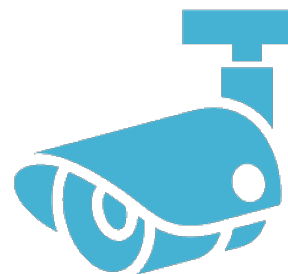




Proyecto SURPRISE: Principales Resultados



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	7
3 Vigilancia, privacidad y seguridad	9
3.1 Vigilancia.....	9
3.2 Privacidad y protección de datos: ¿son cuestiones importantes?	9
3.3 Seguridad.....	10
4 Cinco tecnologías de seguridad	12
5 CCTV inteligentes.....	13
5.1 Mejoras en la seguridad	13
5.2 Problemática	13
6 Drones	14
6.1 Mejoras en la seguridad	14
6.2 Problemática	14
7 Cibervigilancia mediante inspección profunda de paquetes	15
7.1 Mejoras en la seguridad	15
7.2 Problemática	15
8 Sistemas de localización y seguimiento a través de smartphones.....	16
8.1 Mejoras en la seguridad	16
8.2 Problemática	16
9 Biometría.....	17
9.1 Mejoras en la seguridad	17
9.2 Problemática	17
10 La participación ciudadana en el proyecto SURPRISE: la Cumbre Ciudadana y la Reunión Ciudadana.....	18
10.1 La Cumbre Ciudadana: Citizen Summit	18
10.2 La Reunión Ciudadana: el Small Scale Event	19
11 Principales resultados.....	21
Información sobre el documento	25
Miembros del Proyecto	26

1 Bienvenidos a SURPRISE

Bienvenidos a SURPRISE: un proyecto de investigación a nivel europeo. SURPRISE es la versión abreviada de 'Surveillance, Privacy and Security' (Vigilancia, Privacidad y Seguridad). El objetivo de este proyecto es recopilar el punto de vista de los ciudadanos con respecto a las llamadas tecnologías de seguridad (SOSTs por sus siglas en inglés). La mayor parte de este tipo de tecnologías se basa en la vigilancia de 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.

La Comisión Europea financia este proyecto porque desea conocer qué opinan los ciudadanos que se debería hacer para garantizar su seguridad y conseguir que se sientan protegidos. Y es que en los últimos años, en el camino hacia una sociedad segura, se han ido desarrollando y adoptando cada vez en mayor medida tecnologías de vigilancia orientadas a la seguridad. El objetivo de estas tecnologías es transformar las amenazas en eventos predecibles mediante la recolección continua de datos, la monitorización de comportamientos sospechosos, el análisis y el intercambio de información.

Sin embargo, a pesar de la pérdida de intimidad y espontaneidad que la vigilancia conlleva, no siempre la vigilancia repercute en un aumento real de la seguridad. Es por ello que a la hora de abordar las implicaciones de esta paradójica situación, en Europa se han realizando diferentes trabajos de investigación con el objetivo de responder a la pregunta ¿en qué medida y bajo qué condiciones, los ciudadanos europeos están dispuestos a intercambiar parte de su intimidad y de su libertad de expresión a cambio de un aumento de la seguridad personal y colectiva?. La mayoría de estos estudios toman como punto de partida la existencia de una

inevitable relación inversa entre seguridad pública e intimidad individual, y no permiten cuestionar la base de este trade-off ni imaginar fórmulas novedosas que permitan que la seguridad y la intimidad se complementen en lugar de encontrarse enfrentadas.

Ante esta compleja situación, el proyecto SURPRISE re-examina la relación entre seguridad y privacidad y sugiere que ha de tenerse en cuenta el impacto que las medidas de seguridad tienen sobre los ciudadanos existiendo cuestiones complejas que subyacen a los problemas de privacidad, como el escepticismo público hacia las tecnologías de vigilancia orientadas a la seguridad, que pueden no ser evidentes para los expertos de los ámbitos legales y tecnológicos. Además los expertos tecnológicos de seguridad han venido pasando por alto la preocupación por los derechos humanos en el contexto del rápido cambio tecnológico.

Hasta ahora, las decisiones sobre cuestiones relativas a la seguridad y la privacidad han dejado sin respuesta las preguntas esenciales: ¿Qué características tiene que tener una tecnología de seguridad aceptable en Europa y por qué? ¿Cómo ven los ciudadanos europeos la relación entre la seguridad y la privacidad? ¿Cómo divergen en sus opiniones los ciudadanos de los diferentes países europeos acerca de la seguridad y de la privacidad?

