación.
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.

8 Sistemas de localización y seguimiento a través de smartphones

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.

8.1 ¿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.

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 legislación europea en vigor dispone que los operadores deben almacenar dichos datos durante un periodo mínimo de seis meses y un máximo de veinticuatro. Aunque el Tribunal de Justicia de la Unión Europea invalidó la directiva en cuestión en abril de 2014 todavía no se han enmendado las respectivas legislaciones nacionales.

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 disponi-

bles 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.

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 obtuvo los registros de los datos de localización de su teléfono móvil correspondientes

a un periodo de seis meses, le parecieron una sucesión de números y letras carentes 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 Esta-

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 es en el caso de 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.

También es posible localizar de este modo otros dispositivos móviles “inteligentes”, como los iPads, tablets y notebooks.

dos 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.”

8.2 ¿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.

8.2.1 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.



8.2.2 Usos relativos a la seguridad pública y nacional

- Búsqueda de personas desaparecidas: 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 “Occupacy” 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 trocar 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.

8.3 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:

- Permiten encontrar y prestar ayuda a personas en situaciones de peligro.
- Permiten a las familias vigilar a sus adultos vulnerables o niños.
- 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.

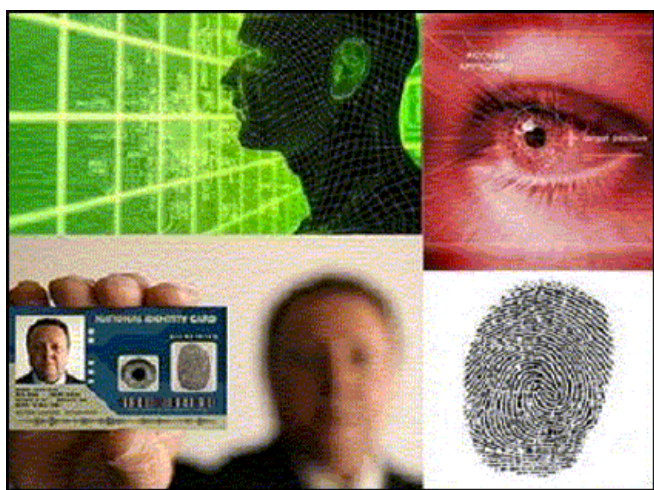
8.4 Problemática

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:

- 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.
- 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.
- 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.
- 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.
- 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.

9 Biometría

El término "biometría" puede hacer referencia tanto a los sistemas que utilizan características físicas medibles de las personas (como huellas dactilares, ADN, patrones de la retina, estructura facial, olores corporales) o bien a sistemas de análisis de rasgos conductuales personales únicos (como el análisis de la forma de andar y la voz o pulsaciones del teclado) con el fin de reconocer la identidad de alguien, verificar la declaración de identidad de un determinado individuo o la definición de una persona.



Algunos países toman las huellas dactilares de sus ciudadanos, así como otros "identificadores" biométricos, y los almacenan en documentos nacionales de identidad o en una base de datos. En ese punto, las características de un individuo quedan registradas en un sistema biométrico. En fases posteriores, la información biométrica de una persona se compara con la información almacenada en el momento del registro con el fin de comprobar la identidad de dicha persona. Los grandes avances que se han dado en el campo del tratamiento informático han hecho surgir sistema biométricos automático que permiten, por ejemplo, realizar comprobaciones masivas de identidad en segundos.

9.1 ¿Por qué se desarrolló la biometría?