En respuesta a estas preguntas, este proyecto ha consultado a los ciudadanos de 9 Estados miembros y Estados asociados de la Unión Europea (España, Reino Unido, Italia, Austria, Noruega, Dinamarca, Hungría, Suiza, Alemania). SURPRISE no sólo examinará si y cómo los ciudadanos parecen estar dispuestos a aceptar nuevas medidas de vigilancias a cambio de una mayor seguridad, también se ha discutido con los ciudadanos en qué medida las tecnologías de vigilancia vulneran la privacidad y si realmente aumentan la seguridad. Asimismo, el proyecto ha explorado nuevas alternativas en las que la seguridad se pueda pensar y lograr sin utilizar necesariamente tecnologías de vigilancia que pongan en peligro los derechos fundamentales, pudiendo ser sustituidas por otras

tecnologías así como por otras medidas de innovación social u organizativa.

SURPRISE tiene así la intención de proporcionar dos tipos de resultados: (1) un profundo conocimiento científico de la razón de ser del rechazo o de la aceptabilidad de las soluciones de seguridad, y (2) ofrecer directrices para los expertos en seguridad, proveedores, diseñadores de políticas y los reguladores que permitan aumentar la pertinencia y la eficacia de las medidas de seguridad que deben enfrentar las complejas realidades sociales.

El proyecto SURPRISE ofrece un nuevo concepto de la investigación social, demostrando que

la conjugación de la metodología cuantitativa y cualitativa real y efectiva es posible y deseable. Supone también un impulso definitivo a la participación ciudadana en la redacción de políticas públicas controvertidas, y en el diseño de un futuro compartido. Una guía desde la que enfocar otros estudios igualmente complejos en los que la aceptabilidad social resulte crucial para seguir avanzando en una sociedad que cada día tiene que hacer frente a nuevos retos científicos, nuevos desafíos sociales y políticos y constantes amenazas terroristas. En definitiva SURPRISE supone un paso hacia delante para la consecución de un modelo de sociedad democráticamente participativo, políticamente responsable y socialmente consecuente.

La ciencia es fuente de información. No nos dice lo que tenemos que hacer. La decisión es nuestra.

2 Resumen

Casi nadie podría hoy en día 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.

Tras los ataques terroristas 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, se han modificado las leyes en vigor y se han aprobado otras nuevas que permiten el acceso a este tipo de información con fines de seguridad. Aunque los gobiernos cuentan con un gran número de fuentes de inteligencia "oficiales", se han dado cuenta de que se podrían detectar actividades de posibles terroristas o delincuentes por nuevas 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. Por lo tanto, es posible que el hecho de obtener más información sobre estas actividades sea la clave para encontrar a terroristas y delincuentes. Más allá, muchos gobiernos consideran que hacer uso de las nuevas tecnologías de seguridad no solo facilita la detención de criminales sino que también juegan un importante papel de prevención haciendo posible su identi-

ficación antes de que comentan ningún delito. 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", se trata de ***tecnologías 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.

A lo largo de esta investigación hemos estudiado en detalle cinco de estas tecnologías:

- Cámaras de video-vigilancia inteligentes: sistemas de CCTV que no sólo se limitan a vigilar espacios públicos. Las 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.

Además, 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. Con su utilización resulta inevitable que se obtenga y analice información de personas inocentes y, en el caso de algunos sistemas, este análisis se produce incluso de manera intencionada. Como tal, estas tecnologías cuentan con pueden invadir nuestra 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 ofrece la utilización de este tipo de tecnologías, algunos ciudadanos no tienen clara su opinión cuando conocen que su información personal se utiliza con fines de seguridad. Si a cambio 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 estas tecnologías 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 se abordaron durante los dos encuentros ciudadanos celebrados en Madrid en febrero y junio de 2014 y cuyos principales resultados abordaremos a lo largo de las siguientes páginas.

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, orientación sexual, género u opiniones políticas), ¿qué haría? Esta es la razón por la cual una vigilancia

excesiva puede tener un impacto negativo en determinados derechos humanos como la libertad de expresión. En ese sentido, la vigilancia también causaría perjuicios a nivel de confianza social, puesto que los unos tendríamos miedo de los otros. Son muchas las cuestiones que poner en la balanza a la hora de utilizar diferentes tipos de datos de vigilancia en el contexto de la seguridad.

3.2 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 diseña” 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

¿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.

A continuación presentaremos brevemente las cinco tecnologías que se han tratado en los eventos participativos organizados por el proyecto SURPRISE. Para una información más detallada sobre los diferentes usos, ventajas e inconvenientes del uso de estas tecnologías, en la página web del proyecto www.SURPRISE-project.eu pueden consultarse los materiales informativos, revistas y vídeos que se han elaborado a lo largo del proyecto.

5 CCTV inteligentes

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.



5.1 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:

- 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.