En el siglo XIX, el desarrollo de los sistemas de justicia nacionales provocaron la necesidad de crear una manera más formalizada de identificar a

las personas. Dichos sistemas buscaban tratar con mayor indulgencia a aquellos que delinquían por primera vez y de manera más severa a los reincidentes. Por tanto, se necesitaba un sistema formal que registrara los delitos junto con rasgos medibles de la identidad del delincuente. En Francia, Alphonse Bertillon desarrolló el "Bertillonage" o la antropometría, un método de identificación de individuos basado en registros detallados de medidas corporales como la altura, la longitud del brazo, descripciones físicas y fotografías. Alrededor de 1890, surgió un enfoque mucho más prometedor cuando Sir Francis Galton fue capaz de desarrollar un método para recuperar registros con los que identificar delincuentes en base a sus huellas dactilares, un sistema de identificación más individualizado en comparación con las mediciones de Bertillon. En el siglo XX se descubrió que otros rasgos se podían utilizar como identificadores potenciales. En 1936, Frank Burch propuso la utilización de los patrones del iris como método para reconocer a los individuos y en la década de los sesenta se desarrollaron técnicas de reconocimiento facial y de voz.

9.2 Cómo se utiliza la biometría

Las fuerzas del orden han utilizado tradicionalmente la biometría para identificar delincuentes, tanto conocidos como desconocidos, y para conceder acceso a lugares restringidos, edificios gubernamentales, locales comerciales, etc.

En el siglo XXI el uso de la biometría se está extendiendo cada vez más en el campo de la seguridad fronteriza. Se toman datos biométricos de aquellas personas que necesitan un visado para visitar un determinado país. A su llegada, dichos datos biométricos se cruzan con una base de datos para comprobar, por ejemplo, si al viajero se le ha denegado el acceso en ocasiones anteriores, si supone un riesgo para la seguridad o si ha rebasado previamente el tiempo de estancia de su visado. Por ejemplo, la UE toma 10 huellas dactilares y una fotografía digital de aquellas personas que solicitan un visado europeo. Estos datos biométricos se almacenan en la base de datos del SIV (Sistema de

Información de Visados). Igualmente, la UE ha creado EURODAC, una amplia base de datos de huellas dactilares de aquellas personas que solicitan asilo e inmigrantes sin documentación que se encuentran dentro de la UE. Esta base de datos ayuda a la aplicación efectiva del Convenio de Dublín relativo a las solicitudes de asilo.

En contextos militares, el ejército de los EE.UU. ha utilizado dispositivos portátiles en los campos de batalla de Afganistán e Iraq que permitían realizar escáneres rutinarios del iris y demás puntos biométricos a aquellas personas con las que se encontraban. Acto seguido, las personas de interés se incluyen en una "Lista de Alerta Biométrica" que permite a los soldados verificar sobre el terreno la identidad de un sospechoso de terrorismo o averiguar si una persona con nacionalidad de ese país local tiene lazos con una red de insurgentes y así

poder denegarle un puesto de trabajo en una instalación militar internacional de los EE.UU. Hasta ahora, la base de datos contiene 209.000 registros de personas de todo el mundo.

Aunque la biometría se desarrolló en un primer momento para identificar a individuos a efectos de seguridad, a lo largo del s. XX se han ido desarrollando cada vez más mecanismos de control de accesos para el mercado comercial. La ventaja sobre llaves y contraseñas radica en que es extremadamente difícil olvidar o perder rasgos personales. Asimismo, copiarlos resulta muy complicado. Razón por la cual mucha gente los considera más fiables y seguros que las llaves o contraseñas. Por ejemplo, los nuevos iPhones de Apple cuentan con un lector de huellas dactilares que detecta la huella del usuario. A su vez, Facebook emplea herramientas de reconocimiento facial para sugerir la identi-

Funcionamiento de la identificación biométrica

El primer paso consiste en obtener del individuo una muestra biométrica, por ejemplo, una huella dactilar o escaneo del iris, que normalmente se realiza por medio de captura de imágenes. Los datos se pueden almacenar como imagen o como patrón, que es una representación digital de la biometría creada utilizando un algoritmo. Para garantizar el máximo nivel de privacidad, sería recomendable almacenar únicamente el patrón y desechar la imagen original.