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

- Cuando una tecnología de seguridad es eficaz, los ciudadanos se sienten más seguros.
- Las cámaras CCTV inteligentes digitales captan muchos más detalles que las cámaras CCTV tradicionales.
- El nivel de privacidad mejora puesto que es posible oscurecer ciertas partes de las imágenes.

5.2 Problemática

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

Los algoritmos de CCTV inteligentes que se utilizan hoy en día presentan una serie de fallos que 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.
- Las cámaras tienen más dificultades para identificar qué está sucediendo en una multitud.
- Existe el riesgo de que los sistemas, ya sea de forma deliberada o accidental, estén programados para centrarse en minorías de un modo discriminatorio.
- El nivel elevado de falsas alarmas podría hacer que se perdiese 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.
- dificulta que los ciudadanos sepan que los está vigilando un CCTV inteligente.
- 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.

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.
- 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 abordo. El uso de drones causó mucha polémica cuando los Estados Unidos comenzaron a intensificar su uso en su guerra contra el terrorismo 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.



El proyecto SURPRISE nos hemos centrado en los drones civiles destinados a acciones de seguridad.

6.1 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.
 - Los drones, a diferencia de los equipos humanos que persiguen personas u objetos, no se cansan y son menos visibles.

2. Reducen el riesgo ante posibles delitos y el grado de intromisión.

6.2 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, los drones pueden tomar imágenes de propiedades privadas a las que las cámaras de CCTV no pueden acceder.
 - 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.
 - 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.
 - Los drones equipados con instrumentos de registro de datos pueden ser vulnerables a piratería.
2. 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

La técnica denominada “inspección profunda de paquetes” (DPI por sus siglas en inglés) permite a las compañías, servicios de inteligencia y gobiernos leer el contenido de las comunicaciones enviadas a través de internet. Para establecer un paralelismo, en el servicio de correo postal, la DPI sería el equivalente a abrir las cartas, leerlas y, en algunas ocasiones, cambiarlas, borrarlas o no entregarlas. La DPI es capaz de controlar cada uno de los aspectos de las comunicaciones digitales. Esto abarca desde la información que usted lee online, las páginas web que visita, los vídeos que ve y las palabras que busca, hasta con quién se comunica por e-mail, mensajería instantánea o redes sociales.



7.1 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 o perjudiciales. 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.

7.2 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.
- Dado que las comunicaciones ya no son privadas 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.
- En países en los que el gobierno central y los proveedores nacionales de comunicaciones están estrechamente relacionados, la información podría compartirse de forma que el Estado tenga acceso a todas las comunicaciones de los ciudadanos.

3. Es complicado saber exactamente quién y dónde se está utilizando la DPI.

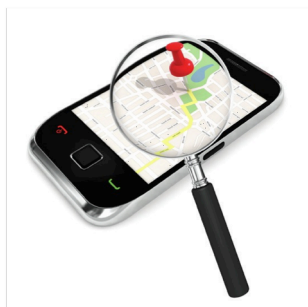
- Las disposiciones legales tendrían que ser las mismas para todo el mundo.

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 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.



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.

8.1 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.

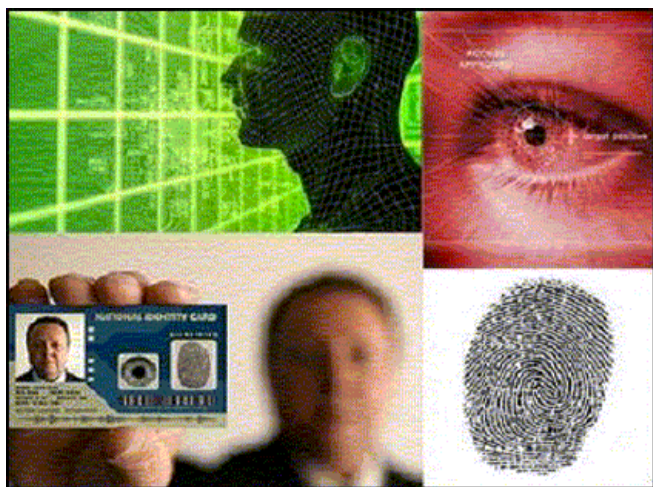
8.2 Problemática

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.. 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.
 - 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.
 - 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.



9.1 Mejoras en la seguridad

La biometría pueden mejorar la seguridad en los siguientes sentidos:

3. 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.
4. La obtención de datos biométricos se puede utilizar para aumentar la seguridad de aquellas actividades de procesamiento de datos particularmente sensibles.

9.2 Problemática

Se plantean ciertos inconvenientes que deben tenerse en cuenta:

1. Los datos biométricos no son infalibles.
2. Se podría afirmar que dos capturas de un mismo rasgo biométrico nunca serán

exactamente iguales.