Los datos biométricos, bien en forma de imagen o de patrón, se pueden almacenar en diversas ubicaciones, por ejemplo, en el centro de operaciones donde se tomó el registro (por ejemplo, en un lector) de cara a un uso posterior, así como en un dispositivo que lleva el individuo (por ejemplo, en una tarjeta inteligente). También es posible enviar y almacenar los registros en una base de datos centralizada compuesta por uno o varios sistemas biométricos.

Cuando se accede a un sistema biométrico, el sistema pedirá que se introduzcan las características biométricas. En ese momento el sistema compara la imagen o el patrón de la muestra introducida con el dato biométrico de la persona que consta en el sistema.

Si el proceso de comparación de datos biométricos es positivo, el sistema reconocerá y aceptará al individuo en cuestión. Si la comparación arroja un resultado negativo, no se reconocerá al individuo y, por tanto, se le "rechazará". La imagen o el patrón creados cuando se registran por primera vez los datos biométricos rara vez serán idénticos a los de la imagen o patrón de las características biométricos que se introducirán más adelante. Con frecuencia, las características más relevantes cambiarán ligeramente o se enviarán de manera un tanto diferente a cuando se registraron por primera vez. Por tanto, es inevitable que exista cierto grado de probabilidad en la comparación.

La biometría también se puede utilizar en la prevención de los delitos, especialmente cuando emplea el análisis de rasgos de comportamiento; en ese caso el objetivo no es la identificación de un individuo en concreto sino su categorización. Las funciones de reconocimiento facial y el análisis del comportamiento de las cámaras de CCTV inteligentes se pueden considerar funciones biométricas de las cámaras de vigilancia.

dad de las personas que aparecen en fotos. Su proyecto de investigación, DeepFace, puede afirmar con un 97,25% de precisión si dos fotografías contienen el mismo rostro. Los bancos están desarrollando sistemas de biometría de voz para facilitar el acceso de sus clientes a tarjetas de créditos y realizar pagos a través de sus teléfonos móviles con solo pronunciar una contraseña. Las empresas utilizan portátiles que incluyen lectores de huellas dactilares para realizar controles biométricos de acceso. Incluso los expositores publicitarios ubicados en la calle pueden mostrar diferentes anuncios dependiendo de la persona que los mire, en base a su edad o género.

No obstante, la biometría se utiliza cada vez más, no solo como herramienta de identificación sino para realizar análisis de comportamiento. Existen ciertas aplicaciones deportivas que utilizan sistemas de biometría en tiempo real por ejemplo, para medir el ritmo cardíaco o la frecuencia respiratoria de modo que pueda ofrecer recomendaciones deportivas a los usuarios de la aplicación. Por lo que respecta a los sistemas de seguridad, las nuevas funciones de procesamiento biométrico se combinan con sistemas existentes (por ejemplo, reconocimiento facial junto con sistemas de CCTV) lo que genera nuevas funciones de vigilancia. En dicho contexto, es importante señalar que estos nuevos sistemas biométricos cuentan con el potencial de recopilar información a distancia o en movimiento sin necesidad de que el individuo realice acciones específicas o coopere. Dichos sistemas pueden activar determinadas alarmas cuando, por ejemplo, una cámara de CCTV identifica a un delincuente conocido cuya imagen se encuentra en una base de datos policial.

9.3 Mejoras en la seguridad

La biometría pueden mejorar la seguridad en los siguientes sentidos:

- Las fuerzas del orden llevan usando la identificación a través de lectores biométricos durante más de cien años tanto a efectos de verificación como de identificación. Aquellos sistemas que analizan el rostro de las personas o los que analizan su ADN pueden contribuir de manera muy efectiva a la lucha contra el crimen así como a revelar de forma

eficiente la identidad de los sospechosos de delitos graves.

- La obtención de datos biométricos se puede utilizar para aumentar la seguridad de aquellas actividades de procesamiento de datos particularmente sensibles. Por ejemplo, pueden contribuir a garantizar que únicamente aquellas personas autorizadas de una operadora de telefonía tenga acceso a datos de tráfico (y datos de localización) que se deban retener a efectos de aplicación de determinadas leyes.

9.4 Problemática

Se plantean ciertos inconvenientes que deben tenerse en cuenta:

1. Los datos biométricos no son infalibles.
 - Se podría afirmar que dos capturas de un mismo rasgo biométrico nunca serán exactamente iguales. Las diferencias existentes en el tipo de equipo utilizado en el momento del registro o las diferencias ambientales (luz, temperatura) podrían provocar ciertas tasas de aceptación o rechazo erróneos; es decir, un determinado sistema biométrico podría identificar de manera incorrecta a un individuo o no ser capaz de reconocer a un impostor (tasa de falsa aceptación). Los falsos rechazos se dan cuando los datos de un individuo no se corresponden con su propio registro biométrico.
 - Además, las características biométricas de una persona pueden cambiar durante el transcurso de su vida debido a, por ejemplo, la edad, intervenciones quirúrgicas o accidentes. Por tanto, un determinado sistema biométrico puede dejar de reconocer a dicha persona.
 - Asimismo, también es posible falsificar los datos biométricos, lo cual aumenta las posibilidades de usurpación de identidad.
 - En base al estado actual de la tecnología, es aún relativamente sencillo engañar a sistemas de reconocimiento biométrico realizando simplemente pequeños cambios en la apariencia como peinados, barbas,

maquillaje, gafas, lentillas, etc.

2. En el pasado, el uso de sistemas biométricos era caro y requería mucho tiempo. A consecuencia de estas restricciones, el impacto sobre los derechos de protección de datos de los individuos estaba limitado. No obstante, esto ya no es así, por lo que podrían surgir ciertos tipos de discriminación genética y una pérdida gradual de la privacidad si no se aplican las garantías necesarias. Por ejemplo, si se dotaran los sistemas de vigilancia y los smartphones con sistemas de reconocimiento facial basados en las bases de datos de redes sociales, se podría acabar con el anonimato de los individuos y la privacidad de sus movimientos.
3. En la mayoría de casos, el registro implica una participación activa por parte del individuo en cuestión; por ejemplo, en el caso de la toma de huellas dactilares y, por tanto, supone una buena oportunidad para facilitar información así como un certificado de procesamiento legítimo. No obstante, también es posible registrar individuos sin su consentimiento o conocimiento, por ejemplo, mediante la utilización de sistemas de CCTV que incluyan funciones de reconocimiento facial. Lo anterior afecta gravemente a su capacidad de ejercer su libre consentimiento o de obtener información acerca del procesamiento.
4. La biometría, en cuanto a que se basa en características inalterables, también puede resultar problemática ya que, una vez se ha consentido al registro, puede conllevar una falsa estigmatización del individuo en cuestión.

10 ¿La tecnología basada en la vigilancia es 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. Las tecnologías de seguridad orientadas a la vigilancia se basan en el supuesto de que la mejor manera de detectar actos potencialmente peligrosos y de identificar a posibles delincuentes una vez han cometido el delito, o incluso antes de que se haya cometido, es mediante un sistema de vigilancia que controle al mayor número de personas de la forma más precisa posible. Por tanto, cuando se aplican dichas tecnologías, la seguridad se obtiene casi de forma exclusiva mediante sistemas de vigilancia mejorados.

Esto es cierto en parte, pero es una realidad incompleta. Mientras que las tecnologías de seguridad se utilizan para localizar a delincuentes y terroristas y predecir sus próximos movimientos, existen distintas estrategias que buscan mejorar la seguridad a través de otros medios. En este capítulo vamos a dar ejemplos de medidas de seguridad alternativas.

La seguridad es un concepto social ambiguo que se puede percibir de maneras distintas. Los factores que se asocian con la estabilidad social, certidumbre o confianza social, por nombrar unos cuantos, están estrechamente relacionados con los diferentes niveles de seguridad.