3. Además, las características biométricas de una persona pueden cambiar durante el transcurso de su vida. Por tanto, un determinado sistema biométrico puede dejar de reconocer a dicha persona.
4. Asimismo, también es posible falsificar los datos biométricos, lo cual aumenta las posibilidades de usurpación de identidad.
5. 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.
6. 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.
7. 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.
8. 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 participación ciudadana en el proyecto SURPRISE: la Cumbre Ciudadana y la Reunión Ciudadana

A la hora de explorar los eventuales marcos interpretativos existentes, SURPRISE adoptó una metodología innovadora y original, como se refleja en el diseño de la investigación y los procedimientos de recogida de datos. No se trata solo de la puesta en marcha de un macro ejercicio participativo, sino también de la implementación de un complejo diseño de la investigación que permite conjugar tanto métodos de investigación cualitativos como cuantitativos. Este diseño de la investigación mixto no solo permite entender las razones que se esconden detrás de las decisiones tomadas por los ciudadanos (análisis cualitativo de los datos) si no también evaluar de forma sistemática y objetiva el nivel de asociación entre los distintos factores (análisis cuantitativo de los datos) (Degli Esposti, Santiago y Pavone, 2013). Estas características diferencian a SURPRISE de otros proyectos, como PRISMS y PACT, que persiguen objetivos similares.

10.1 La Cumbre Ciudadana: Citizen Summit

La versión de Citizen Summit desarrollada por el *Danish Board of Technology* en colaboración con *The Open University* garantiza que los ciudadanos no sólo tuvieron la oportunidad de ser informados, reflexionar y expresar sus preferencias entre un conjunto de opciones predeterminadas, sino que también tuvieron la oportunidad de expresar sus propios puntos de vista, ideas, conocimientos y propuestas.



La metodología propuesta por SURPRISE se apoya de hecho en los estudios CTS que han demostrado que el nivel de concienciación e información de los ciudadanos influencia en larga medida su preferencia u aversión hacia las nuevas tecnologías. Por eso la metodología del SURPRISE organizó los eventos a lo largo de los cuales los ciudadanos han tenido la oportunidad de reflexionar sobre el tema tratado de forma completa e informada. Los participantes tuvieron además la posibilidad de escuchar las opiniones de otras personas sentadas en su misma mesa y de discutir e intercambiar sus opiniones como sucede habitualmente en la vida real.

Y es que para responder a las preguntas del cuestionario y para apoyar los debates que se propusieron tras las baterías de preguntas, los participantes contaron con un documento escrito, una revista informativa que fue enviada a sus domicilios con unas semanas de antelación a la celebración del evento para que, quienes así lo desearan, pudiesen informarse sobre el funcionamiento, ventajas e inconvenientes de las SOSTs. Este material ha sido diseñado minuciosamente por el equipo de investigación del proyecto buscando al mismo tiempo la rigurosidad de la información y la claridad de su presentación siempre desde una posición neutral y libre de juicios de opinión hacia las SOSTs. Además, como apoyo visual, a lo largo de la jornada participativa se proyectaron tres películas cortas de unos cinco minutos, una por cada una de las tecnologías seleccionadas para ser evaluadas, así los participantes escucharon a expertos en el ámbito y contando así con distintos argumentos sobre los que luego discutir en las mesas de debate y votar en el turno de preguntas. De este modo hemos podido identificar los criterios desde los que la población estructura su discurso y su posición hacia las SOSTs de una forma reflexionada y reflexiva.

Respecto a la parte cuantitativa del diseño de la investigación, el cuestionario no solo permite medir la gran cantidad de factores que han sido

seleccionados y que hasta la fecha no han sido nunca probados en un mismo estudio, siendo los trabajos precedentes más sencillos en su diseño y por lo tanto menos ambiciosos; sino que además, en los eventos participativos, se utilizaron un sistema de voto con mandos a distancia (*clickers*). Así, se proyectaron en una gran pantalla a lo largo de la duración del evento las preguntas y los participantes las respondieron utilizando el mando a distancia. Este procedimiento obliga a que tanto las preguntas como las categorías de respuesta sean sencillas en un doble sentido, en cuanto a su redacción a fin de que puedan traducirse comprenderse sin equívocos en las 12 lenguas del conjunto de países en los que se celebraron los citizen summit; al mismo tiempo las categorías de respuesta están limitadas a fin de que puedan ser respondidas utilizando el mando pulsando un único botón.