10.1 Medidas de seguridad alternativas: a nivel global

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 apari-

ción 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 global. Una vez hemos acotado el concepto seguridad en términos de "seguridad humana general" sería recomendable señalar algunos desafíos a los que se enfrenta la sociedad a nivel global.

Es posible proponer y aplicar, hasta cierto punto, iniciativas de seguridad destinadas a aumentar los niveles de seguridad en relación con catástrofes naturales o aquellas provocadas por los hombres. Dichas iniciativas suelen basarse en estrategias integrales a largo plazo. La promoción de sistemas de comercio justo, las ayudas o el alivio de la deuda, por ejemplo, son medidas destinadas, no solo a solucionar cuestiones económicas sino también a solucionar problemas medioambientales relacionados con la sobreexplotación de recursos naturales, la contaminación y las alteraciones de ciclos climáticos. En última instancia, son cuestiones relacionadas con la seguridad. De la misma forma, las políticas destinadas a mejorar las respuestas locales y nacionales ante catástrofes naturales o las políticas que se centran en la mejora de infraestructuras de comunicación e información también son formas alternativas de mejorar las condiciones de vida y, por tanto, de potenciar los niveles de seguridad de las zonas en cuestión.

Se han desarrollado distintas maneras de entender la seguridad y, por tanto, de promoverla, y no únicamente a nivel mundial. Por tanto, nos gustaría que centrara su atención en su contexto local para

visualizar una serie de estrategias adicionales que pretenden potenciar la seguridad.

En resumen: soluciones nacionales e internacionales.

- Fomento de sistemas globales justos de comercio, asistencia y alivio de la deuda.
- Fomento de políticas económicas y sociales para garantizar una distribución equitativa de la renta y el empleo.
- Mejora de las infraestructuras y recursos de respuesta ante catástrofes.
- Uso más eficiente de fuentes de energía sostenibles y alternativas.
- Mejora de las infraestructuras de suministro de agua, comunicación e información y abastecimiento de alimentos en las partes del mundo que más lo necesitan.

10.2 Medidas de seguridad alternativas: a nivel local

Existen formas diferentes y alternativas de entender y obtener unos niveles de seguridad más elevados a nivel local. Por ejemplo, se puede obtener la seguridad por medio de la aplicación de tecnologías que no conllevan el uso de vigilancia. Algunas de las tecnologías que aumentan los niveles de seguridad sin introducir vigilancia u obtención de datos son los detectores de metales, sensores de movimiento, alarmas volumétricas, dispositivos de alarma generales, o incluso teléfonos públicos para emergencias. En su lugar, pretenden potenciar la habilidad de las personas de reacción e intervenir en su propia protección y en la de sus bienes. Por otra parte, tecnologías como los detectores de metales contribuyen con las autoridades públicas a identificar peligros potenciales centrándose en el origen de la amenaza (el metal del objeto) en vez de en las características de la persona que constituiría la amenaza. Su efectividad puede resultar muy alta, pero quedaría limitada al momento y el lugar concretos en el que se utilizan. Además, no suponen una amenaza en términos de privacidad o vigilancia.

Asimismo, se puede prevenir el crimen y aumentar la seguridad en espacios públicos por medio de la gestión y la planificación urbanística. Si se aplica-

sen modificaciones estructurales con el fin de potenciar un entorno constructivo más seguro, por ejemplo, reduciendo las "áreas peligrosas" (aquellas calles, plazas y parques difíciles de vigilar) se podría, por una parte, aumentar la percepción de seguridad del espacio público y, al mismo tiempo, conseguir que los ciudadanos tengan mayor conciencia de su entorno inmediato y de los peligros que pueden surgir.

En resumen: estrategias que no se basan en la vigilancia y la obtención de datos.

- Prevención de la delincuencia por medio de la planificación urbanística y el diseño del entorno.
- Aplicación de tecnologías que no conlleven el uso de vigilancia.