A pesar de las dificultades, el formato elegido está lleno de ventajas, se trata de un formato dinámico, característica realmente fundamental en un evento que dura más de seis horas, y es que la utilización de los mandos permite comentar los resultados de cada pregunta en tiempo real y hacer comentarios y debatir tras las votaciones, así tras cada pregunta, en la pantalla se muestran de forma inmediata, y tras cada votación, el reparto de los resultados de las respuestas. Por último el diseño también permite tener todos los datos procesados tan pronto se termine cada evento, independientemente del idioma utilizado, sin tener que introducirlos manualmente en la base de datos general desde cuestionarios en papel, lo que resultaría mucho más tedioso y lento agilizándose por lo tanto la siguiente etapa de análisis de los resultados.

En definitiva, aproximadamente 200 ciudadanos en cada uno de los 9 países europeos (España, Reino Unido, Italia, Austria, Noruega, Dinamarca, Hungría, Suiza, Alemania) representados en el SURPRISE fueron invitados a participar y expresar sus opiniones a lo largo del primer trimestre de 2014 mediante grupos de debate y votos individuales, con respecto a los dilemas fundamentales planteados en SURPRISE.

Se organiza en cada uno de los países participantes en el proyecto un citizen summit en el que mediante la innovadora metodología propuesta probamos el funcionamiento del modelo diseñado

y la influencia de las dimensiones que influyen en la aceptabilidad social de las SOSTs, buscando comprender también los criterios desde los que la población sostiene sus argumentos a la hora de evaluar estas tecnologías.

10.2 La Reunión Ciudadana: el Small Scale Event

Los principales objetivos de la segunda fase de eventos participativos a pequeña escala son la validación y profundización en los resultados de los Citizen Summit:

- A través de la investigación en detalle de los factores y criterios que tienen influencia en la opinión y la actitud de los ciudadanos hacia las SOSTs
- Estudiando la percepción de los ciudadanos hacia dos tecnologías de vigilancia adicionales, los drones y la biometría
- Examinando en detalle preguntas planteadas en las primeras etapas de la investigación

En los cinco eventos a pequeña escala celebrados se introdujo una herramienta web innovadora llamada “Sistema de Soporte de Decisiones SURPRISE” que ayudaba a los facilitadores de las mesas de debate a implicar a los ciudadanos en el proceso de evaluación de las tecnologías, además, permitía que los tomadores de notas introdujesen la información en la herramienta relacionada las cuestiones más importantes que se trataban en los debates así como las recomendaciones y las mensajes orientados a los responsables políticos, y ésta estuviese disponible online en tiempo real.



En conjunto los cinco eventos contaron con la participación de 190 ciudadanos repartidos en cinco mesas –una por tecnología- en cada uno de los cinco países.



El evento tuvo una duración de tres horas en las que los participantes debatieron y respondieron a las preguntas que se plantea la investigación:

- ¿Qué significa la seguridad y la inseguridad, cuales son los retos de la seguridad?
- ¿Qué significado tienen los conceptos de seguridad e inseguridad para los participantes; ¿cuáles son los principales retos de seguridad?

- Que relación consideran los ciudadanos que existen entre los problemas de seguridad y las medidas de seguridad.
- ¿Cómo perciben los ciudadanos la vigilancia en general, y en relación con SOSTs en particular?
- ¿Cómo la propia vigilancia afecta la vida cotidiana de los ciudadanos?
- ¿Qué entiende la gente por privacidad y protección de datos?
- ¿Cuál es el núcleo de la vida privada que debe ser protegido al máximo?
- ¿Qué consideran los ciudadanos sobre el marco legal y de control relativas a las tecnologías de seguridad basados en la vigilancia, y qué tipo de información o comunicación querrían tener?
- ¿Cómo se puede entender mejor la relación entre la confianza y el temor hacia el abuso del poder que agencias de seguridad que emplean estas tecnologías pudieran llegar a ejercer?

11 Principales resultados

Los participantes de la Cumbre Ciudadana se sienten bastante seguros en su vida diaria y consideran que España es un lugar seguro para vivir. Aun así, apoyan la introducción de SOSTs como una medida general para mejorar la seguridad nacional pese a que no consideraron que estas tecnologías realmente mejoraren su propia seguridad individual.

Creo que este país es un lugar seguro en el que vivir.



De hecho, los participantes de la cumbre, se sienten seguros cuando se refieren de forma general al concepto de seguridad pese a mantienen ciertas inquietudes y preocupaciones en áreas o dominios específicos, como el ciberespacio. Esta incongruencia da lugar a una paradoja interesante, en la que la gente se siente segura, pero reclama más y más medidas y tecnologías de seguridad. Esta paradoja puede entenderse debido al hecho de que los ciudadanos no están hoy en día dispuestos a tolerar los riesgos o amenazas. Parece que existe entre la población un deseo de seguridad absoluta, que obviamente no es posible, y que se ha inculcado gradualmente en las sociedades occidentales.

En general creo que las tecnologías de seguridad basadas en la vigilancia deben utilizarse rutinariamente para mejorar la seguridad nacional.



En segundo lugar, la mitad de los participantes adopta un criterio de compensación o trade-off en la relación entre la privacidad y la seguridad: afirmando explícitamente que la relación entre la seguridad y la privacidad establece un juego de suma cero. Sin embargo, esto no significa que los participantes estén dispuestos a comerciar con su privacidad a cambio de seguridad.

Tercero, el posible uso de estas tecnologías en el futuro genera una importante preocupación lo que afecta negativamente a su aceptabilidad. A los participantes les preocupa de que estas tecnologías puedan someterse a abusos para satisfacer los intereses de las poderosas élites políticas y/o de los agentes comerciales. Y es que los participantes desconfían de las autoridades públicas y los organismos de seguridad que utilizan las tecnologías de seguridad orientadas a la vigilancia.

En el Citizen Summit descubrimos que los sistemas de circuito cerrado de televisión inteligentes son percibidos en España de forma diferente dependiendo de su uso privado o público. Los ciudadanos son más críticos hacia el uso privado de las cámaras de circuito cerrado, que se consideran intrusiva, mientras que reciben bastante apoyo en su utilización en lugares públicos.

Además los CCTV tradicionales recibieron en el Citizen summit más apoyo que los CCTV inteligente. Los sistemas de CCTV inteligentes ubicados en zonas residenciales privadas, por ejemplo, se consideran ejemplos típicos de medidas concebidas para proteger a las familias ricas y sus pertenencias, aumentando la separación entre ricos y pobres, y las desigualdades sociales. Mientras que los sistemas tradicionales de CCTV se consideran formas bastante equitativas de vigilancia.

En cuanto a la DPI, la falta de transparencia e información en torno a esta tecnología plantea serias preocupaciones entre los ciudadanos. No está claro cuáles son las normas que establecen lo que se define normal o lo que se considera como un comportamiento anormal y por lo tanto es susceptible de ser vigilado por esta tecnología y

eso preocupa enormemente a los ciudadanos. Las decisiones autónomas que toman los algoritmos con los que funciona la DPI también levantan y dejan importantes preguntas sin respuesta.

Para los ciudadanos estas tecnologías se implementan bajo una estrategia del miedo orientada a acrecentar la sensación de inseguridad de los ciudadanos manipulando así sus sentimientos y orientándolos hacia la aceptación de estas tecnologías. Sin embargo cuando se les da la oportunidad de valorar su necesidad, los ciudadanos coinciden en opinar que la tecnología es o debería ser una **herramienta neutral**, ni buena ni mala en sí misma, el peligro está en los **usos** futuros y en los posibles **abusos** a los que pueda someterse su utilización por parte de la élite poderosa.

Es por ello que los ciudadanos reclaman que se establezcan unos límites claros sobre cuales son los marcos de actuación de este tipo de tecnologías, cuales son los parámetros bajo los que se ejerce la vigilancia para poder obrar en consecuencia. También destacan que su confianza en los responsables es una **confianza limitada o contextualizada** que depende de cuales sean los fines por los que se implementa la tecnología y cuales sean los mecanismos de funcionamiento y control de la misma. Esta confianza se renegocia constantemente y no puede ser considerada como una postura estable.

Para los ciudadanos la implementación de nuevas tecnologías de seguridad basadas en la vigilancia responde a una estrategia de abaratamiento de los costes de la seguridad, y preferirían que se invirtiese en medios humanos tradicionales como la policía, y se fomentasen los comportamientos cívicos.

Profundizando en la necesidad de la vigilancia, algunos ciudadanos señalan que el conflicto con la aceptabilidad de las tecnologías de seguridad orientadas a la vigilancia se evitaría si se atacasen las causas que están detrás de la inseguridad invirtiendo en educación y empleo para evitar la exclusión social.

En conclusión lo que los ciudadanos reclaman es una legislación adaptada a la nueva realidad del siglo XXI y a las nuevas amenazas, y

que respetando las desigualdades regionales funcione a nivel internacional ya que los nuevos riesgos no responden a las fronteras nacionales.

Los mecanismos de vigilancia que esas nuevas leyes definan han de ser transparentes y ha de permitirse y facilitarse la comprensión del funcionamiento y el uso de las tecnologías de seguridad por parte de los ciudadanos, para ello se consideran fundamentales las campañas de información y educación de los ciudadanos, y se sugiere la creación de un mediador que permita a los ciudadanos conectar con los responsables de estas tecnologías para saber en todo momento cómo éstas invaden su privacidad y cuáles son sus derechos en caso de abuso.