Asimismo, es posible introducir medidas de seguridad destinadas a mejorar los niveles de seguridad a través de la vigilancia pero que no conllevan necesariamente el uso de tecnologías de seguridad que traen consigo la recopilación y almacenamiento masivo de datos. Un ejemplo típico sería el refuerzo de la actividad policial, aumentando el número de patrullas, por ejemplo. En efecto, las actividades policiales tradicionales es una manera de aumentar los niveles de seguridad sin recurrir a la vigilancia tecnológica. Por otra parte, existen programas de vigilancia de barrios que funcionan mediante la redistribución de las patrullas de vigilancia entre los vecinos de las zonas residenciales que observan actos sospechosos en sus barrios y los denuncian a la policía local. Otro ejemplo de medida de seguridad que se basa en la vigilancia para aumentar la seguridad sin utilizar tecnologías de obtención masiva de datos serían los controles de identidad por medio de listas cerradas de asistentes para regular el acceso de personas a lugares públicos o privados que llevarían a cabo porteros o personal de seguridad.

En resumen: estrategias para reforzar la vigilancia que no se basan en el uso de tecnología:

- Incremento de las acciones policiales tradicionales.
- Aplicación de programas de Vigilancia de Barrios y similares.

- Utilizar vigilantes físicos, es decir, personal de seguridad o porteros.

Por último, existen maneras de enfocar la seguridad que buscan incrementar los niveles de seguridad no tanto a través de la represión de actos delictivos o medidas disuasorias, sino más bien a través de estrategias integrales a largo plazo capaces de atajar las causas sociales y económicas subyacentes que provocan violencia, delincuencia, odio religioso, racismo o discriminación social. Una vez más, las tecnologías de seguridad son menos efectivas a la hora de enfrentarse a estos problemas de seguridad humanos más complejos a largo plazo.

Siguiendo con este enfoque de seguridad en un sentido amplio, se han propuesto diferentes medidas como, por ejemplo, establecer mejores relaciones entre la policía y la comunidad o integrar a los grupos religiosos u otras comunidades en la gestión de problemas locales con el fin de aumentar la confianza y la cohesión social. Otras opciones de seguridad pasan, en última instancia, por aumentar el nivel de apoyo social y económico mediante medidas activas de creación de empleo, formación y orientación para aquellos con mayor susceptibilidad de verse abocados a la delincuencia. Otros ejemplos de medidas locales que sirven para aumentar la cohesión social a la vez que mejoran los niveles de seguridad en una zona determinada lo constituirían las asociaciones de voluntarios que trabajan para rehabilitar a personas con problemas de adicción al alcohol y las drogas, la creación de centros de acogida de inmigrantes y demás centros sociales autogestionados.



La idea básica que subyace a estas estrategias de seguridad reviste una doble naturaleza: por una parte, se basa en la participación activa de los afectados (es decir, de los ciudadanos locales) para la resolución de conflictos y, por otra, también aspira a la (re)integración de los delincuentes a través de trabajos comunitarios, en lugar de aplicar sanciones disciplinarias.

Las políticas de educación activa orientadas a la integración, autogestión y respeto por la diversidad mutua pueden contribuir a la disminución de las tensiones sociales, culturales y económicas y a mejorar el sentimiento de pertenencia a las comunidades locales y nacionales a la vez que contribuyen de manera indirecta al aumento de los niveles de seguridad.

En resumen: estas son las estrategias que se pueden aplicar a largo plazo con respecto a las condiciones sociales y la reducción de los problemas

- Inversión en recursos y medidas sociales, así como personal.
- Fomento de la participación activa de los ciudadanos para la resolución de problemas y conflictos locales.
- Creación de mejores relaciones sociales entre los distintos grupos que componen la comunidad.
- Aumento del apoyo (económico) para las políticas de empleo, oportunidades de formación e iniciativas similares.
- Creación de centros de acogida, centros comunitarios y centros sociales.