En cuanto al trade-off entre privacidad y vigilancia, según la opinión de los ciudadanos no se puede realizar una balanza entre privacidad y libertad en el caso del uso de las tecnologías de seguridad orientadas a la vigilancia ya que los riesgos que este tipo de tecnologías pretende evitar son riesgos sociales que afectan a los ciudadanos de manera individual. Por ejemplo, a la mayoría de los ciudadanos de a pie les preocupa el terrorismo y consideran que sea uno de los principales problemas del mundo contemporáneo, sin embargo muy pocas personas creen que puedan ser víctimas de un ataque terrorista y por tanto el coste que la utilización de estas tecnologías supone les resulta inasumible ya que pone en riesgo los valores democráticos y los derechos humanos, bajo esta argumentación la balanza no puede realizarse ya que los niveles son diferentes, los beneficios que estas tecnologías ofrecen están en la protección de los individuos, mientras que los riesgos que suponen atacan a las estructuras sociales.

Frente a este argumento si una persona concreta ha tenido una experiencia directa y traumática entonces nunca someterá sus opiniones a la balanza ya que para esa persona la privacidad deja de ser una prioridad y aceptará cualquier tipo de limitación de sus derechos y libertades con tal de protegerse del daño.

Para completar estas ideas principales sugeridas en el citizen summit, en la reunión ciudadana a pequeña escala se profundizó en las

ideas de vigilancia y privacidad, los ciudadanos tienen una idea clara de que la privacidad es todo aquello que la persona no quiere que sea conocido por terceros siempre y cuando no se trate de una actividad o comportamiento delictivo. Especialmente y de forma incuestionable se entiende que la privacidad es todo aquello que sucede dentro de nuestro domicilio familiar, esta percepción resulta especialmente problemática dado que toda la actividad que podemos tener a través de la web, es a juicio de los ciudadanos una actividad privada, y eso incluye –en su opinión– no sólo las comunicaciones a través de email, sino también la actividad comercial online o la presencia en redes sociales.

Asimismo, uno de los principales problemas en la aceptabilidad de este tipo de tecnologías está en la ruptura de la confianza en la clase política. Si los ciudadanos no confían en los responsables de la toma de decisiones con respecto a la seguridad tampoco confían en la implantación de tecnologías de vigilancia con fines de seguridad. Esta actitud de rechazo se agrava al no estar claros los límites en el uso comercial y el uso con fines de seguridad en la mayoría de estas tecnologías. Los ciudadanos reclaman por tanto ser parte en el debate y tener la posibilidad real de decidir en este y otros asuntos que afectan a la vida, la seguridad y la privacidad.

Para terminar, y de forma esquemática, queremos presentar las que son las principales conclusiones que se extrajeron durante esta reunión sobre cada una de las tecnologías analizadas:

Inspección profunda de paquetes (DPI):

- Su funcionamiento resulta difícil de entender.
- Tiene algunas ventajas de seguridad nacionales en la lucha contra lo que la población considera graves delitos como la pornografía o el terrorismo.
- Resulta altamente intrusivo cuando se utiliza para la vigilancia de masas (un peligro para la libertad de expresión y la libertad democrática, ya que los datos podrían ser manipulados, modificados o interpretados fuera de su contexto).
- Se reconoce que puede ser una herramienta útil, pero su utilización se restringe a aquellas

situaciones en que se maneje con autorización judicial.

Smartphone seguimiento de la ubicación (SLT)

- Se considera la menos intrusiva de las tecnologías analizadas.
- Mejora la sensación de seguridad personal, gracias a la disponibilidad permanente de ponerse en estar localizable por parte de los servicios de emergencia.
- La intrusividad que se percibe en su utilización se refiere a la falta de control sobre los datos extraídos relacionados con la localización y su posterior utilización.
- La desconfianza hacia los proveedores de servicios es evidente y tiene un impacto negativo en la confianza hacia las autoridades de seguridad que utilizan SLT.

La identificación biométrica

- Es poco conocida ya que se encuentra en su etapa inicial de desarrollo y a los ciudadanos les resulta complicado posicionarse acerca de su utilización con fines de seguridad.
- Se considera útil en las investigaciones
- Se considera altamente fiable y segura
- No se percibe como una tecnología intrusiva de la privacidad salvo en aquellos casos de personas con discapacidad o alguna característica física que pueda ser objeto de discriminación.
- Las preocupaciones están relacionadas con el desarrollo y almacenamiento de bases de datos biométricos y su posible uso futuro.

(Smart) CCTV

- Las funciones de las CCTV inteligentes no se conocen.
- Se consideran útiles en su capacidad de prevención con respecto a los delitos menores.
- Puede ayudar en las etapas de investigación de delitos.