Aunque en este capítulo hemos introducido algunas estrategias y conceptos alternativos, puede que usted tenga otras ideas con las que se puede mejorar la seguridad. O a lo mejor opina que Europa debería centrar sus políticas de seguridad en otras cuestiones que no sean la delincuencia o el terrorismo.

11 Le cedemos la palabra...

Ha llegado al final del documento y ahora puede tomarse un tiempo para reflexionar sobre los asuntos tratados en esta revista.

Hemos descrito las cinco tecnologías de seguridad sobre las que se hablará en la reunión 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 reunión 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>.

"Los problemas relativos a la seguridad plantean tanto cuestiones políticas como legales y tecnológicas."

Colin J. Bennett, profesor y experto en seguridad del Departamento de Ciencias Políticas de la Universidad de Victoria, Canadá.

Información sobre el documento

El presente documento informativo se ha elaborado con el fin de informar a los ciudadanos que participarán en las reuniones ciudadanas. 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. 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.

La presente publicación es una versión extendida y reeditada de la publicación informativa redactada por la Dra. Kirstie Ball (The Open University) en 2013 para la cumbre ciudadana a gran escala celebrada en nueve países durante los tres primeros meses de 2014.

- Autores: Dra. Kirstie Ball, The Open University; Maria Grazia Porcedda y Mathias Vermeulen, EUI; Elvira Santiago y Vincenzo Pavone, CSIC; Regina Berglez, IRKS; Eva Schlehn, ULD; Márta Szénay, Medián.
- Consejo Asesor en Materias Científicas: Dra. Monica Areñas Ramiro, Mr Robin Bayley, Prof. Colin Bennett, Dra. Gloria González Fuster, Dr. Ben Hayes, Dr. Majtényi László, D. Jean Marc Suchier, D^a Nina Tranø, Prof. Ole Wæver.
- Diseño: Zsolt Bartha, Medián, basado en la primera publicación elaborada por D. Peter Devine, D. David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University.
- Imágenes: Mr David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University. página 12: Vision Systems, <http://www.visionsystems.co.nz/assets/Video-Analytics1.jpg> página 16 Mat Wellington, "Police Use QuadCopter – UK" 23 de marzo de 2011, <http://multirotor-news.com/2011/03/23/police-use-quadcopter-uk> página 24 © iStockPhoto.com / alexsl, página 26 Senseable City Lab, Massachusetts Institute of Technology página 28 © KIVI NIRIA DV, 2011
- El proyecto SurPRISE ha recibido financiación del Séptimo Programa Marco de la Unión Europea para acciones de investigación, desarrollo tecnológico y demostración en virtud del acuerdo de subvención n^o 285492.
- La presente publicación se encuentra disponible en: <http://surprise-project.eu>

Miembros del Proyecto

5. Institut fur Technikfolgen-Abschätzung/Osterreichische Akademie der Wissenschaften,
6. Coordinador, Austria (ITA/OEAW)
7. Agencia de Protección de Datos de la Comunidad de Madrid*, Spain (APDCM)
8. Instituto de Políticas y Bienes Públicos/Agencia Estatal Consejo Superior de Investigaciones
9. Científicas, Spain (CSIC)
10. Teknologiradet - The Danish Board of Technology Foundation, Denmark (DBT)
11. European University Institute, Italia (EUI)
12. Verein für Rechts-und Kriminalsoziologie, Austria (IRKS)
13. Median Opinion and Market Research Limited Company, Hungría (Median)
14. Teknologiradet - The Norwegian Board of Technology, Norway (NBT)
15. The Open University, Reino Unido (OU)
16. TA-SWISS/Akademien der Wissenschaften Schweiz, Suiza (TA-SWISS)
17. Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein/Germany (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.

Este proyecto ha recibido financiación del Séptimo Programa Marco de la Unión Europea para acciones de investigación, desarrollo tecnológico y demostración en virtud del acuerdo de subvención nº 285492

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.