- Mejoran la sensación de la seguridad pública debido a su posible efecto disuasorio.
- Es de las tecnologías estudiadas la que cuenta con una mayor aceptabilidad.

Drones

- Los ciudadanos desconocen como pueden funcionar como tecnología de vigilancia orientada a la seguridad.
- Uso militar genera gran desconfianza
- Se considera que pueden mejorar la seguridad nacional y personal sólo si se utiliza en situaciones específicas, tales como:
 - Accidentes, desastres, ataques terroristas, incendios - para proporcionar una visión general;
 - Para la búsqueda y rescate para evitar poner a las personas en situaciones de riesgo;
 - Después de un grave delito durante el seguimiento de los criminales;
 - En situaciones peligrosas para aumentar la seguridad pública (por ejemplo, eventos masivos)
- Se considera una tecnología muy intrusiva si se utiliza para la prevención en términos generales.

Recomendaciones

- El uso de las SOSTs debe ser proporcionado y evitando la vigilancia masiva;
- Su despliegue y utilización debe estar estrictamente regulada y ser transparente.
- Se deberá proporcionar información sobre la vigilancia y el control en un lenguaje comprensible para los ciudadanos.
- El uso complementario de "máquinas", además de los humanos es aceptable en el corto plazo, pero a largo plazo, la raíz de los problemas de seguridad deben ser subsanadas;

- La vigilancia debe respetar la privacidad y las libertades civiles.
- Las discusiones públicas y debates abiertos sobre el uso de estas tecnologías son necesarias;
- Las personas deben ser educados para utilizar las tecnologías de vigilancia de una manera más responsable y prudente ya en la escuela.

Conclusiones

En los últimos diez años, en un contexto de terrorismo global, proliferación nuclear, y delincuencia transnacional organizada, nuevos enfoques para garantizar la seguridad nacional y personal han surgido. De hecho, la seguridad es un concepto altamente controvertido cuyas definiciones cambian su alcance y profundidad a medida que escribimos. Los nuevos enfoques de la seguridad se caracterizan por una serie de principios y características, que sin duda tienen implicaciones cruciales en la relación entre la seguridad, la tecnología y la democracia.

Un énfasis mayor en la tecnología de vigilancia a menudo implica una menor atención hacia los determinantes sociales y económicos de la inseguridad y la delincuencia y restringe enfoque sólo a los aspectos de seguridad que pueden ser abordados por una tecnología de vigilancia. Y es que estas tecnologías a menudo han introducido la vigilancia como una práctica rutinaria, con el resultado -no deseado- de una restricción significativa de la privacidad individual, y, por lo tanto, de los derechos democráticos y civiles que dependen de la preservación del anonimato, la confidencialidad y la intimidad de la conducta.

Así a los ciudadanos a menudo se les pide que renuncien a parte de su libertad a cambio de un mayor nivel de seguridad. Sin embargo los ciudadanos no pueden ser libres, a menos que estén seguros y no pueden estar seguros a menos que sean libres o ya no serían ciudadanos. Es por esto que mantener el trade-off entre seguridad y libertad resulta problemático y tal y como se ha enunciado a lo largo de estas páginas deben dejar de considerarse como conceptos mutuamente excluyentes para pasar a ser ideas mutuamente constituyentes.

Información sobre el documento

El presente documento informativo se ha elaborado con el fin de informar a los ciudadanos de los resultados obtenidos en las reuniones ciudadanas organizadas por el proyecto SURPRISE en España.

La información contenida en el presente documento proviene por una parte 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. Y por otra parte, de los resultados obtenidos de los debates y cuestionarios planteados a los participantes de la Cumbre y la Reunión ciudadana celebradas en Madrid.

- Autores: Dr. Vincenzo Pavone, Consejo Superior de Investigaciones Científicas, Dra. Elvira Santiago Gómez, Consejo Superior de Investigaciones Científicas, Los capítulos 1 a 8 son una reedición de los materiales utilizados para las revistas informativas que han contado además con los autores: Dra. Kirstie Ball, The Open University; Maria Grazia Porcedda y Mathias Vermeulen, EUI; Regina Berglez, IRKS; Eva Schlehahn, ULD; Márta Szénay, Medián.
- Consejo Asesor en Materias Científicas: Dra. Monica Arenas 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: Elvira Santiago Gómez, basado en las versiones de Zsolt Bartha, Medián, y D. Peter Devine, D. David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University utilizado en las revistas informativas.
- 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 nº 285492.
- La presente publicación se encuentra disponible en: <http://SURPRISE-project.eu>

Miembros del Proyecto

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

